# Geographical Routing Protocols in VANets: Performance and Security Analysis

Messaoud Benguenane[1,*], Ahmed Korichi[1], Nadjet Azzaoui[1],
[1] *Department of Computer Science and Information Technology, Kasdi Merbah University, Ouargla, Algeria*
*{azzaoui.nadjet,ahmed.korichi,messaoud.benguenane}@univ-ouargla.dz*

**ABSTRACT**
Vehicular ad hoc networks (VANETs) enable communication between automobiles and communication equipment positioned along the street to provide road safety and convenience applications. Security is a must for all of these applications. Due to its highly dynamic architecture and frequent connectivity breakdowns, security is a significant challenge in automobile ad-hoc networks. Due to the open nature of wireless communication, the attacker can overhear and change the messages broadcast by another node. We explored security vulnerabilities against VANETs spatial routing protocols in this article. Then, we suggested a novel security solution based on an Intrusion Detection System Algorithm that would provide adequate protection against black holes and jellyfish attacks.

***Keywords:*** *Vehicular Ad Hoc Networks, Routing protocol, Security, Intrusion Detection System.*

## 1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are a subset of Mobile Ad Hoc Networks (MANETs) that serve as the backbone of an Intelligent Transportation System (ITS) with the primary objective of increasing road safety [1]. Vehicle communication in Vanet networks enables drivers to receive potential danger warnings as soon as possible using sensors deployed in vehicles or at the edges of roadways and control centers [2]. Additionally, these networks enable the provision of new services to road users, enhancing the comfort of road travel [3]. Further, due to the increased mobility of vehicles, Geographical routing protocols outperform standard ad hoc routing protocols in Vanet due to their significant route finding and maintenance overheads [4,5]. Geographic (or position-based) routing methods locate a path to a destination by utilizing the geographic coordinates provided by a positioning system (GPS) [6]. Routing tables provide the geographic coordinates of nodes [7]. Specifically, a node includes the destination's identity and position in the packet to be transmitted. Then the intermediate nodes retransmit the packet and continue the process until it reaches the destination using the geographic information included in the packet and those available in their routing tables [8]. Rather than relying on route tables or route storage, it uses the location information of adjacent and destination nodes to calculate the next transmission hop, which is the closest neighbor to the destination [5].

On the other hand, security is a significant concern in these networks due to their open environment, changeable topology, lack of central management, distributed collaboration, and limited capacity. Indeed, rogue nodes may intercept, alter, or erase communication messages, resulting in accidents and putting people's lives in jeopardy [9]. However, before establishing these networks, suitable security measures must be built to avoid these unwanted situations and identify the entities responsible for these harmful acts [10]. Thus, the primary goal of secured routing protocols is to ensure that any data packet provided is delivered from the source to the intended destination without being intercepted, tampered with, or dropped [11].

To provide an overview of secure routing protocols, we have analyzed several geographical routing protocols in this study (secured and insecure protocols). Then, we proposed IDIS4JB (Intrusion Detection and Isolation System for Jellyfish and Black Hole), a novel security approach based on the Intrusion Detection System Algorithm, to resist data traffic assault nodes that delay or delete forwarding packets going through them by identifying and isolating Black Hole and Jellyfish nodes.

The remainder of this essay is organized in the following manner. Section 2 discusses geographical routing techniques and the various security solutions researchers have working on VANETs network security. Section 3 details our security model. Section 4 discusses how to evaluate performance and how to compare. Section 5 finishes the study and summarizes the obtained results.

## 2. RELATED WORKS AND CONTRIBUTIONS

This section summarizes many experiments on automotive networks that have been undertaken to develop a secure system for transmitting packets to their intended destinations. BASSMA et al. [12] proposed a geographic routing approach based on Named Data Networking (NDN) with support for Delay-Tolerant Networking (DTN). The packets are forwarded using a hybrid routing strategy that includes greedy, perimeter, and DTN methods. RAMIN et al. [13] presented a Geographic Routing Protocol Predictive in Nature (PGRP). Each node in this protocol assigns a weight to its neighbors based on the node's position. It is capable of predicting the location of each node based on the acceleration of the node and then forwarding packets accordingly. In [14], the authors presented GSTR, a system for distributing secure messages via socially connected trust nodes (Secure Multi-hop Message Dissemination in Connected Vehicles using Social Trust Model). The authors employ a cloud-based storage structure for messages that cannot be stored on a trusted node to boost the likelihood of successful message distribution. They establish the nodes' trustworthiness based on their social network relationships. This method is limited to multi-hop message propagation over a social network based on node-to-node trust calculation. For delay-tolerant networks, Xie and colleagues [15] suggest a service priority-based incentive scheme (SIS). This protocol gives the node with the highest relaying bundle a higher service priority and receives a higher delivery ratio. Three options are provided for defending against security attacks: a signature chain, cooperation frequency statistics, and combination clearance. The primary disadvantage of this technique is that it requires third-party oversight to ensure confidence. Abdelkader et al. [5] introduced Geo-QoE-Vanet (a Quality of Experience-Aware Geographic Routing Protocol for Video Streaming over Vehicular Ad-hoc Networks), a geographical routing protocol optimized for video streaming over Vanets. This protocol uses a Quality of Experience and Quality of Service associated formula to determine the next relay node. In [16], the authors suggested an Intersection-based Geographic Routing in Urban VANETs with Guaranteed Transmission Quality. This protocol collects data about road segment connectivity and delays to assign a weight to each road segment—the weight data assists in optimizing the routing path. To mitigate message forgery or modification attacks, ADNAN et al. [17] developed a secure trust-based architecture (Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET) that leverages blockchain technology based on GPSR to enhance security and privacy. This approach protects against attacks on the MAC layer. SUSHMA et al. [18] presented a Secured Multi-Hop Clustering Protocol for Location-based Routing in VANETs, which used a security mechanism based on GPSR to distinguish and drop all invalid messages for reducing VANET communications attacks. Bogus nodes verification technique used by CELES et al. [19] to limit the impact of spurious nodes employed a position verification technique to assess the falsified position information. A Secure SDN-Based Routing Protocol for the Internet of Vehicles was presented in [20]. SDN (Software Defined Networking) distributed architecture and Blockchain system within the RSU (Road-Side Unit) network are used to route messages securely. This protocol employs SDN in two ways: within the RSU network and across all VANETs.

**Table 1** provides an examination and comparison of geographical routing techniques.

**Table 1. Geographical Routing Protocols**

| Ref.year | Protocol name | Delay tolerant | Forward strategy | Transmission delay | Routing Overhead | Architecture | Secured | Implementation |
|---|---|---|---|---|---|---|---|---|
| [12], 2019 | GeoDTN-NDN | Yes | Greedy | Large | High | V2V | No | Difficult |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [13], 2018 | PGRP | Yes | Greedy | Large | High | V2V | No | Difficult |
| [5], 2020 | GeoQoE-Vanet | No | Greedy | Large | Large | V2V | No | Easy |
| [14], 2019 | GSTR | Yes | Greedy | Large | High | V2V | Yes | Difficult |
| [15], 2016 | A Secure SIS for DTN | Yes | Spray and wait | Large | High | V2I | Yes | Difficult |
| [16], 2018 | IGRTQ | No | Greedy | Large | High | V2V | No | Difficult |
| [19], 2018 | Verification for Bogus | No | Greedy | Large | High | V2I | Yes | Easy |
| [17], 2019 | Secure Trust-Based Blockchain | No | Greedy | Large | High | V2V | Yes | Difficult |
| [18], 2019 | Secured Multi-Hop Clustering | No | Greedy | Large | High | V2V | Yes | Difficult |
| [20], 2021 | SURFER | Hybrid | Greedy | Large | Low | V2I | Yes | Difficult |

## 3. PROPOSED SECURITY MODEL

The Intrusion Detection and Isolation System for Jellyfish and Black-hole (IDIS4JB) is a novel secure protocol built on intrusion detection and isolation of malicious nodes to protect against black hole and jellyfish assaults allowing for speedy decision making. In the suggested technique, the malicious node is viewed as an attacker (black hole or jellyfish attack), and the malicious node is removed from all routing tables' neighbor tables. Nodes in the network use three different types of lists: white, red, and black. Three types of nodes exist:

- Cooperative nodes that make themselves available for communication ("C").
- Nodes that refuse to participate ("R").
- Attackers ("A").

When communication between two nodes fails, and the detecting node is unable to determine whether the failure is due to ("R") or ("A"), the node is placed on the red list. If communication with the same node fails, it will be flagged as an attacker ("A") and added to the blacklist. The routing table will be cleared of nodes on the blacklist.

**Algorithm 1**

```
Initially For all neighbors WhiteList.insert(Neighbor) ;   // add all neighbor nodes to the white list
        If Communication with Node failed then   // When the communication with node failed
        Begin
            WhiteList.delete(Node);      // Remove the node from the white list
            RedList.insert(Node);         // Add the node to the red list
        End;
        If Communication with the same Node failed again then   //If the communication with the same node failed
        Begin
            Node considered as Attacker   //The node considered as attacker
            RedList.delete(Node);            // Remove the node from the red list
            BlackList.insert(Node);           // Add the node to the black list
        End;
        RoutingTable.delete(BlackList);          // Remove black list nodes from routing table
End.
```

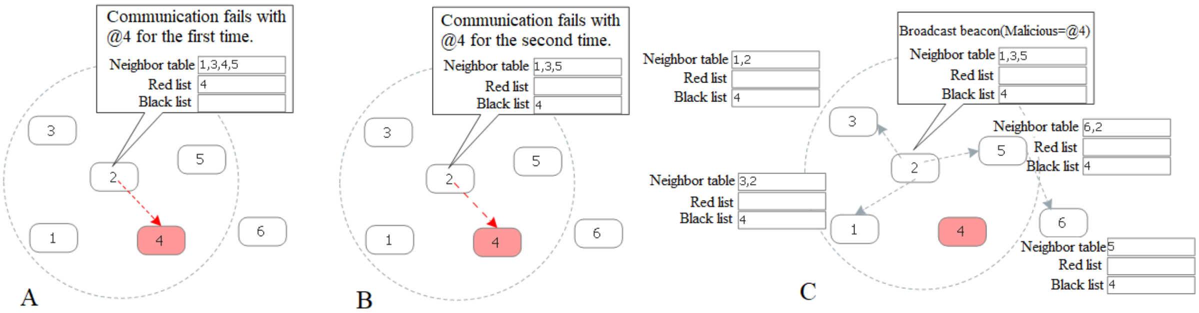

**Figure1: Proposed approach scenarios.**

Our suggested method uses periodic beacon packets to alert vehicles to malicious nodes. We include a field identifying the rogue node in the beacon packets (**Figure 1A**). When a detective node finds a malicious node, it transmits a beacon packet to warn its neighbors about the attacker and update their lists. When a node receives these beacon packets, it updates its information. When communication fails, as illustrated in Figure 1, node 2 takes action by adding node 4 to the red list. In **Figure 1B,** connection with node 4 fails for the second time, indicating a malicious node added to the blacklist. The beacon with the field corresponding to the negative node broadcasting to his neighbors to update their lists is seen in **Figure 1C.**

## 4. PERFORMANCES EVALUATION

This section describes the evaluation metrics that were used to assess four regimens (SURFER[20], Geo-QoE-Vanet[5], Secure Trust-Based Blockchain[17], and GSTR[14]). We employ two criteria in this evaluation: Packet Delivery Ration and End to End Delay. The packet delivery ratio (PDR) is the ratio of packets received by the destination to those delivered by the source vehicle. As shown in Figure 2, Secure Trust-Based Blockchain [17] has the highest PDR of the four protocols, while SURFER [20] has a slightly lower PDR in scenarios involving 60 to 100 vehicles. In any event, due to SURFER [20], the packet delivery ratio increases when the number of vehicles is increased. GSTR's PDR declines with the number of cars until it hits 50, which decreases less than SURFER's PDR [20]. GeoQoE-[5] Vanet's PDR is lower than the other protocols in 40–100 vehicles scenarios. The average time between when a data packet is sent and successfully received at its destination is called the End to End Delay. Figure 3 illustrates the influence of vehicle count on the End-to-End Delay for situations ranging from 20 to 100 cars. Geo-QoE-[5] Vanet's demonstrated a considerable rise in End-to-End Delay as the number of vehicles increased compared to other protocols. As illustrated in the figures, both Secure Trust-Based Blockchain [17] and SURFER [20] saw a consistent, decreased End to End Delay, with SURFER [20] experiencing a modest drop. According to GSTR [14], when the number of cars increases, the End-to-End Delay increases slightly.

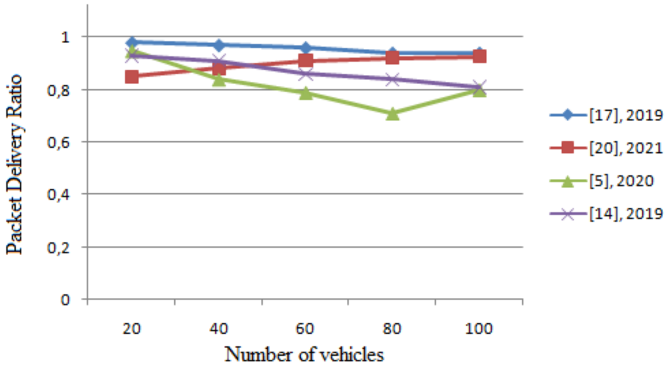

**Figure2: Packet Delivery Ration for the number of vehicles.**

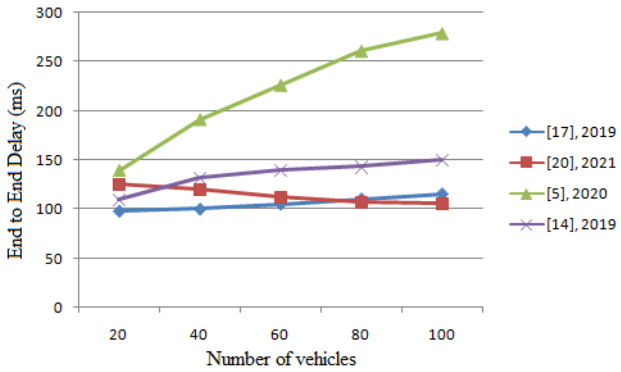

**Figure3: End to End Delay for the number of vehicles.**

## 5. CONCLUSION

Enhancing communication security in vehicle ad hoc networks was a potential issue for academics and industrials. Malicious nodes will decrease communication efficiency and harm network performance. This paper examined and classified numerous types of geographical routing protocols. Additionally, we presented a novel secure protocol based on intrusion detection and node isolation to offer security against black holes and jellyfish assaults while allowing speedy decision-making. Our proposed strategy can be used in conjunction with existing methods for enhancing security routing in automotive ad hoc networks. An efficient simulator will be used to study the simulation of active and passive attacks in V2V and V2I communication in future work. The proposed protocol's performance will be compared to that of other types of secure vehicular ad hoc routing protocols using various stimulation settings and metrics.

## REFERENCES

[1] A. Fitah, A. Badri, M. Moughit and A. Sahel, ***"Performance of DSRC and WIFI for Intelligent Transport Systems in VANET"***, *Procedia Computer Science*, pp. 360-368, 2018.

[2] DN. Vadhwani and S. Buch, ***"A Novel Approach for the ITS Application to Prevent Accidents using Wireless Sensor Network, IoT and VANET"***, *IEEE International Conference on Electrical, Computer and Communication Technologies*, pp. 1-7, 2019.

[3] C. Tripp-Barba, A. Zaldívar-Colado, L. Urquiza-Aguiar and JA. Aguilar-Calderón, ***"Survey on Routing Protocols for Vehicular Ad Hoc Networks Based on Multimetrics",*** *Electronics*, p. 1177, 2019.

[4] R. Karimi and S. Shokrollahi, ***"PGRP: Predictive geographicrouting protocol for VANETs"***, *Computer Networks*, pp. 67-81, 2018.

[5] A. Benmir, A. Korichi, A. Bourouis, M. Alreshoodi and L. Al-Jobouri, ***"GeoQoE-Vanet: QoE-Aware Geographic Routing Protocol for Video Streaming over Vehicular Ad-hoc Networks"***, *Computers*, p. 45, 2020.

[6] R. Arnous, ESMT. El-kenawy and M.Saber, ***"A Proposed Routing Protocol for Mobile Ad Hoc Networks",*** *International Journal of Computer Applications*, p. 8887, 2019.

[7] M. Naderi, F. Zargari and M. Ghanbari, ***"Adaptive beacon broadcast in opportunistic routing for VANETs"***, *Ad Hoc Networks*, pp. 119-130, 2019.

[8] GD. Singh, R. Tomar, HG. Sastry and M. Prateek, ***"A Review on VANET Routing Protocols and Wireless Standards"***, *Smart computing and informatics*, pp. 329-340, 2018.

[9] H. Hasrouny, AE. Samhat, C. Bassil and A. Laouiti, ***"Trust model for secure group leader-based communications in VANET"***, *Wireless Networks*, pp. 4639-4661, 2019.

[10] H. Hasrouny, AE. Samhat, C. Bassil and A. Laouiti, ***"VANet security challenges and solutions: A survey"***, *Vehicular Communications*, pp.7-20, 2017.

[11] MA. Burhanuddin, AAJ. Mohammed, R. Ismail, ME. Hameed, AN. Kareem and H. Basiron, ***"A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective"***, *Journal of Telecommunication, Electronic and Computer Engineering*, pp. 17-21, 2018.

[12] B. Aldahlan and Z. Fei, ***"A Geographic Routing Strategy with DTN Support for Vehicular Named Data Networking"***, *IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 361-366, 2019.

[13] R. Karimi and S. Shokrollahi, ***"PGRP: Predictive geographic routing protocol for VANETs"***, *Computer Networks*, pp. 67-81, 2018.

[14] A. Paranjothi, MS. Khan, S. Zeadally, A. Pawar and D. Hicks, ***"GSTR: Secure Multi-hop***

***Message Dissemination in Connected Vehicles using Social Trust Model"***, *Internet of Things*, p. 100071, 2019.

[15] Y. Xie and Y. Zhang, ***"A secure, service priority-based incentive scheme for delay tolerant networks",*** *Security and Communication Networks*, pp. 5-18, 2016.

[16] L. Liu, C. Chen, Z. Ren and FR. Yu, ***"An Intersection-Based Geographic Routing with Transmission Quality Guaranteed in Urban VANETs"***, *IEEE International Conference on Communications*, pp. 1-6, 2018.

[17] AS. Khan, K. Balan, Y. Javed, S. Tarmizi and J. Abdullah, ***"Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET"***, *Sensors*, p. 4954, 2019.

[18] KS. Eunice and I. Juvanna, ***"Secured Multi-Hop Clustering Protocol for Location-based Routing in VANETs"***, *International Journal of Advanced Computer Science and Applications*, pp. 121-126, 2019.

[19] AA. Celes and NE. Elizabeth, ***"Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication",*** *International Conference on Communication and Signal Processing*, pp. 0388-0392, 2018.

[20] K. Mershad, ***"SURFER: A Secure SDN-Based Routing Protocol for Internet of Vehicles"***, *IEEE Internet of Things Journal*, pp.7407-7422, 2021.