EAI Endorsed Transactions
on Mobile Communications and Applications
Research Article EAI.EU

Performance Analysis of RACODSR Protocol in Smart Grayhole Attacks on VANets

Kaoutar Ourouss*, Najib Naja and Abdellah Jamali

National Institute of Posts and Telecommunications, Rabat, National School of Applied Sciences, Berrchid, Morocco

Abstract

As a subclass of Mobile Adhoc Networks (MANets), Vehicular Ad Hoc Network (VANET) is a set of interconnecting vehicles that aim to provide a wide spectrum of encouraging road services, such as safety and traffic management. This key component of Intelligent Transportation Systems (ITS), is impacted by the vehicle's mobility and suffers from frequent link disruptions caused voluntarily or intentionally by malicious attackers, which make the security issue more challenging and even life-threatening when critical attacks occurred. This work focuses on analyzing the smart grayhole attacks within VANets environments and evaluating the Reputation-based Ant Colony Optimization Dynamic Source Routing (RACODSR) and Dynamic Source Routing (DSR) protocols performances under two different scenarios. For this purpose, VANets mobility models with and without collisions are generated using OpenStreetMap and Simulation of Urban Mobility (SUMO) tools and simulated in Network Simulator NS2 to assess the effectiveness of the compared protocols using the Drop rate, Packet Delivery Ratio, Throughput, Jitter, End-to-End delay, and consumed energy metrics.

Received on 06 April 2022; accepted on 30 May 2022; published on 01 June 2022

Keywords: Mobile ad hoc networks, Vehicular networks, DDoS Attacks, Reputation System, Trust Management, ACO

doi:10.4108/eai.1-6-2022.174088

1. Introduction

With the continuous researchers working in the communication and networking field, the new VANet networks, enabling communication between vehicles, came to exist. Indeed a vehicular network is considered as a particular kind of MANet, but with a little difference, is that vehicles within VANET move in an organized fashion, not as mobile nodes in MANets who move randomly, and their mobility patterns are constrained in streets. They communicate with each other using technologies namely, IEEE802.11p, Wireless Access in Vehicular Environments (WAVE), and Dedicated Short Range Communication (DSRC) standards [1], and this under two different fashions, Vehicle to Vehicle architecture (V2V) or Vehicle to Infrastructure one (V2I) with Road-side-Units (RSU) and cellular Base Stations (BTs). As a sub-branch of MANets, VANets are the Key components of Intelligent Transportation Systems (ITS) [2], that can improve road safety and offer a multitude of services that meet the needs and challenges of smart cities. VANets are characterized by their openness and the very high dynamism related to the vehicle's mobility, which results in frequent link disruption. In addition, vehicles within VANets, as MANets, should be self-organized without the need for any previously deployed administration, which increases the exposure to wide security threats [3] that impact adversely the safety and security of the road users [4]. All these characteristics and mobility support result in nontrivial challenges [5] that make the VANets a very interesting research field in industry and academia.

1.1. Smart grayhole attacks

Security vulnerabilities related to the nature of wireless environments are exploited by malicious nodes to carry out various types of routing attacks [3] that damaging the network functioning especially packet dropping attacks and particularly smart grayhole attacks. Smart grayhole attack is categorized as a denial service attack that violate the traffic routing by reducing the throuput

*Corresponding author. Email: ourouss@inpt.ac.ma

and maximazing the end to end delay [6]. In this harmful attack, the malicious node behaves genuinely at the discovery phase to ensure its presence among the selected nodes to form the path that the packet will be transmitted on, afterwards, when a data packet passes through this node, it exibits its malicious intent and drops it. It should be noted that these attackers behave unpredictably and silently which make their malicious actions hardly detectable.

1.2. Ant Colony Optimization Metaheuristic

Genetic algorithms, Ant Colony, Memetic algorithms, Tabu search, simulated annealing are considered as a high level algorithmic strategies that are used to solve any kind of NP-hard problems in engineering through optimizations named metaheuristics. the Ant Colony Optimization [7] as one of these successful solution dedicated to solve the combinatorial optimization problems, is based on forging behavior of ant species when each one deposits an amount of volatile chemical pheromone on the traversed path to reflect its preference. This behavior was adopted to many routing protocols [8] due to its adaptation to topological changes and its self maintenance, the RACODSR is one of the multiple routing protocols that are based on this metaheuristic to enhance the security aspect of source routing as explained in the next paragraph.

1.3. the Reputation-based Ant Colony Optimization Dynamic Source Routing (RACODSR) for VANets

The RACODSR [9] proposes a new secure variant of DSR protocol based on a trust evaluation system to identify and defeat smart grayhole attacks. The proposed mechanism combines two interacting subsystems to monitor the node's behavior and investigate their malicious intents. The first subsystem consists of a trust management scheme with a measurement functionality model relied on the beta reputation distribution to assign a reputatio value to each node. While, the second subsystem admits the ACO metaheuristic to rate the nodes according to their efficient participation in routing tasks. Based on the trust information obtained jointly from the statistical and the metaheuristic models, the optimal path with less maliciousness rate is selected. the table below compares the RACODSR and the DSR protocols in terms of come routing features:

Table 1. Comparision of RACODSR and DSR

Routing Features	RACODSR	DSR
Routing Structure	Flat	Flat
Security defense against DDoS Attacks	No	Yes, with a trust management system
Periodic Updation	Not required	Not required
Control Overhead	Medium	Low
Route Creation	By Source	By Source
Route Selection criterion	Short Path	Short Path with Genuine Nodes

This paper investigates the impact of grayhole attacks on VANets environments and qualify the efficiency of the proposed RACODSR protocolon the V2V communications. For this purpose, the next sections discuss the security issues on VANets, detail the simulation scenarios, and analyze the obtained results.

2. Implementation of RACODSR on VANets scenarios : Motivation

Obviously, VANETs rely on wireless communications so most of the issues encountered in MANets will have to be faced in VANets too. In VANets, security has a major impact on road users safety and even can be life-threatening especially when critical messages are circulated between vehicles, such as Emergency brake, Speed breaker ahead, Accident happens on the road, Traffic jam ahead, Bad weather, etc [10], and thus, hamper the performance of networks. In this context, a huge interest has been paid to pledge the security measurements in VANets through multi detection systems and security schemes in order to avoid the malicious nodes from communicating with other vehicles. VANET, as a component of the ITS, evolved progressively in smart trendy countries to offer a wide spectrum of encouraging ITS applications and thereby alleviate many of the current transport complications, nevertheless, this effective technology in communication between mobile nodes and infrastructure, suffer from various security issues as well as MANets. In the purpose of overcoming these weaknesses and drawback, multiple papers proposed different schemes and architectures to secure VANets, such as cryptography, hash functions, and digital signatures and addressed the denial of service and replay attacks [11] [12] [13] [14], and [15].

VANets are prone to many different types of attacks [16], and especially the active DoS attacks such as the grayhole ones. In this kind of attack, malicious vehicles drop the messages and interrupt the functioning of the networks, which may interrupt the spreading of alerting messages around the network, regarding warnings and dangerous situations/conditions, and consequently lead to high damages. In this vision, this chapter is dedicated to investigating the impact of smart grayhole attacks on VANets networks and that under two different real scenarios, in the first one, the communication between vehicles takes place without any interruption, while in the second scenario, multiple car collisions occur and disrupt the vehicle's communication. Moreover, the simulations are conducted with the proposed RACODSR protocol to qualify its effectiveness in this emerging high mobile wireless network. For this purpose, the next section describes the simulation methodology and analyze the obtained results.

3. Scenario 1: V2V communications without car crash

The first scenario simulates a smart grayhole attack within a VANet network with a realistic mobility model when vehicles move correctly without any collision. This kind of mobility model is used in the deployment of warnings services for several applications such as traffic management on motorways and emergency services. Hence the importance of simulating this V2V architecture with smooth traffic flow but under smart grayhole attack.

3.1. Simulation environment settings

This work aims to evaluate the effectiveness of RACODSR according to a VANet scenario with a realistic mobility model, for this purpose, the OpenStreetMap [17] framework is used to extract manually and microscopically the traffic map for a real scenario. In this simulation, the road traffic in Kathipara Junction in Chennai, India. at the intersection of the Grand Southern Trunk Road, Inner Ring Road, Anna Salai and Mount-Poonamallee Road. 1 is chosen and exported in .osm format file to be used as a mobility model for the conducted simulations.

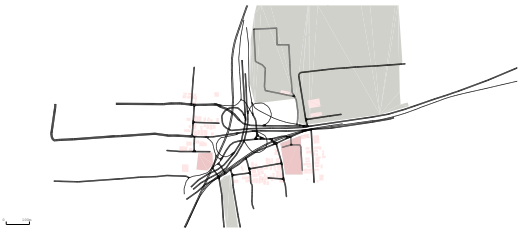


Figure 1. View of Kathipara Junction in Chennai, India, in SUMO

This osm map is next edited by the Simulation of Urban MObility (SUMO) tool [18] to generate the relevant network map configuration as well as the mobility traffic pattern of vehicles 2 that will be used in the NS2 simulator as an input.

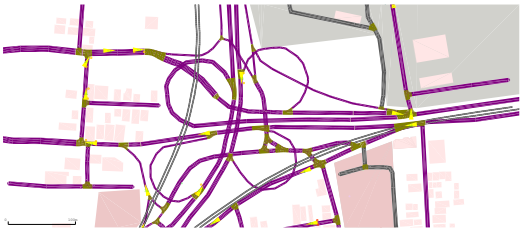


Figure 2. SUMO road infrastructure map of Kathipara Junction in Chennai, India.

The conversion of this osm file to tcl file is ensured by the TraceExporter tool executed by the python language, the obtained vehicles trace files provide road maps, the number of traveling vehicles, their maximum speed, and departure and arrival times with the corresponding trips. These files are therefore injected into the NS2 script. The next flow chart 3 resumes the followed steps to generate the tcl file that will be simulated by the NS2 simulator.

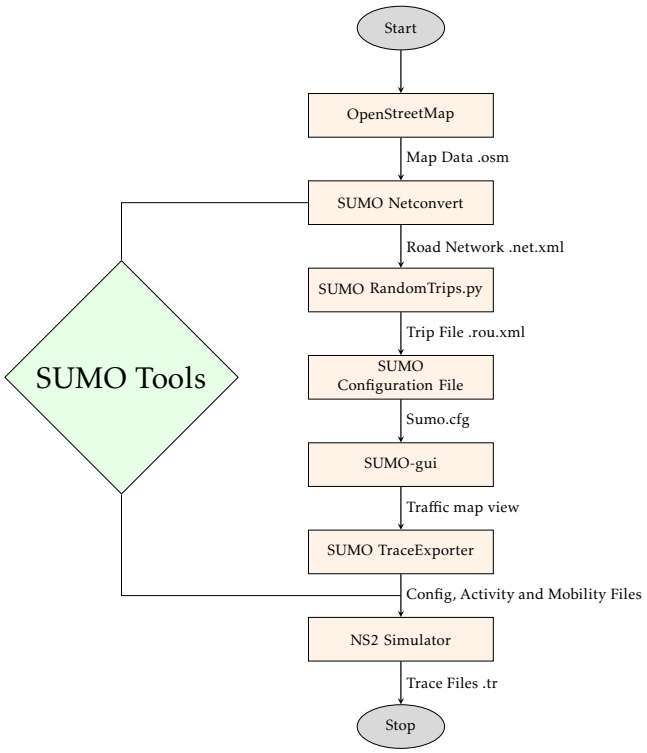


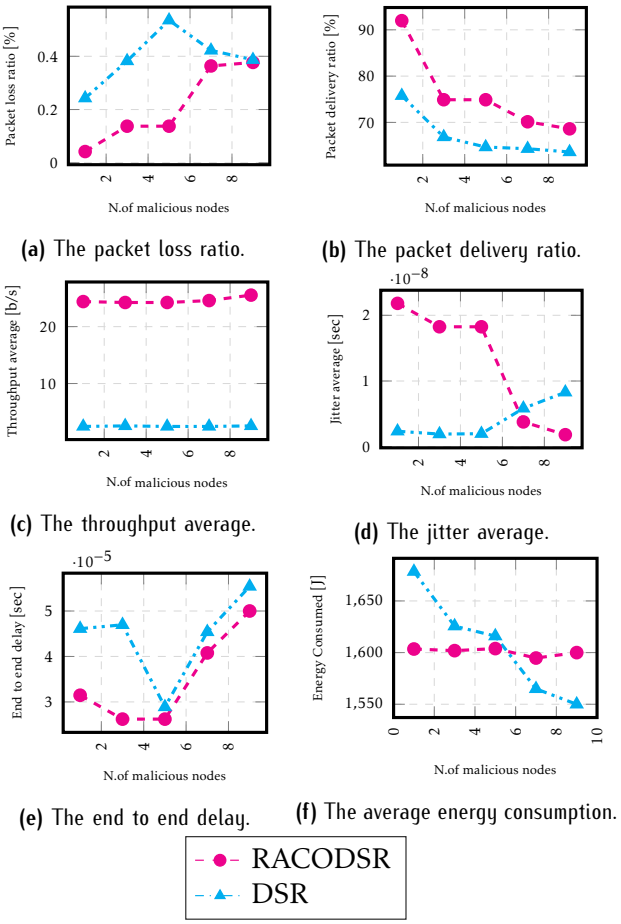
Figure 3. Simulation Process using OpenStreetMap, SUMO, and NS2 for Scenario 1

The simulations are conducted using the collected flow data for around sixteen mins with 35 vehicles including those malicious cars that are responsible for launching grayhole attacks. The scenario aims to introduce periodically malicious vehicles and repeat the simulations ten times to increase the accuracy of the obtained results. The parameters setting of the conducted simulations are listed in the table below:

Table 2. VANets Simulation parameters

Vehicles Number	35
Network Map	Kathipara Junction, India
Traffic Type	CBR
Duration	960 Secs
Maximum connections	8
Topography Dimensions	$2825 * 1940 m^2$
The power consumed in transmission state Tx	0.33 Watt
The power consumed in reception state Rx	0.1 Watt
The power consumed in idle state	0.05 Watt
The power consumed in the sleep state	0.03 Watt
Initial energy	1000 Joule
Transition power	0.2 Secs
Transition time	0.005 Secs

3.2. Results Analysis



(a) The packet loss ratio.
(b) The packet delivery ratio.
(c) The throughput average.
(d) The jitter average.
(e) The end to end delay.
(f) The average energy consumption.

Figure 4. The QoS evaluation in different VANets maliciousness rate scenarios

This section analyzes the results obtained from conducted simulations in order to evaluate the routing performance of RACODSR and DSR protocols [19] under grayhole attacks within VANets scenarios. In this context, the maliciousness rate was varied between 2%, 8%, 14%, 20%, and 25%, and the Drop rate, PDR, Throughput, Jitter, End-to-End delay, and consumed energy metrics are used too. As can be shown in figure 4a, the RACODSR is more resistant in terms of lost packets even when the number of attackers gets higher, and guarantees a good amount of delivered packet which is demonstrated by the results in 4b with amelioration of 10% than standard DSR. These results are proved also again with the high amount of throughput portrayed in figure 4c. in terms of time processing, figures 4d 4e highlight the variation in packets delay between RACODSR and DSR which gets higher with the presence of malicious vehicles which is explained by time processing in eliminating those vehicles from participation in data transmission according to RACODSR, and by the delay related to packets regeneration in the context of DSR. The last figure 4f shows the performance of RACODSR in terms of the average of consumed energy which remains stable with the presence of intruders, unlike DSR, when more energy is consumed to ensure the retransmission of the high number of dropped packets as shown in figure 4a.

4. Scenario 2: V2V communications with car crash

Vehicles crash is an important factor in the mobility model of VANets [20], it impacts the reaction time and action of the surrounding cars. Indeed, when an accident happens, the vehicles around the crash point stop or change their destination, furthermore, the emergency messages are sent from crashed cars to inform other road users which influence directly the network performances [21]. Based on these facts, in the second scenario, the simulations are conducted in VANet networks where multiple collisions occur between vehicles to extract useful information regarding the RACODSR routing protocol and its effectiveness against smart grayhole attack within this typic environment.

4.1. Simulation environment settings

As it was produced in the first scenario, a network map is extracted from the OpenStreetMap [17] framework and this time for the intersection Zizhuyuan Road, Zizhu Garden, Haidian District, Pékin, 100048, Chine 5. following the steps mentioned in the previous flow chart 3, the SUMO [18] is used to convert the network map into a mobility model trace file.

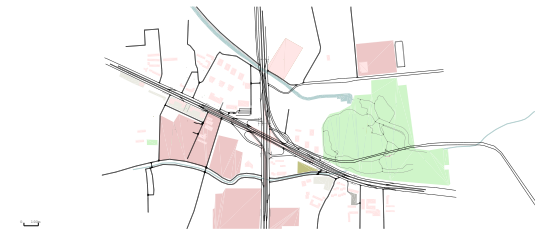


Figure 5. View of Zizhuyuan Road, Pékin, Chine, in SUMO

In fact, the default mobility model generated by SUMO aims to be car accident-free, hence, the need for collision creation manually. For this purpose, the route file .rou.xml that was extracted through randomTrips.py can be manipulated using the Mingap parameter that SUMO uses to detect a collision, indeed, when the gap between two vehicles is below the predefined value of each vehicle, a collision is registered.

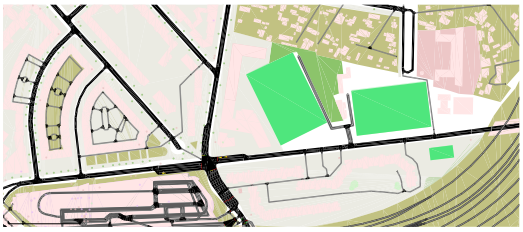


Figure 6. SUMO road infrastructure map with collisions of Zizhuyuan Road, Pékin, Chine.

The collision model adopted aims to define the Mingap parameter value for vehicles that will have a crash and force them to halt for some time. To achieve this goal, the behavior of vehicles can be modified in the .rou.xml file by setting the Mingap parameter to '0' in the <vType/> tag and forcing their stop in a specific lane for a specific time using the <stop/> tag. After setting the pre-collision parameter, the consequence of those collisions can be also modeled using the option –collision.action when in the case of the conducted simulation the attribute Warn was used to send warning messages to other vehicles 6. The next flow chart resumes the followed steps to generate a VANets mobility model with collisions.

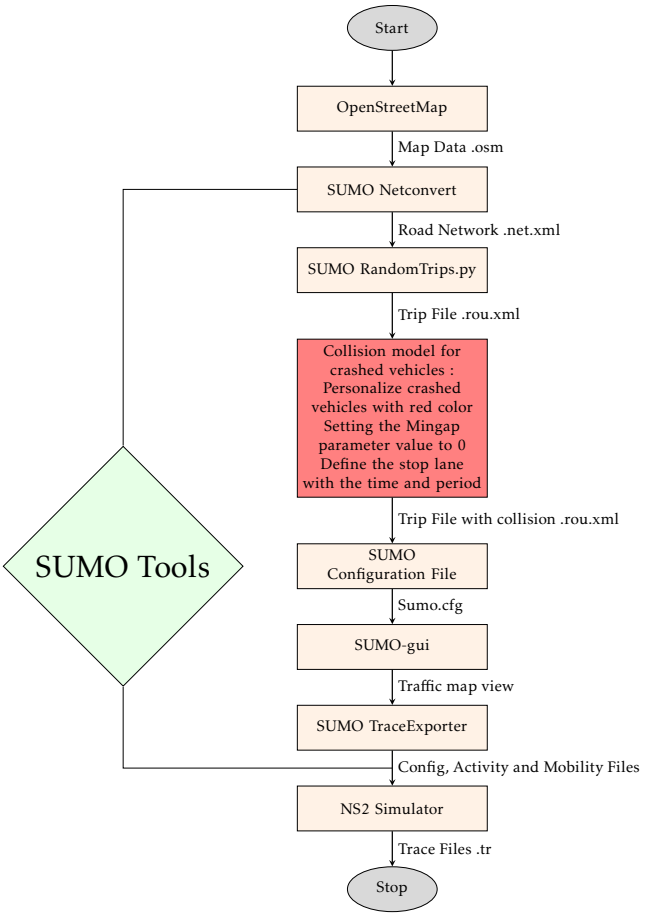


Figure 7. Simulation Process with Collision model using OpenStreetMap, SUMO, and NS2 for Scenario 2

After generating the mobility model with collision, the trace files are injected into NS2 simulator with the parameters setting listed in the table below.

Table 3. VANets with Collision Simulation parameters

Collisions Number	11
Crached vehicles	6
Crashed Vehicles stopping time	10 sec
Collision action	Warn
Collision Mingap factor	2
Vehicles Number	26
Network Map	Zizhu Garden, Pékin, Chine
Traffic Type	CBR
Duration	10000 Secs
Topography Dimensions	$16440 * 3533m^2$
The power consumed in transmission state Tx	0.33 Watt
The power consumed in reception state Rx	0.1 Watt
The power consumed in idle state	0.05 Watt
The power consumed in the sleep state	0.03 Watt
Initial energy	1000 Joule

4.2. Results Analysis

The conducted simulations with the scenario detailed in the previous section provide the results portrayed in figure 8 below. Clearly, the collision number influence directly the loss packet ratio which is 10 times higher in VANets with collision scenario than in scenario 1 as shown in figure 5, and it gets higher with the number of malicious vehicles, but the proposed RACODSR guarantees less amount of dropped packets. This statement is approved with the graph in figure 6 when the packet delivery ratio remains higher with the bio-inspired protocol than the DSR one, however, it must be noted that the 11 collisions that occurred during the simulations have decreased the packet delivery ratio because the 6 crashed vehicles had to stop which interrupt the transmission of the packets, which is also demonstrated by the throughput values presented in figure 8a. In terms of time processing figures, 8b and 8c show the graphs respectively of jitter and end-to-end delay when it is clear that when malicious vehicle number gets higher the processing time increases too for DSR, unlike the RACODSR when the trust model is applied to avoid dropping nodes from communication and thereby ensure less number of retransmissions. In terms of consumed energy, figure 8d shows that both DSR and RACODSR consume less energy compared to VANets scenario without collisions in figure 4d, which is related to the stopping period of crashed vehicles when they are suspended from communication participation.

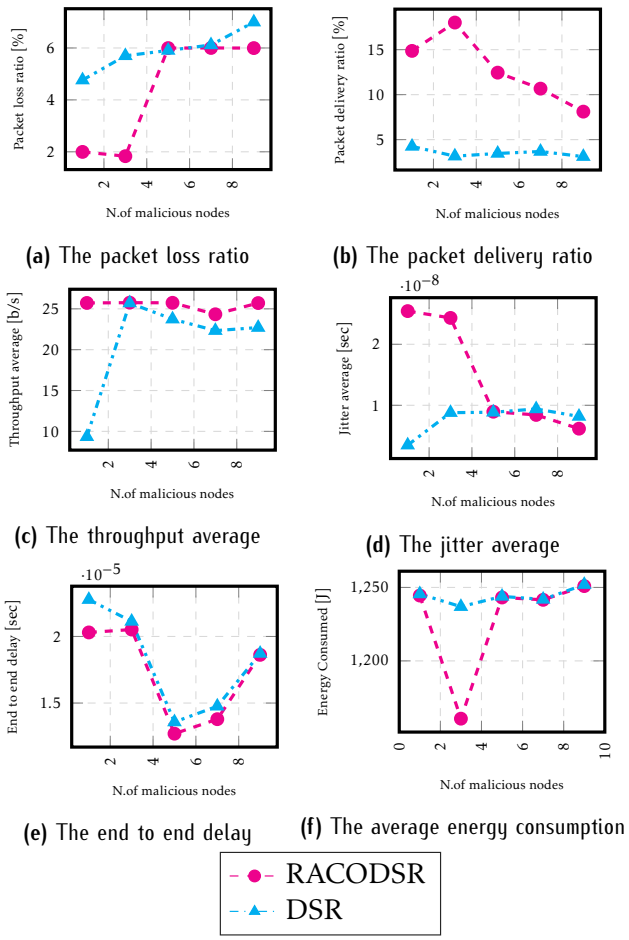


Figure 8: The QoS evaluation in different VANets maliciousness rate scenarios with collisions

Conclusion

The main focus of this paper is to evaluate the efficiency of the proposed source routing protocol RACODSR with a VANet scenario. This emerging high mobile wireless network is considered as a sub-branch of MANets but with an organized mobility model and with two different architectures V2V and V2I. Based on these facts, and with the emerging challenges of smart cities when everything is connected anywhere and anytime, it proved necessary to examine VANets in-depth and especially in terms of security since this kind of networks are responsible for road safety and any misuse or interruption in its functioning may lead to life-threatening. In this vision, two different scenarios were simulated using realistic V2V network maps with a smart grayhole attack. The first scenario evaluates the performance of RACODSR and DSR protocols with mobility model without collision, it was witnessed that the RACODSR outperforms the standard DSR even in VANet environment in terms of QoS performance metrics and also the energy consumption. In the second scenario, a collision model was added to the mobility model of a realistic VANet map in order to assess the collision factor on the performance of the RACODSR and DSR, obviously, the amount of data packet was reduced due to the suspension of crashed vehicles which affected the QoS metrics but once again the RACODSR shows its outperformance over DSR in VANets environments.

References

[1] Singh, A. and Singh, B. (2020), A study of the ieee802.11p (wave) and lte-v2v technologies for vehicular communication. doi:10.1109/ICCAKM46823.2020.9051468.

[2] Zhang, J., Wang, F., Wang, K., Lin, W., Xu, X. and Chen, C. (2011), Data-driven intelligent transportation systems: A survey. doi:10.1109/TITS.2011.2158001.

[3] Sumra, I., Sellappan, P., Abdullah, A. and Ali, A. (2018) Security issues and challenges in manet-vanet-fanet: A survey. *EAI Endorsed Transactions on Energy Web* **5**(17).

[4] Dhamgaye, A. and Chavhan, N. (2013) Survey on security challenges in vanet 1 .

[5] AK Azameti, A., A Katsriku, F., Chong, P. and D Abdulai, J. (2018) The effect of congestion control model on congested traffic flow in vehicular ad hoc networks (vanets). *EAI Endorsed Transactions on Mobile Communications and Applications* **3**(10).

[6] Ur Rehman, M., Ahmed, S., Ullah Khan, S., Begum, S. and Ahmed, S.H. (2018) Performance and execution evaluation of vanets routing protocols in different scenarios. *EAI Endorsed Transactions on Energy Web* **5**(17).

[7] Fendji, J.L.E.K., Yakam, M. and Fendji, M.D. (2020) Ant colony-based tabu list optimization for minimizing the number of vehicles in vehicle routing problem with time window constraints. *EAI Endorsed Transactions on Context-aware Systems and Applications* **7**(21): 166041.

[8] Prakash, J., Sengottaiyan, N. and Nandhini, S.H. (2018) Smart routing for vehicle at optimal position with ant colony optimization and aqrv in vanet. *EAI Endorsed Transactions on Energy Web* **5**(20): 155566.

[9] Ourouss, K., Naja, N. and Jamali, A. (2021), Defending against smart grayhole attack within manets: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol. doi:10.1007/s11277-020-07711-6, URL https://doi.org/10.1007/s11277-020-07711-6.

[10] Raya, M. and Hubaux, J.P. (2007), Securing vehicular ad hoc networks.

[11] Elsadig, M.A. and Fadlalla, Y.A. (2016), Vanets security issues and challenges: A survey.

[12] Al Hasan, A.S., Hossain, M.S. and Atiquzzaman, M. (2016), Security threats in vehicular ad hoc networks.

[13] Haas, J.J., Hu, Y.C. and Laberteaux, K.P. (2009), Real-world vanet security protocol performance.

[14] Kaur, R., Singh, T.P. and Khajuria, V. (2018), Security issues in vehicular ad-hoc network (vanet).

[15] Samara, G. and Al-Raba'nah, Y. (2017), Security issues in vehicular ad hoc networks (vanet): a survey.

[16] Godse, S. and Mahalle, P. (2017), Secure & efficient routing mechanisms in vanet using cbds.

[17] Mooney, P., Minghini, M. *et al.* (2017), A review of openstreetmap data.

[18] Krajzewicz, D., Erdmann, J., Behrisch, M. and Bieker, L. (2012), Recent development and applications of sumo-simulation of urban mobility.

[19] Johnson, D.B., Maltz, D.A., Broch, J. *et al.* (2001) Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking* **5**(1): 139–172.

[20] AK Azameti, A., A Katsriku, F., Chong, P. and D Abdulai, J. (2018) The effect of congestion control model on congested traffic flow in vehicular ad hoc networks (vanets). *EAI Endorsed Transactions on Mobile Communications and Applications* **3**(10).

[21] Santamaria, A.F., Tropea, M., Fazio, P. and De Rango, F. (2018), Managing emergency situations in vanet through heterogeneous technologies cooperation.