International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)
ISSN: 2305-0543 (Online), ISSN: 2411-6173 (Print)
Vol. 12 (44), Apr. 2022, pp. 5202-5207

Detection of rogue nodes in broadcast routing algorithm using the signal power in VANET

Somayyeh ImanAlizadeh
Islamic Azad University, Shahriyar Branch,
Shahriyar, Iran
imanalizadehsomayeh@yahoo.com

***Abstract*— The vehicular ad hoc networks have a considerable role in increasing the roads safety and traffic improvement in the intelligent transportation systems. To this purpose, there is the need for efficient emission of data among vehicles. However, these vehicular ad hoc networks have their own special features such as nodes movement, the topology limited to predefined roads, and high speed of vehicles. Thus, designing of the routing protocols is a challenging work. One of the significant challenges is the safety of vehicular ad hoc networks when they are communicating with each other or with the roadside units. The routing protocols in vehicular ad hoc networks must be able to avoid the attacks and detect the rogue nodes. In this paper, by concentrating on safety in vehicular ad hoc networks, a combinational criterion is proposed to detect the rogue nodes that according to calculating the power of the real signal and power of signal obtained by sending the transferred beacon packets in terms of distance, if the difference of which is larger than a threshold value, the node will be considered as rogue and omitted from the sending set. The results of simulation have represented that proposed method has caused 14% and 7% increase of delivery rate, 18% and 17% increase in the throughput, 26% and 12% decrease in the packet loss rate, 28% and 19% decrease in the end to end delay compared to the FD and BDSC methods.**

Keywords*— *vehicular ad hoc networks, rogue nodes, broadcast of data messages, signal power

I. INTRODUCTION

The existed applications in wireless networks are developing day by day. One of the emerging technologies in this field is the ad-hoc mobile networks that have been converted to the one of the important parts in our daily life. The ad-hoc mobile network is a wireless network without the infrastructure in which the nodes are able to be self-configured and self-organized [1]. The vehicular ad hoc networks are the sub class from the ad-hoc mobile networks that will provide the capability of presenting the communicational services among the vehicles and the vehicle with infrastructure [2].

The main idea of these networks is the present of communicational services and ability to connect the moving vehicles to each other. The vehicular ad hoc networks in recent years regarding to their wide capability and supporting of various applications have attracted many researchers attention. These applications have been used in different ranges such as the making connections among the vehicles in order to better safety and the applications that present the facility services to passengers and presentation of traffic information. The vehicular ad hoc networks will have a considerable role in increasing the roads safety and improving the traffic in intelligent transportation systems. For this aim, there is the need for effective methods when the data emit among the vehicles. Many protocols have been investigated and evaluated for routing in vehicular ad hoc networks in order to improve the data dissemination. When the data disseminates, for ensuring the homogeneous and proper network operation, considering safety issues is one of the important challenges in vehicular ad hoc networks that has attracted many researchers attention [3].

Still, so far the method has not been presented to able to all needs related to various applications and security issues in these types of networks which is consistent with natural features of the vehicular ad hoc networks. The aim of conducting this paper is to concentrate on vehicular ad hoc networks and the safety in such networks in an attempt for providing a comprehensive investigation of it.

Also, the aim is to improve the parameters of the services quality such as delivery rate and throughput [4]. In the following, the previous works will be reviewed in section 2 and then, in section 3, the BDSC routing protocol will be discussed. In section 4, the details of proposed method are investigated. In sections 5 and 6, the evaluation criterion and the results of proposed method are given. In last section, the conclusion is brought.

II. 2. THE PREVIOUS WORKS

In [5], a method named Event Based Reputation System (EBRS) is proposed to detect and prevent Sybil attacks. In this method, each vehicle has a general key and an alias for a limited and authenticated time by means of the trusted authority (TA) on the RSU (road side unit). Moreover, each road side unit will save an alias and also a verification certificate for each vehicle. When the vehicle V receives a message in relation to an event from the node N that is in the vicinity of it, V sends the message including the alias and temporary verification certificate to the road side unit.

Then, the road side unit has ability of key of corresponding to N. If the encrypted certificate with received certificate is the same, N will be detected as authenticated node in the network and authority of which is verified. Therefore, by this method, the possibility of forging, the identity change will reduce in network. Moreover, the vehicle V will save the reliability value of event E in its event table or if it exists before in the table, will update it. If the reliability value of event E is less than a threshold value, the warning

Article History:
Received Date: Jan. 07, 2022, Accepted Date: Mar. 05, 2022, Available Online: Apr. 01, 2022

message will not be sent to other drivers. If the warning message is received from an attacker and rogue node, the reliability value of event will not be changed in neighbors table, because this event has been reported by other vehicles as a false event. With regarding to the conducted simulation from the proposed method EBRS, this method will reduce the Sybil attacks and their detection effectively. However, this supposition that road side units and vehicles always simultaneously with each other exposed to hazard does not hold.

In [6], a protocol named TFDD is presented based on the trust created among vehicles in order to capability of detecting the DoS and DDoS attacks as distributed. Each vehicle V uses the various parameters using the different modules to detect such attacks. The first used parameter is honesty weight (H) that for each neighbor node (N) has been initialized. If the vehicle V receives the packets more than a threshold value from a neighbor vehicle, the detection module will penalize the penetration of node N by reducing the honesty value.

The second parameter used in this method is quality weight that refers to the quality of received packets in vehicle N. these two parameters will be evaluated periodically by the delay confirmation module in order to calculate the probability weight of Dos and DDoS generated Dos weight (DW) of attacks for investigating and detecting the kinds of attacks.

On the other hand, the trust weight (TM) for each message M received from the vehicle N is combined with parameter Q by the same module. If the TM is less than a threshold value, the least value of those will be considered. Then, two factors of TM and DW will be combined with each other and reliability level between two vehicles V and N will be calculated. If the both values TN and DW are less than a threshold value, vehicle N will be added to the black list of vehicle V. According to the conducted simulations and obtained results and the allocated threshold values, this method increases the detection rate of attacks.

In [7], a model is presented trust-based based on central part to detect the attacks of black hole in vehicular ad hoc networks. In this method, each vehicle uses three reliability parameters with the initialized presuppose values. At first, the vehicle A calculates its reliability value to a neighbor vehicle like B based on the rate of sending data and the weight of sending data regarding its classification such as safety traffic, traffic efficiency, and entertaining data. Then, the value proposed by the vehicle A to the vehicle B is calculated based on the value of trust in its neighbors and the value of trust in B. Also, the third used parameter is the general trust that will be calculated by combining two other parameters.

If the value of general and comprehensive trust of the vehicles A and B is higher than a threshold value, vehicle B will be detected as attacker in network and as a result, it is isolated. Through this method, the attacks of black hole can be detected with maintaining the network operation. Based on the conducted simulations, the rate of malicious vehicles in network has not been detected. In [8], a mechanism has been done to intelligently detect the false behavior of nodes called CEAP based on support vector machine and optimization of the services quality in routing protocol OLSR (optimized link state routing). The aim of this method is to detect the false behavior of nodes.

The proposed model in this method includes four steps. During the phase of gathering data, the cluster-heads and other members of cluster monitor continuously the behavior of MRP nodes (nodes that have link with two-step neighbors). After the phase of exchanging data including the share of gathered data with other cluster members, each vehicle performs monitoring operations in order to classify the MRPs as rogue node and or cooperative node. This issue is possible based on the tracking and monitoring the nodes behavior. Finally, in dissemination step, the cluster-heads are able to exchange data with each other.

Through the conducted simulations, it has been represented this method can provide the high delivery rate of data and detect the high rate of attackers. This method, still, has supposed the cluster-heads have been authenticated by a third party. In [9], a trust-oriented mechanism called T-VANET is proposed that mainly includes two parameters that these parameters work as parallel with each other. These two parameters are the trust among the vehicles with each other and trust between the vehicles and road side units. The trust among vehicles will be calculated by combining the evaluation of data content from the messages received from the neighbor vehicles N that are a report from its own neighbors.

These reports are done by nodes to detect the positive and negative changes in behavior of vehicle N. the RSU trust also to vehicles is by gathering the RSUs report from the vehicles in their behavior that will cause the obtaining a trust from the nodes. Since the RSUs are connected to each other, after that RSUs and vehicles discovered the trust values between themselves and their neighbors, by combining these two values, a total trust value will be obtained. If there is no road side unit in vicinity of the vehicles, this estimation can be done as limited. After it, this trust value will be exchanged periodically among vehicles using the cooperative-oriented awareness messages (CAM) by adding the fields to it. CAM in ETSI standard is the messages that will be exchanged periodically between the vehicles and roadside units [10].

CAM in this method will be exchanged to evaluate reliability of nodes. Another standard of ETSI in ITS named decentralized environmental notification messages (DENM) will be done periodically in order to calculate the reliability of the event-oriented messages [11]. The general trust of vehicle V will be calculated based on the reports obtained from the trust of event-oriented messages. The events with reliability less than a threshold value will not be rebroadcasted. After doing these steps, the general trust value will be updated again. This method has shown there is possibility to effectively detect the malicious vehicles by determining the threshold values efficiently.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

In farthest distance (FD) [12], a multi-step broadcast scheme has been presented for vehicular ad hoc networks in order to broadcast the warning messages. This method by considering the highway scenario is in attempt to reduce the delay and present a real model of dissemination environment for the vehicular ad hoc networks. In this method, relay node will be selected among the set of neighbors based on distance criterion, in such a way that the node that is farthest distance from the node sending the message will be selected as the relay node. By using this method, the number of steps will be reduced, however, considering the distance criterion alone, according to channel instability and a lot of obstacles and also the high speed of vehicles will cause more loss of packets that is not favorable for vehicular ad hoc networks and the delay sensitive applications.

III. THE BDSC ROUTING PROTOCOL

In BDSC protocol, a two-direction broadcast technique has been proposed in order to communicate as multi-steps in the vehicular ad hoc networks. This method uses receiving the beacon messages broadcasted by neighbors as the confirmation messages. Figure (1) shows the use of beacon messages as confirmation messages. In this method, a set of the sending among the neighbors as set of candidate will be selected to broadcast the received packet. A node with maximum calculated value will be selected as the relay node. In this method, the quality of link and the distance between sender and receiver have been used as the routing criterion and choosing the relay node.

By making a compromise between these two criteria, priority will be given to a node that, in addition to further distance, also has better bond quality. Moreover, this method uses a scheduling mechanism in order to rebroadcast the data packets in case of being defeated the relay node in sending the packet. Based on this waiting time, if the relay node is not able to send the data packet after special time period, other candidate nodes will be rebroadcasted the packet. However, this method has also presented its own criterion without taking into consideration to instability of the wireless channel and mobility of nodes. This method cannot be a proper solution for the vehicular ad hoc networks.

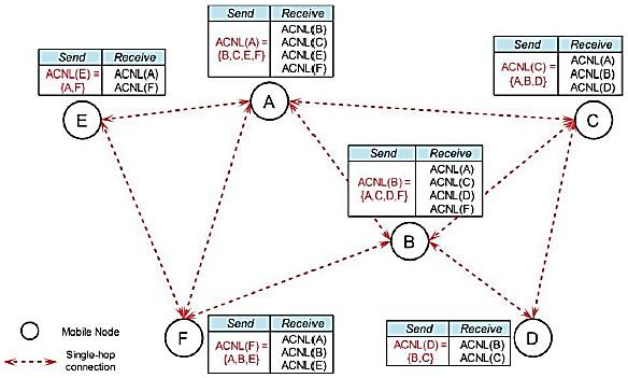

Figure 1: using the beacon messages as confirmation messages [13].

IV. PROPOSED METHOD

By investigating the prior methods, it can be concluded that broadcast routing protocol presented for vehicular ad hoc networks is without an efficient criterion in order to consider the reliability level and increase reliability in presence of rogue nodes. Most of the presented methods have used the quality criterion of data link or hearing and nodes contribution during the routing in order to allocate a reliability value to nodes. Also, most of the proposed methods have not considered their safety mechanism on a broadcast protocol that has more efficiency and challenges compared to other networks.

Considering the nodes participation and allocating a trust value to them may lead to the wrong recognition of nodes. On the other hand, most of the proposed methods have not considered the needs for routing and applications in vehicular ad hoc networks by focusing on safety mechanism that such issue will lead to reducing in network performance. Thus, there is a need for using a new mechanism in order to detect and identify the malicious nodes in network in addition to consider routing characteristics and existed applications in vehicular ad hoc networks. In this regard, in this research, by focusing on broadcast protocol presented in [13] and providing an efficient criterion in order to counter to presenting of malicious nodes in network, we try to increase reliability level of routing in vehicular ad hoc networks. The scheme includes three main steps that are:

1. Providing a criterion based on quality of link, Euclidean distance and the difference of Euclidean distance with distance obtained from the received signal power in order to investigate the legitimacy of nodes in network.

2. The mechanism of selecting the relay nodes based on the proposed criterion.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

Figure (2) shows the flowchart of proposed method.

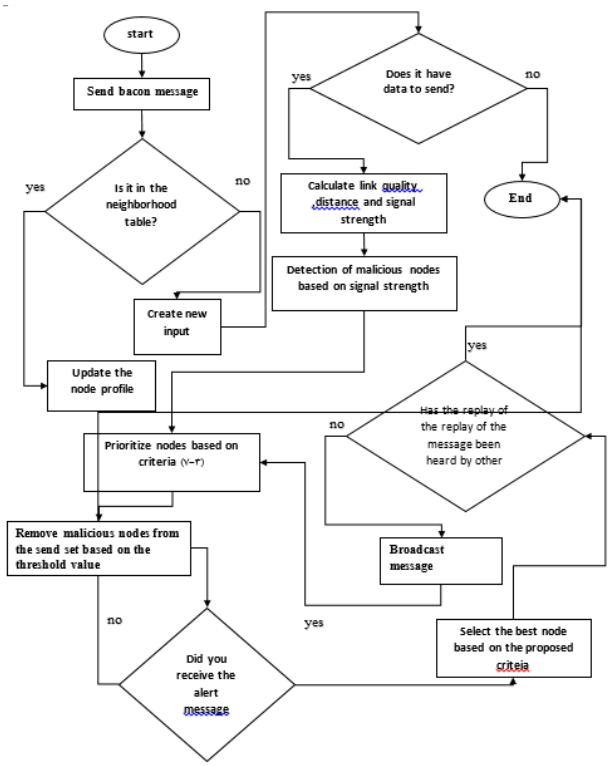

Figure 2: flowchart of the proposed method

First, the nodes will hold local data from their neighbor nodes by using the exchange of beacon messages. These messages are periodically sent as for the high mobility speed of nodes. If the receiver node does not have input for the sender node, it creates a new input and locates specifications like speed, direction, and situation in the input. In next step, if the node has a message for sending, it will calculate the criteria of the link quality, signal strength and the distance based on the criteria explained in the previous section. After that, in order to detect malicious nodes, the strength of signal obtained from the beacon messages is compared to the real strength of signal. If the difference between these two values is greater, then the node will be detected as a malicious node.

To this end, it will not be considered as the relay node. After determining the malicious nodes in network, remain nodes will be prioritized based on the proposed criterion and the node with the greatest value will be selected as the relay node. Other nodes with the lower priority will only rebroadcast the packet if the node with high priority fails to send data messages. If the low priority nodes hear the data broadcast by the high priority nodes, the scheduling on the data message will be canceled and the packet will be eliminated from their buffer. This mechanism will be repeated for each data message sent in network.

V. Evaluation Criterion

To evaluate the performance of proposed method, a multi-directional scenario has been considered. The length of the roads is considered equal to 15000 meters and the transition radius of each vehicle is considered 450 meters. The sending rate of beacon messages in the proposed method and other methods is equal to one packet per second. The size of the messages has been considered 512 bytes. These messages will announce an emergency situation in the network. The range for sending messages is one packet per second. The TwoRayGround propagation model in network is considered with capability to create the inter-vehicular connection. In simulation scheme, in order to present the results closed to the real world, we have supposed the access layer to medium is not reliable and the noise, distortion and signal attenuation in environment affect the behavior of network layer. The access layer to the medium is based on ETSI standard, IEEE 802.11p standard that has ability to support communications without infrastructure in vehicular environment. The simulation time has been also considered 60 seconds. The nodes mobility model in order to distribute the nodes randomly and by using the Manhattan mobility model is obtained, the initial situation of which is random and then the nodes are moving with a movement limited to roads and streets with a minimum speed of 60 kilometers per hour and a maximum speed of 120Km/hour.

VI. Simulation Results

According to the multi-step feature of the wireless networks, it is necessary that packets are sent through middle nodes from the source to destinations that are in out of range of theirs own sending. On the other hand, increasing the number of steps increases the delay. Also, the presence of nodes that incorrect data in the network using the beacon messages broadcasted causes the packet to dropped. The increase in the number of attacker nodes causes to reduce the list of selected sending set and the success probability of packet reduce in packet delivery. Figure (3) shows the average end-to-end delay for different percentage of malicious nodes.

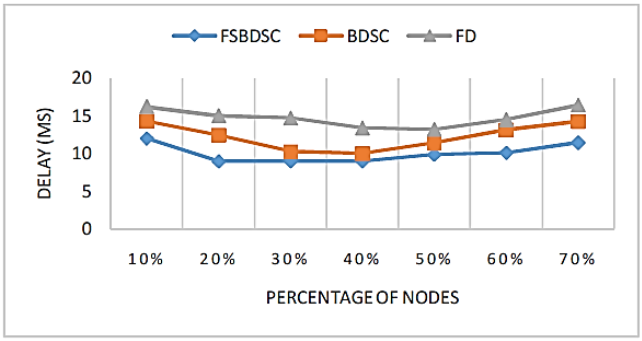

Figure (3): average end-to-end delay for different percentage of malicious nodes.

Figure (3) shows the delay in proposed method has a less value. The reason for this issue is to consider criteria consistent with the specifications of vehicular ad hoc networks such as packet advance, quality of link, connection life time, and the signal strength of nodes as a criterion that can detect the malicious nodes in network. In this way that nodes with greater signal strength have the less probability in packet loss. For this reason, the selected paths have better power during the data rebroadcast.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

By increasing percentage of nodes in the network, the number of steps will increase during the routing. In the proposed method, there is possibility to detect the malicious nodes by calculating the received signal strength and obtaining the difference distance between sender nodes and receiver nodes. The proposed method has caused the 28% and 19% improvement compared to FD and BDSC methods. In figure (4), throughput has been shown for the number of percentage of malicious nodes.

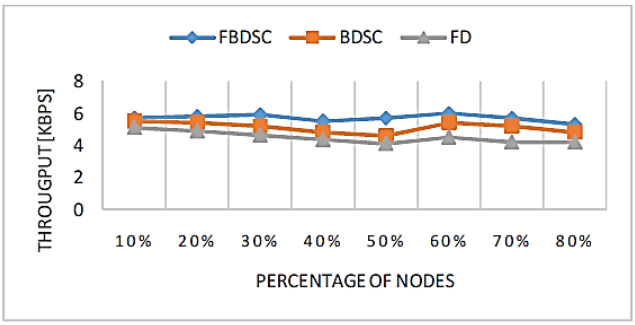

Figure (4): throughput for number of percentage of malicious nodes.

According to figure (4), the proposed method will cause the presentation of better results due to selecting the links with proper transition quality by considering the paths with more signal strength and better transmission quality. As a result of this issue, more flows of data will pass through the selected link that will lead to increasing the throughput of system. On the other hand, this will decrease the number of relay nodes by considering nodes in the network that will send their own situation wrongly. To this end, by considering the recognition criterion of such nodes in the network, it led to the increase in characteristics of network such as throughput, because candidate nodes will be chosen so that they do not locate in the classification of malicious nodes in the network. The proposed method has been improved by an average of 17% and 8% compared to FD and BDSC methods.
Figure (5) shows the delivery rate for different percentage of malicious nodes.

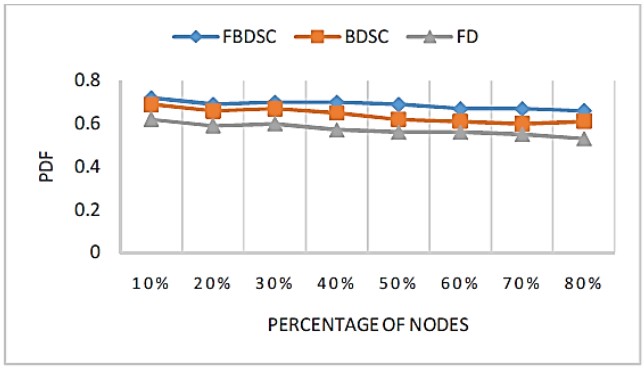

Figure (5): the delivery rate for different percentage of malicious nodes

The delivery rate has been reduced for all routing protocols. The reason for this is to increase the probability of choosing these nodes as data relay. Given that malicious nodes will eliminate data packets if they receive data message and are chosen as the relay node, it is obvious that delivery rate will be reduced by increasing percentage of the malicious nodes presence. This is true for each three routing methods. However, the proposed method leads to presenting the better performance by considering the effect of presence of malicious nodes during routing. Given that in proposed method, if the difference between the strength of real signal and strength of signal obtained from the beacon messages is greater that a threshold value, the node will be removed from the sending set, the proposed method reduces the effect of malicious nodes on performance of the network and especially the delivery rate. Thus, the delivery rate of proposed method has been improved 14% and 7% compared to FD and BDSC methods.
Figure (5) shows the loss rate for different percentage of malicious nodes.

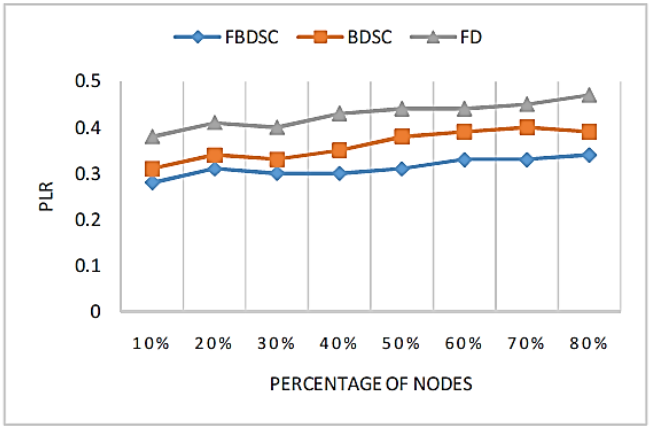

Figure (5): loss rate for different percentage of malicious nodes

In figure (5), the loss rate has been increased for all three routing methods. The reason for this is to increase the presence of malicious nodes in the network that leads to the loss of more packets. Therefore, considering a mechanism in order to counter to the effect of malicious nodes can lead to reducing the loss rate and improving the performance of network. Thus, improving the performance (reducing the loss rate) leads to increase in delivery rate. In the proposed method, an attempt has been made this effect reaches the minimum of its value among the presented methods by focusing on detecting the malicious nodes by considering the signal strength. In this regard, the loss rate in the proposed method has been reduced more than other methods. On the other hand, the proposed method causes the selection of paths with more life time and in result of which, increase in network performance in terms of the loss rate of packets by considering an efficient criterion that other methods do not take into account it, namely the signal strength. The proposed method has been improved 12% and 26% compared to FD and BDSC methods.

VII. Conclusion and Upcoming Works

In this paper, the results obtained from conducted simulations have shown that proposed method has better performance from the delivery rate, end to end delay rate, throughput, and loss rate in different methods. The main reason is to consider the effect of malicious nodes presence and present a mechanism in order to counter to it. According to the obtained results, a new combinational criterion has

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173

improved the performance of network and has increased the reliability of system by considering the effect of malicious nodes presence. In upcoming researches, it can be investigated the limited bandwidth of nodes and the competition for holding the channel that it is necessary the shared bandwidth has been considered as an important issue in vehicular ad hoc networks. In this regard, the new routing criteria can be used during the selection of relay nodes. On the other hand, in order to use optimally from the network resources such as bandwidth, the control beacon messages that are periodically sent in constant times can be reduced without reducing in the performance of network. Reducing beacon messages in addition to reducing overload and using less bandwidth can improve the characteristics of vehicular ad hoc networks like delay and delivery rate.

REFERENCES

[1] [1] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection" IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6703-6710, 2016.

[2] [2] H. Hasrouny, C. Bassil, A.E. Samhat, A. Laouiti, "Group-based authentication in V2V communications, in: DICTAP", pp. 173-177, 2015.

[3] [3] K. Lim, D. Manivannan, "An efficient protocol for authenticated and secure mes-sage delivery in vehicular ad hoc networks", vol. 4, pp. 30-37, 2016.

[4] [4] A. M. E. Ejmaa, S. Subramaniam, Z. A. Zukarnain, and Z. M. Hanapi, "Neighbor-based dynamic connectivity factor routing protocol for mobile ad hoc network" , pp. 8053-8064, 2016.

[5] [5] X. Feng, C. Li, D. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET" Peer-to-Peer Networking and Applications, vol. 10, no. 2, pp. 305-314, 2017.

[6] [6]. C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs" Vehicular Communications, pp. 643-651, 2016.

[7] [7]. X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs" Ad Hoc Networks, vol. 55, pp. 107-118, 2017.

[8] [8]. O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks" Expert Systems with Applications, vol. 50, pp. 40-54, 2016.

[9] [9]. C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS" Computer Communications, vol. 93 pp. 68-83, 2018.

[10] [10]. Gh. Samara, W.A.H. Al-Salihy, R. Sures, "Security analysis of vehicular ad hoc networks (VANET)", pp. 55-60, 2018.

[11] [11]. V. La Hoa, A. Cavalli, "Security attacks and solutions in vehicular ad hoc net-works", vol.4, no.2, pp.1-6, 2017.

[12] [12]. W. Ben Jaballah, M. Conti, M. Mosbah, C.E. Palazzi," Fast and secure multi hop broadcast solutions for intervehicular communication", vol. 15 (2), pp. 433-450, 2014.

[13] [13]. R. Osama and O-Khaoua, and B. Hadj, "An adaptive relay nodes selection scheme for multi-hop broadcast in VANETs", vol. 87, pp. 76-90, 2018.

IEEE Office - SEET Complex, Federal University of Technology, Owerri, Nigeria, https://aeuso.org
EISSN: 2305-0543, PISSN: 2411-6173