# A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack


**Gaurav Soni and Kamlesh Chandravanshi**

**Abstract** Vehicular ad hoc networks (VANETs) establish dynamic connections between cars, vehicles, and RSUs at a 6G data rate of 1KGbps. Communication between or among cars is feasible with the assistance of an RSU or an intermediary vehicle, and also the vehicles convey traffic status to the leading and neighboring vehicles. If any car engages in inappropriate activity with other vehicles, the data privacy is jeopardized. This paper offers a novel privacy-preserving under denser traffic management (PPDM) routing strategy for the 6G-VANET to protect it against malicious black hole attacks in VANET. All key information from traffic status packets supplied by leading cars to the following vehicles is discarded by black hole vehicles. A security system detects and prevents packet drops on a connection through a node. The performance of the present SAODV security system is compared to that of the innovative PPDM. After preventing malicious vehicles operating in the network, the PPDM secures the VANET and improves performance. The performance of the proposed PPDM scheme is compared with the existing SAODV. The PPDM has enhanced the performance and reduced the data dropping when compared to SAODV. The network performance in the presence of attack and secure PPDM performance is measured through the performance metrics like throughput, PDR, and end-to-end delay. PPDM is proven that it improves the data receiving and minimizes data dropping in the network.

**Keywords** VANET · 6G · PPDM · Black hole attacker · Routing · Security

## 1 Introduction

In recent years, the research interest in intelligent transportation systems (ITSs) has increased in industry and academia [1]. ITSs' primary goal, in addition to providing entertainment services in automobiles, is to improve road safety and driving conditions [2]. Vehicular ad hoc network (VANET) is built using two forms of

G. Soni · K. Chandravanshi (✉)
Lakshmi Narain College of Technology(Excellence), Bhopal, India
e-mail: kamlesh.vjti@gmail.cm



P. Karrupusamy et al. (eds.), *Sustainable Communication Networks and Application*,
Lecture Notes on Data Engineering and Communications Technologies 93,
https://doi.org/10.1007/978-981-16-6605-6_49

communication, namely vehicle-to-vehicle (V to V) communication and vehicles-to-infrastructure (V to I or RSU) communication to transmit the essential driving information [3]. The larger bandwidth and high data rate show better results in traffic control and monitoring since the number of vehicles on roads continually increasing**.** Vehicles interact with adjacent vehicles to replace the data in V to V communication, whereas the vehicles communicate directly with roadside units (RSUs) in V2I communication [4]. For V to V and V to I communications in VANETs, a dedicated short-range communication (DSRC) radio [5] and a handful of IEEE standards can be utilized. VANETs' unique properties, such as their great mobility and instability, have rendered them to be more vulnerable to many types of external and internal assaults [6]. These assaults have given rise security, privacy, and trust challenge in the design of safe VANETs. The major goal of VANETs is to enhance the road safety for drivers. VANETs will transmit different types of information, such as traffic signal violation warnings, precrash sensing, traffic jam warnings, curve speed warnings, and many more. Since mobility is a primary element of VANETs, any relevant simulation model should consider the consequences of mobility with the varied mobility patterns, and a suitable mobility model that depicts various facets of the experienced movement [7]. The VANET uses IEEE 802.11 standard Industrial, Scientific, and Medical band (ISM) band, and it is useful for many real-time implementation with the ad hoc nature. One of the vital features of such networks is flexibility, and it can be implemented without pre-existing infrastructures. Therefore, these networks are appropriate for an emergency application. The example of V to V and V to RSU is mentioned in Fig. 1. Here, the vehicles are also exchanging the traffic information with other vehicles and RSU. The prominent role of RSU is to control the traffic, check the traffic information of vehicles, and monitor the vehicle's activities.

When dealing with mobility models, it is also important to understand mobility, which is divided into macro- and micromobility. Macromobility defines and addresses motion limitations such as road topology, street features, traffic signals and signs, node flow, density, and distribution, i.e., any street element that may limit or impact mobility. On the other hand, micromobility refers to the movement of individual vehicles and their interactions with other vehicles, such as overtaking and acceleration/deceleration [8]. The 6G network will certainly improve the network service when compared to previous generations. The 6G vision is expected to be developed between 2022 and 2023 in order to define the 6G requirement,

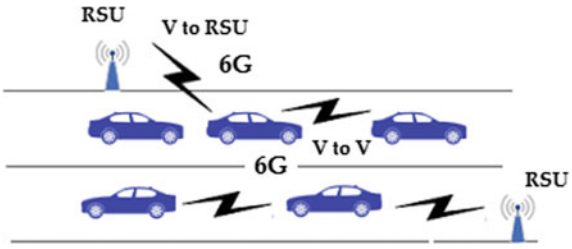


**Fig. 1** Example of V to V and V to RSU communication

and it assesses 6G development, technologies, standards, and so on. The International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP) are anticipated to develop the standards for 6G by 2026–2027 [9 ,10].

The presence of a black hole attacker causes harmful activity in the network [11]. Without security guarantees, some misbehaving or malevolent vehicles render the system to be susceptible for offering low-quality services or even put user vehicles in unsafe circumstances in 6G-VANET. As a result, identifying the misbehaving or malicious vehicles has become a critical task in VANET security. The security method of finding an attacker's vehicle is based on the information identified about the traffic network. The scheme detects the attacker's presence and estimates the total number of packets dropped by the black hole attacker in the network.

## 2 Network Model

In VANET, network model for vehicles can be separated into three groups [12]. These groups include servers for application and authorization, facilities on the road side, and nodes/vehicles in 6G-VANET.

### *2.1 Application and Authorization Servers*

These are powerful workstations, which are, respectively, responsible for managing and providing service data. The authority knows all the keys and is accountable for maintenance planning. For cars, device servers provide the operation details. The government or foreign operators will fund them. We assume that there are powerful processing capabilities for authorization and application servers. So, here we ignored the computation time.

### *2.2 Road Side Infrastructure*

Road infrastructure consists of power supplies located near roads, and it is also responsible for the collection and dissemination of data. Through wired networks, RSUs are connected to power and it will communicate via radio signals with vehicle but for vehicle-to-vehicle wireless communication radio or microwave signals are used.

### *2.3 Nodes/Vehicles*

Nodes or vehicles move in the road and communication with the RSU or also their information exchange information is received by RSU in network. Every vehicle is presumed to be fitted with a differential GPS receiver with an order accuracy and On-Board Unit (OBU) responsible for all communication and computing tasks [13].

## 3 6G Overview

The sixth-generation (6G) communication technology provides faster data rate for communication among or between the vehicles. 6G operates at a higher frequency to obtain a broader bandwidth, i.e., in Terahertz. The huge amount of bandwidth is available for users for sharing traffic information. The responses of RSU to V and V to V also improved. Compared to 5G, 6G can boost data rates by up to a hundred times, sustaining Tb/s highest data rate and 1000 Gb/s data rate experienced by user [9, 14]. Furthermore, 6G may employ flexible frequency sharing technologies to improve frequency reuse efficiency. 6G is a customized intelligent network because broad area for communication here is available to vehicles. 6G should be a ubiquitous and integrated network with more extensive and deeper coverage, covering terrestrial communication, satellite communication, short-range device-to-device communication, and so on. 6G is intellectual mobility management technology that can operate in various situations, including airspace, land, and water, resulting in a worldwide ubiquitous mobile broadband communication system. When combined with artificial intelligence technologies, 6G will enable virtualized personal mobile communication, with the network transitioning from a classic function centralized type for user centralized, data centralized, and completely content centralized. The main drawback in centralization is dependency on centralized unit for communication. It is also supports decentralized networks like WSN, MANET, and VANET. The 6G commutation is also very helpful for sustaining the current location of vehicles. It is same as location information of nodes in MANET [15, 16]. The 6G network will feature an endogenous security scheme or function security integrated design.

Furthermore, by incorporating trust and safety mechanisms, 6G can self-awareness, real-time dynamic analysis, and adaptive risk and confidence evaluation, all of which will aid in the realization of cyberspace security. Furthermore, 6G will combine processing, sensing with communications and navigation. For example, 6G will incorporate with satellite communication systems, satellite navigation, and positioning systems, as well as radar sensing systems. Finally, 6G might have a more efficient structure that includes software-defined core networks and radio access networks. 6G will be capable of rapid and self-intelligent expansion and quick dynamic exploitation of network functionalities. 6G can generate massive amounts of data via the Internet of Everything; 6G can also combine with novel technologies

such as artificial intelligence, block chain, cloud computing, edge computing, and so on [9].

## 4 Routing in VANET

Routing protocols may be divided into several types based on their characteristics [14, 15]. Most popular method for differentiating VANET routing protocols depends on obtained and preserved routing information. The routing protocols are classified as follows:- (Table 1).

## 5 Literature Survey

This section discussed the previous work on security with its drawbacks. The different author's contribution provides different security approaches for securing vehicular communication.

Li et al. [11] proposed an approach that maintains the reliable and safe communication between vehicles and improves the functioning of routing protocol in presence of threats in vehicular ad hoc networks. When a vehicle receives an AODV control message requesting that it establishes or modifies a route for a specific destination, it searches its routing database for an entry that leads to the location. AODV control messages are sent to vehicles to establish or change routes for specific destinations. The system produces a route entry with the sequence number specified in the control packet if there is no route entry; otherwise, the sequence number is flagged as invalid. The most significant flaw in the study is that the author restricts his attention to comparing the performance of various routing protocols. As a result, there is nothing unique about this work. The vehicle's speed is likewise indicated in kilometers per hour (km/h), but in milliseconds per second (m/s) is mentioned in Fig. 2 [11].

Soni et al. [17] proposed the PSO method for V to RSU communication to ensure security and communicate information about the attacker's vehicle to all RSU at rest and the vehicles near the attacker. The suggested preventive technique is intended to thwart the harmful acts of the attacker while still ensuring a secure connection in the VANET environment. However, the most significant flaw in this work is that it fails to specify the range of pheromones and the dropping behavior of the attacker.

Dhaya et al. [18] proposed an ACO scheme to find the shortest path among several possible paths. Accordingly, the probability of street consistency can be calculated using the expression given in the previous sentence. The buses are employed as a way of transporting the packages and directing them to their intended destinations. In each path connecting the two ends, streets are used as connecting points, and the relay bus that corresponds to the specified street is picked along with the path. Its primary weakness is that the ACO method by default supports the multipath approach, which is not ideal. Even in the presence of traffic congestion, the multipath routing

**Table 1** Routing protocols of VANET

| Proactive routing | Reactive routing | Hybrid routing |
|---|---|---|
| Proactive routing is also known as table-driven routing protocols. They monitor the networks topology at all the times, and the routes will be continuously evaluated for all the destinations | Reactive routing protocols are often known as on demand routing protocols, and it only performs route determination on demand. In data transfer, reactive protocols only select a route at the start of a connection | The benefits of both proactive and reactive routing systems are combined in hybrid routing strategies. Hybrid protocols make use of hierarchical network designs |
| Routes are stored by performing periodically interchanging routing tables in network, like the wired network | Once the route is created, the details are kept in the database of routing until the destination is unable to reach or the route expires | Table-driven routing guarantees great quality in static topologies but cannot be used to mobile networks |
| An advantage of this protocol is that routes must be decided and maintained in the buffer so whenever routing takes place these routes are used immediately so that the overall delay in the system must be reduced. To get the information of route and making a session is not very time consuming | The advantage of routing information is not updated on a regular basis, routing overhead is decreased dramatically during topology changes | The advantage of this protocol is combining the best features of both, a few hybrid routing protocols have been devised, in which routing is launched with certain proactive routes and subsequently satisfies demand from other nodes via reactive floods |
| This protocol has a disadvantage that whenever the topology changes, it reacts to those changes, though traffic is not affected, and results in the unwanted use of the bandwidth even there is not transfer of data | The delay experienced during route finding is one of these systems' drawbacks. These protocols, however, must be particularly efficient for highly mobile networks | In a dynamic network, typical routing protocols of this category function depends on radius of zone. On-demand routing offers less routing costs than traditional routing, however it suffers from routing latency |
| The protocols of this type are Optimized link State Routing (PLSR) protocol and Destination Sequenced Distance Vector Routing (DSDV) protocol | Ad hoc On-demand Distance Vector routing protocol (AODV) and Dynamic Source Routing (DSR) are reactive routing protocols | Zone Routing Protocol (ZRP) is the example of zone routing |

condition will not function well. ACO approach is based on pheromone values but not mentioned.

Hu et al. [19] proposed a REPLACE trust-based platoon service recommendation approach, to rank platoon head vehicles by developing a trust and reputation system. They also recommended that based on feedback from user vehicles, the server computes platoon head vehicle reputation rankings for the platoon head vehicle. This allows the server to clearly distinguish between well-behaved platoon head vehicles

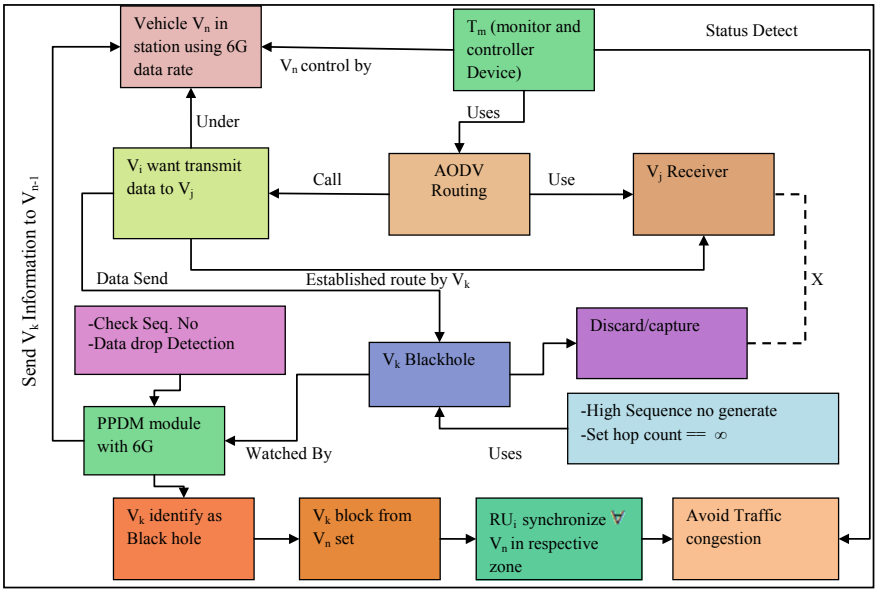


**Fig. 2** Security architecture of PPDM

and poorly behaved platoon head vehicles based on their reputation ratings. The malicious functioning of vehicles is based on bad and good behavior. The network's overhead increases because the server-side first verifies the traffic information and then declares it is a normal or malicious vehicle. It increases overhead in the network.

Qureshi et al. [20] proposed an Intelligent Secure Routing Scheme (ISRS) to assure data security during data transfer while transferring large amounts of data. This technology protects traffic information data in the network during data transfer from potentially damaging attacks and guarantees it remains secure. Forging, modification, and replay attacks are the three most serious security concerns that the proposed solution in VANET is designed to address. The main drawback of the paper is that the clustering mechanism is used but it is better for stationary or slow speed vehicles scenarios. That is why the delay is showing in *seconds* but it is better in *milliseconds*.

Memon [21] describes developing an authentication key setup approach based on IPv6 road networks. Using this technique, each neighboring car or RSU provides an unique address to a mobile vehicle, which prevents the mobile vehicle from receiving duplicate addresses. It includes a cryptographic authentication technique based on zero-knowledge proof, which each node may use to convince another node of the presence of a given secret without revealing it. The drawback of research is that the speed of vehicles is considered in meters/seconds but practically, it is measured in km/hour. Duplicate address identification procedure is complex. Not mentioned the specific use of IPv6 in research.

## 6 Problem Identification

Malicious vehicles might act both positively and negatively. The attackers have the ability to produce false information in the network and delete all traffic packets. Since packets are heavily lost on the network, the attacker cars increase network overhead. Because of the packet dropping attacker, retransmission of packets increases network latency even further. It is impossible to secure vehicle connection and deliver traffic status appropriately. In recent trends, it is observed that continuously the number of vehicles on the road increases. So the main problem is how to manage the traffic efficiently. The 6G communication technology provides a faster data rate for communication. The vehicles are continuously moving on roads but have no information of traffic on routes. The 6G communication support provides larger bandwidth and high data rate, i.e., the primary requirement of VANET. Although no significant research is being conducted in this area, it has been discovered that the offered solutions are not comprehensive in terms of effective and efficient routing security. All solutions have limits. They may have a substantial computational or communication overhead.

## 7 Privacy-Preserving Under Denser Traffic Management (PPDM)

VANET is highly dynamic and may expose internal and external attackers, posing significant technological problems in dependability and safe routing. Compared to the way roads are built, the attacker driving pattern is a less sustainable and more expensive approach to alleviate network load and increases the risk of routing misbehavior. The novel PPDM algorithm offers a security method against black hole attacks using an RSU unit to gather and evaluate audit data for the whole network. So, based on the above description, we infer that VANET is dispersed in nature and that we cannot trust any of the vehicles, since we cannot manage the network's topology as it changes. The PPDM secures routing from malicious attacks in VANET. The proposed PPDM allows for the safe transmission of data packets in a multihop way for identifying and blocking malicious vehicles.

### *7.1 Proposed Algorithm*

**Input:**
$V_n$: nth vehicles in network.
$T_m$: m traffic monitoring system.
$RSU_i$: no. of ith road side unit.
$B_{la}$: black hole attacker.
$M_r$: monitoring and preventer node $\forall$ $RSU_i$.

$S_i$: message sender $\forall V_n$.
$R_k$: message receiver $\forall V_n$.
$M_l$: intermediate vehicle $\forall V_n$.
$R_{req}$: route request.
$R_{rep}$: route reply.
$h_{seq}$: higher sequence number.
$Y_p$: capture packet.
$E_p$: drop packet.
$a_{bh}$: abnormal behavior ($h_{seq}$, $Y_p$, $E_p$).
$P_{roto}$: AODV for routing.
$\psi$: $RU_i$ control range.
dr: 6G data_rate(Tbps).
**Output:** Throughput, drop analysis, PDR, end-to-end delay.

***Method 1:*** *Black hole Detection and Network Monitoring*

$T_m$ watch the activity of assigned route
$T_m \leftarrow RSU_m$
**If** $V_k$ receive $R_{req}$ & not forward to $V_{k+1}$ **Then** // 1Tbps data rate (6G)
Watch $V_k$ activity by $T_m$ node
**If** $V_k$ generate the false $H_{seq}$ of $R_{req}$ **Then**
$T_m$ trace $V_k$ $a_{bh}(h_{seq})$
**If** match $a_{bh}(h_{seq})$ **Then**
$V_k \leftarrow B_{la}$ set by $T_m$
$T_m$ Send feedback to $M_r$ module
**Else**
In real time watch $V_k$ by $T_m$
**End If**
**End if**
**Else If** $V_k$ receives message of $S_i$ & $V_k$ != R & not forward **Then**
$T_m$ trace $V_k$ $a_{bh}(Y_p, E_p)$
$V_k$ create loop
**If** match $a_{bh}(Y_p, E_p)$ Then
$V_k \leftarrow B_{la}$ set by $T_m$
$T_m$ Send feedback to $M_r$ module
**Else**
In real time watch $V_k$ by $T_m$
**End If**
**End If**

***Method 2:*** *Black hole Prevention*
$M_r$ take response of route from $T_m$
$M_r$ re-analysis the activity of detected $B_{la}$
$M_r \leftarrow RU_m$
**If** $V_k$ as $B_{la}$ **Then**
$M_r$ check $S_i$ to $V_k$ Hop count , $Y_p$, $E_p$, $H_{seq}$ field
**If** $V_k$ as $a_{bh}(h_{seq}, Y_p, E_p)$ & hop count == $\infty$ **Then**
$M_r$ take confirmation $V_k$ as $B_{la}$
Block $V_k$ and Send negative response of $V_k$ to all $V_{n-1}$
$S_i$ call forward AODV($S_i$, $R_k$, $R_{req}$)
$RSU_i$ provide safe route to $S_i$ $\nexists$ $V_k$
$RSU_i$ communicate with $V_n$ or $RU_j$
$RSU_i$ synchronize $\forall$ $V_n$ in respective zone
Avoid congestion through $T_m$ module
**End If**
**End If**

The black hole attacker has degraded the network's routing performance, and the attacker infection is measured in forty node density scenarios. After detecting the malicious vehicles, the proposed security mechanism is also prevented from an attacker by denying the possibility of routing through hostile vehicles. The PPDM approach employs V to V and V to RSU communication to preserve security and forwards attacker vehicle information to all RSU and their surrounding vehicles.

## *7.2 Propose PPDM Architecture*

The architecture of privacy-preserving scheme is mentioned in Fig. 2. In this architecture, all vehicle-controlled vehicles are controlled by the Tm base station. If any vehicle wants to communicate with another vehicle, then Vi calls AODV routing and broadcasts routing packets to search the route. At the same time, route is found through the $V_k$ node in between source to destination and using 6G data rate. The step-by-step description of secure routing in 6G mentioned in Fig. 2.

Data privacy is not guaranteed due to the intermediary vehicle that facilitates communication from source to destination. Various man-in-the-middle attacks exist in network communication. The cross (X) in between Vj receiver and discard/capture block means attacker functioning. Black hole attackers generate a high sequence number, and false route information is given and captured and drop the data packet. To handle this situation, a PPDM module is proposed that periodically watches every active node. If any node drops the data by false routing behavior, block the particular vehicle from the communication and provide a new path from source to destination and preserve privacy during transmission. Proposed PPDM mechanism is considered as a more secured routing mechanism when compared to existing mechanism.

## 8 Result Description

A number of nodes 10, 20, 30, 40, and 50 are taken for simulation having 550 m radio range. The grid layout is about 800 m*800 m and propagation is two-ray ground. The simulator version is employed for simulation is Network Simulator version 2.31 (NS-2.31) [22]. The performance of PPDM security scheme routing is measured with previous SAODV and black hole AODV (BAODV). The number of nodes scenarios is same in all modules.

### *8.1 Throughput Analysis*

When the throughput performance is high, the data reception in the network will be improved. In this graph (Fig. 3), the throughput performance measurement of the existing scheme, black hole attack, and PPDM is measured in high 6G data rate. In SAODV existing approach, the throughput performance reaches about a maximum of 20,000 Kbps in the network. Still, in the case of black hole assault, the throughput performance is negligible or about 500 bits/sec in all different vehicle density but after applying the proposed PPDM scheme, the throughput is enhanced up to 27000Kbps. Thus, the proposed PPDM scheme improves the network performance and provides the attacker-free background of communication between sender and receiver through intermediate vehicles.

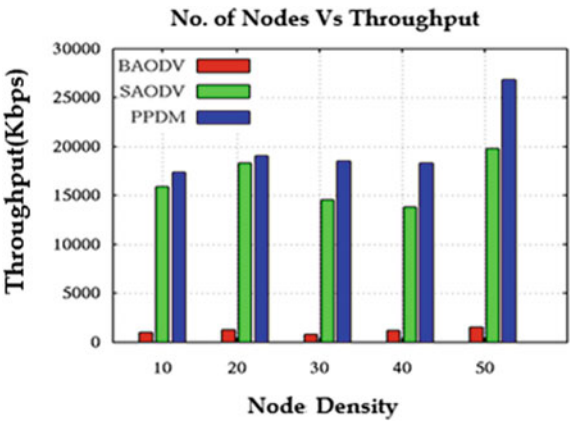


**Fig. 3** Throughput performance analysis

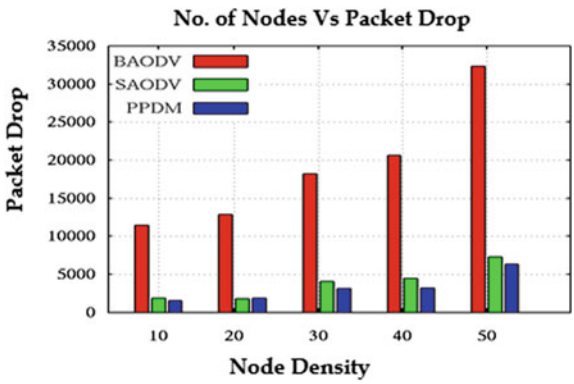


**Fig. 4** Packets dropping analysis

## *8.2 Packet Drop Analysis*

The attacker's presence in the network will degrade the routing performance. The vehicles in the attacker's range can send the fake message to the sender or send the wrong information of traffic to the sender vehicle. The number of vehicles directly connected to the assailant and attacker receives the packets from the sender and drops the whole packets mentioned in Fig. 4. The data dropping also increases due to delay in response of leading vehicles. The vehicles OBU used 6G standard for communication. The traffic status sharing using 6G improves the traffic controlling and examines traffic information. The performance data drop will decrease due to malicious vehicles mentioned in all different vehicle density scenarios. The number of attacker vehicles in the network is in different quantities in other vehicles density scenarios. The data dropping in the network is more than 30,000 in the presence of an attacker. That is, the attacker consumes the data packets in the network as well as the remainder of the data received at the destination, but the data received is much less.

## *8.3 PDR Analysis*

The packets percentage performance is measured through of delivery ratio (PDR). This graph (Fig. 5) evaluated the PDR analysis in black hole attack, previous security scheme, and privacy-preserving under denser traffic management (PPDM). The standard routing performance is only evaluated to stint the network performance after applying the proposed PPDM scheme. The PDR of black hole attack in the network is only 20%, which means an 80% data drop in 20 vehicles density and the rest of scenarios PDR performance showing in between 5 and 10%. The PPDM scheme improves the network performance and provides secure routing. The network's performance almost provides 80% PDR minimum in 50 vehicles, 91% maximum in 10 vehicles, and 20 vehicle scenarios. After applying a security scheme against

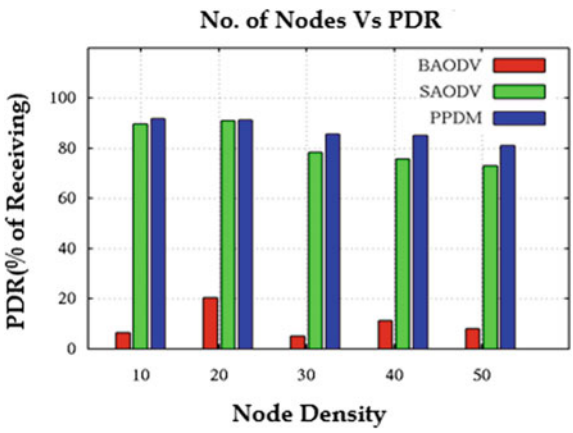


**Fig. 5** PDR performance analysis

attack, PDR performance is improved and better than SAODV. The proposed security scheme has enhanced the performance in the presence of malicious vehicles. The performance of the proposed method reduces the overhead that improves receiving.

## *8.4 End-to-End Delay Analyses*

The end-to-end delay analysis is measured in the presence of the attacker, in the existing security scheme and in PPDM proposed scheme mentioned in Fig. 6. The performance is measured in a scenario of five different vehicles density, and 6G high data rate quick response improves communication capability. The main reason

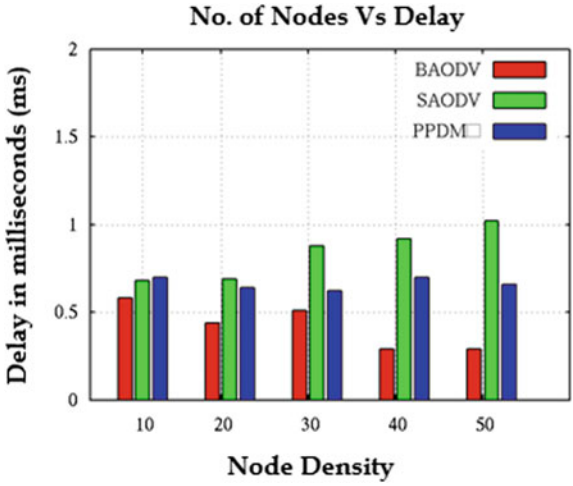


**Fig. 6** Delay performance analysis

for the delay is re-establishing the connection frequently due to link breakage or successful not receiving the data at the destination. The end-to-end delay in attacker presence is high and the delay is minimized by applying the existing security scheme. The proposed PPDM scheme minimizes the delay by providing strong connection establishment in between source to destination. The delay in the network degrades the routing performance due to the presence of a black hole attacker.

## 9 Conclusion and Future Scope

The privacy-preserving under denser traffic management for the 6G-VANET (PPDM) security algorithm provides security from black hole attack/s, which is to be a part of a fake path established for loss data packets. The 6G existence in the network also reduces the possibility of delay in communication because a sufficient bandwidth is available for proper traffic status delivery. The performance metrics show the difference in the performance of attacker, previous SAODV, and novel PPDM. It is clearly shown that proposed scheme is providing secure communication and prevent network from attacker. The PDR is about 92% evaluated in novel PPDM scheme, and it is about to 5% more than the existing SAODV. The presence of an attacker is atrocious because packet dropping is really more than 30,000 packets (50 vehicles scenario). The PPDM reduces the packet dropping and enhances receiving of data packets, i.e., also enhances throughput in 6G communication. The attacker's presence is confirmed by detecting the loss of data and fake route information in a dynamic network. The PPDM minimizes overhead and delay, i.e., the leading cause degrades the routing performance because more packets are drooping that enhancing the delay.

In future, the same concept also simulates with MP-DSR multipath routing protocols and also using a security concept with a location tracker system that traces attackers easily in a dynamic network. The location tracker system maintains the separate table for attacker and normal nodes with its mobility speed.

## References

1. M. Alam, J. Ferreira, J. Fonseca, Introduction to intelligent transportation systems. in *Intelligent Transportation Systems.* (Springer, Cham, Switzerland, 2016) pp. 1–17
2. M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions. Vehicul. Commun. **1**(2), 53–66 (2014)
3. A. Dua, N. Kumar, S. Bawa, A systematic review on routing protocols for vehicular ad hoc networks. Vehicul. Commun. **1**(1), 33–52 (2014)
4. M. Azees, P. Vijayakumar, L.J. Deborah, Comprehensive survey on security services in vehicular ad-hoc networks. IET Intell. Transport Syst. **10**(6), 379–388 (2016)
5. D. Jiang, L. Delgrossi, IEEE 802.11p: towards an international standard for wireless access in vehicular environments. in *Proceeding of IEEE Vehicular Technology Conference* (VTC Spring), May (2008), pp. 2036–2040

6. R.G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys. Comput. Commun. **44**, 1–13 (2014)
7. H. Hartenstein, K.P. Lanerteaux, A Tutorial on vehicular ad hoc networks. IEEE Commun. Magazine (2008) pp. 164–171
8. J. Haerri, F. Filali, C. Bonnet, M. Fiore, Vanet MobiSim: generating realistic mobility patterns for VANETs. (California, 2006)
9. M. Wang, T. Zhu, T. Zhang, J. Zhang , S. Yu, W. Zhou, Security and privacy in 6G networks: new areas and new challenges. Digital Commun. Netw. 281–291 (2020)
10. K.B. Letaief, W. Chen, Y. Shi, J. Zhang, Y.-J.A. Zhang, The roadmap to 6G: AI empowered wireless networks. IEEE Commun. Magaz. **57**(8), 84–90 (2019)
11. A.P. Jadhao, D.N. Chaudhari, Security aware routing scheme in vehicular adhoc network. in *IEEE Proceedings of the Second International Conference on Inventive Systems and Control* (ICISC 2018) (2018)
12. Y. Hao, Y. Cheng, C. Zhou, W. Song, A distributed key management framework with cooperative message authentication in VANETs. IEEE J. Selected Areas Commun. **29**(3), 616–629 (2011)
13. G. Li, L. Boukhatem, J. Wu, Adaptive quality-of-service-based routing for vehicular ad hoc networks with ant colony optimization. IEEE Trans. Vehicul. Technol. **66**(4), 3249–3264 (2017)
14. Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G.K. Karagiannidis, P. Fan, 6G wireless networks vision, requirements, architecture, and key technologies. IEEE Vehicul. Technol. Magazine (2019)
15. G. Soni, K. Chandravanshi, A multipath location based hybrid DMR protocol in MANET. in *IEEE 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things* (ICETCE) (2020)
16. G. Soni, M.K. Jhariys, Quadrant base location tracking technique in MANET. in *IEEE 2nd International Conference on Data, Engineering and Applications* (IDEA) (2020)
17. G. Soni, K. Chandravanshi, M.K. Jhariya, A. Rajput, An IPS approach to secure V-RSU communication from blackhole and wormhole attacks in VANET. in *First International Conference on Communication, Cloud, and Big Data* (CCB) (2020)
18. R. Dhaya, R. Kanthavel, Bus-based VANET using ACO multipath routing algorithm. J. Trends in Comput. Sci. Smart Technol. (TCSST) **03**(01), 40–48 (2021)
19. H. Hu, R. Lu, Z. Zhang, J.Shao, REPLACE: a reliable trust-based platoon service recommendation scheme in VANET. IEEE Trans. Vehicular Technol. **66**(2) (2017)
20. K.N. Qureshi, F. Bashir, A.H. Abdullah, Provision of security in vehicular Ad hoc networks through an intelligent secure routing scheme. *in IEEE International Conference on Frontiers of Information Technology* (2017)
21. I. Memon, A secure and efficient communication scheme with authenticated key establishment protocol for road networks. Wireless Pers. Commun. **85**, 1167–1191 (2015)
22. Network NS-2 (The Network Simulator) (2021). https://www.isi.edu/nsnam/ns/. Access from March