

A comprehensive verification of the header format and bandwidth utilization to detect distributed denial of service attack in vehicular ad hoc network

Arun Singh Kaurav, K. Srinivas

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India

Article Info

Article history:

Received Sep 7, 2023

Revised Jul 27, 2024

Accepted Aug 6, 2024

Keywords:

Comprehensive verification of header format and bandwidth
Distributed denial of service
Routing
Security
Vehicular ad hoc network

ABSTRACT

Vehicular ad hoc network (VANET) is a promising technology for controlling traffic on roads. Nowadays, heavy traffic is a major issue, and the presence of attackers exacerbates the situation. The most important challenge in VANET is its security from malicious vehicles. In order to defend against distributed denial of service DDoS attacks, we propose a comprehensive verification header format bandwidth detection (CVHB) in VANET. The behavior of a DDoS attack is unknown for all the other normal nodes in network. The header format of packer contains all the information of nodes that are actively participating in routing. The attacker infection probability measured by P_b and P_m or ($P_b > 0.9$). If both the parameters are high means attacker presence confirm in network. The CVHB scheme checks the packet header format of the attacker node, and only the attacker is one of the nodes whose sequence number is frequently changing. So, CVHB blocks the flooding of unwanted packets that consume the limited bandwidth of a wireless link and identify packets that contain no useful information. To measure the performance of the network, the basic performance metrics that are used are dropping percentage, packet delivery ratio (PDR), throughput and delay. The result of CVHB is showing improvement as compared to multilayer distributed self-organizing maps (MSOM) in VANET.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Arun Singh Kaurav

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation

Room no. F-302, Staff Quarters, Guru Nanak Institutions, Hyderabad, Telangana 501506, India

Email: arun.singh@klh.edu.in

1. INTRODUCTION

Vehicular ad hoc network (VANET) is a sort of network in which vehicle nodes connect with one another in a multihop fashion on the road [1]. VANET applications are majorly classified as either safe or unsafe. In nature, safety applications are extremely significant because they are directly tied to users and their lives. These programs give warning-related information to drivers, such as a post-crash notice on a certain road [2]. Each vehicle on-board unit (OBU) is linked to a sensor network to exchange speed, location information, and other data, and it can communicate with the OBUs of other vehicles and nearby road side units (RSUs) [2], [3]. The growing need for the services of broadband in-vehicle services offers new issues for the design and implementation of intervehicle communications in vehicular ad-hoc networks. Vehicle-to-vehicle (V to V) and vehicle to RSU or infrastructure (V to RSU or I) are two communication paradigms in VANET. The data rate plays an important role in quick response to requestor vehicle. The quick response means trailing vehicles are avoid the unnecessary traffic jamming on roads and also improves quality of service (QoS) of network [3]. Vehicle-to-infrastructure communications allow automobiles to connect to the Internet through a roadside base

station (BS). Intensive research and testing have been conducted to develop vehicle-to-infrastructure (V to I) technology in order to support in-vehicle applications like real-time traffic and weather updates [4]. Meanwhile, significant research has been devoted to short-range radio-based (V to V) communication technologies, like dedicated short-range communications (DSRC) [5], to support active safety applications. The routing protocols play an important role in forwarding traffic information to other vehicles, and each routing protocol has its own routing approach [6], [7]. Routing protocols are vulnerable to attacks. Security is an important challenge in the network [8]. The presence of an attacker in a network is very harmful to all connected nodes because the attacker's presence directly affects resources and data packets or files. A VANET is a subset of Mobile Ad-hoc network (MANET), and the nature of a distributed denial of service (DDoS) node attack is to generate unwanted packets in the network [9]. The bandwidth exhaustion probability (P_b) and memory exhaustion probability (P_m) consumption affected by attacker flooding. These two factors are important for proper incoming and outgoing of packets by nodes. The sensor network nodes are also affected by an attacker's flooding in a high-speed network because flooding is more in higher data rate [10], [11]. The vehicle to vehicle and vehicle to RSU or Infrastructure communication is mentioned in Figure 1. The vehicles can directly send requests or traffic information to other vehicles, which can then decide whether to take a route diversion or continue on the same path. The RSU is the superior unit to control traffic and directly or indirectly give instructions and receive traffic information to forward to the next RSU in VANET.

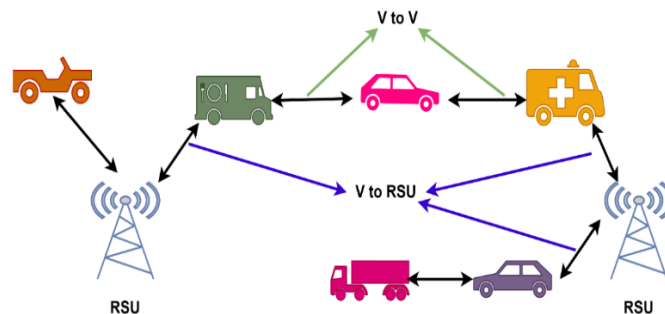


Figure 1. V to RSU and V to V communication in VANET

The attack may cause destruction and exhaustion of the nodes' and network's resources. Eventually, legitimate users will be unable to access the networks. DDOS is not tolerated in the VANET because timely and secure delivery of life-critical information is required. In summary, DDOS assaults can be carried by communication channel jamming, network overloading and packet loss [9], [10]. The routing process in VANETs involves all participating nodes. Because conventional routing protocols are designed for predefined infrastructure networks and cannot be utilized in VANET. VANET protocols were created to meet the need for less infrastructure in network. Routing decision normally based on the number of nearby available vehicles and reply by the vehicles those are participating in routing [12], [13]. The attacker injects or drops unwanted packets into the network. The attacker's goal is to simply divert or control traffic on roads by interfering with normal traffic information exchange [14], [15].

This article is divided into seven sections. Literature survey is described in section 2. Section 3 describes the problem statement. Section 4 describes the solution and proposed model against DDOS attack to secure the network. Simulation tool and simulation parameters is mentioned in section 5. Section 6 describes the results and comparison analysis. Conclusion with future work is mentioned section 7.

Table 1 (see in appendix) [16]–[21] discusses the literature survey i.e. contributions of many researchers in the field of VANET security and also describes the previous work, their limitations, performance and suggestions or possible future enhancement. This earlier work proposes a novel security mechanism for VANET. The research gap also mentioned in considered works.

This article focuses primarily on detecting and preventing the denial-of-service attack (DoS) by verifying the header format and bandwidth utilization and analyzing their impact on the basis of amount of data received in percentage, average delay, and number of DoS packets spread into the network. The presence of DDOS attackers directly affects the performance of the network. The presence of DDOS affects not only a single resource, but also multiple resources used in data forwarding in VANET. This type of attack is the major reason for traffic congestion on a particular route. This research aims to provide DDOS protection in VANET. The unnecessary consumption of bandwidth and buffer space jam the communication in network. Vehicles monitor and control the comprehensive verification of the header format and bandwidth utilization from a connected RSU, which is responsible for providing trust information of any vehicle to other vehicles.

The presence of a DDoS attacker doing the following:

- Single or multiple attackers are injecting unwanted packets in network that unnecessary consumes limited bandwidth for routing ($P_b > 0.9$). It is a common information for all vehicles that creatsconfusion on the route and vehicle cannot communicate with other because already attacker/s are communicating.
- The nodes are getting traffic information from nearby vehicles in the right way, but because of flooding, the attacker is affecting vehicle processing capability easily that means ($P_m = \text{high or buffer space almost full}$).
- Attacker is directly affecting the request and response mechanism of sender vehicles and receiver vehicles by capturing communication resources.
- Attacker assumes the identity of a legitimate user.

Some compromised OBUs or roadside base systems (RSBS) coordinate an attack on the system.

2. IDENTIFICATION OF DISTRIBUTED DENIAL-OF-SERVICE ATTACK

In this article, we identify a distributed denial-of-service attack by calculating the bandwidth, memory, and node exhaustion probability. If the total exhaustion probability exceeds 0.5, we consider the node suspicious and initiate the header format verification module. In this module, we cross-reference each packet header format with a legitimate protocol header format. If we encounter a packet that does not match any fields or field values, we classify it as an attacker packet. As a result, we identify the attacker's node using the packet's identification information. Distributed denial-of-service attackers typically generate high data rates to consume network resources, leading to increased utilization of bandwidth, memory, and nodes. Therefore, we compute their likelihood. The header verification process provides the details about the packet, such as the source id, destination id, sequence number, delay time, and so on. This information aids in calculating the inter frame space (IFSS). If the IFSS is less than average, which ensures that node is the attacker node, and by using the blocking method, we secure the complete network from a denial-of-service attack

A VANET is a network of vehicles and RSUs in which vehicles are controlled by RSU units that provide service to vehicles on the road. Because of the increasing number of vehicles on the road, road safety has become a measurable challenge with the recent advancement of technological growth. In the VANET architecture, some technology is required to monitor and provide efficient path information (software-based operation), which increases road safety and security. The proposed header verification method applies to the RSU, which validates the vehicle ID and computes the sequence number for each vehicle wishing to communicate in the network. Information about the vehicle's sequence number is available at the intermediate node or vehicle. The module explained by route establishment process, DDoS Attack detection by header and DDoS prevention after confirmation.

The following procedure is confirming the attacker presence in network:

- a. Bandwidth exhaustion probability (P_b)

It is represented as a queuing system M/G/k queue which is a queuing model in which arrivals are Markovian (modulated by a Poisson process), service times have a general distribution and there are k servers. It is given by (1):

$$P_b = \frac{\rho^L}{\sum_{m=0}^L \frac{\rho^m}{m!}}, \quad \rho = \frac{\gamma_b}{\mu_b} \quad (1)$$

where, L is channels used for communication and used these channels simultaneously but the (1) is only accurate for $L=1$, γ_b is the influx speed, it also defines the DDoS attack métier and μ_b is the service rate of the system.

- b. The memory exhaustion probability (P_m)

It is represented as a queuing system M/M/N/N given by (2).

$$P_m = \frac{\rho^S}{\sum_{m=0}^S \frac{\rho^m}{m!}}, \quad \rho = \gamma_m \cdot t_w \quad (2)$$

where S is the volume of data that can be kept in the buffer, t_w is the average service time and γ_m is the arrival speed, which is based on γ_b and P_b as (3).

$$\gamma_m = \frac{\gamma_b \cdot (1 - P_b) \cdot r}{q} \quad (3)$$

where q represents the average packets count in one session and r represents the number of packets required establish the session in network in presence of attacker.

- c. The node exhaustion probability (P_c)

It is represented as an M/M/1 queuing system. In this, the arrivals follow a Poisson process, the service times are distributed exponentially and one there exists one server. It is given by (4).

$$P_c = \begin{cases} 1, & \frac{\gamma_c}{\zeta_c} \geq 1 \text{ or } L \geq t_y \\ \frac{L}{t_y}, & \frac{\gamma_c}{\zeta_c} < 1 \text{ or } L < t_y \end{cases} \quad (4)$$

where the average time is L , a light weight process spends in the system, t_y is the time for which the user is ready for a service, ζ_c is the rate of service and γ_c is the arrival speed, which is contingent on γ_b and P_b given by (5).

$$\gamma_c = \gamma_b \cdot (1 - p_b) + \gamma_s \quad (5)$$

where γ_s represents the average request arrival speed for service.

The total success possibility of DDoS attack has to consider the fact that all the nodes involved in the model have an influence between each other. So, the total probability (P_t) of efficacious attack is represented by (6).

$$P_t = 1 - \overline{P_b} \cdot \overline{P_m} \cdot \overline{P_c} \quad (6)$$

2.1. Process of route establishment

There are two types of devices or nodes in a vehicular ad hoc network: OBU and RSU. OBU is equipped with a vehicle, and RSU is treated as the central coordinator of vehicular communication. Using RSU coordination, vehicles communicate with one another and share traffic information, safety information, entertainment information, and security information over a single hop or multiple hops. The route packet arrives at the RSU via direct or multi-hop-based routing from the source vehicle, which is responsible for broadcasting the route packet to other connected RSU as well as its own zone to find the receiver nodes. When a receiver node is found in the network, it creates the reverse path to send the acknowledgment back to the source vehicle (use (1) and (2) for bandwidth consumption and memory consumption). After getting the route acknowledgment source, start sending the data to the receiver node. The roadside unit system would maintain vehicle movement and route information of all connected vehicles in the network.

2.2. Header format verification

DDoS detection is a more critical task because the vehicle appears genuine but gains network resources by flooding the network with highly unwanted messages. In comprehensive verification header format bandwidth detection (CVHB) proposed attack detection system, we use the concept of sequence number verification and the inter frame space of same sequence number to reach the next connected vehicle that receives the unwanted message from the attacker. The attacker uses any of the sliding window's techniques to send frames into network nodes. Assume it uses go back-N in $K = 2$ trail, so the sender generates sequence number $2k$ (whose range is 0 to 3 out of 4 sequence numbers, S_n), and the frame within the sender's window is $S_n - 1$, which means (4-1=3 frames in the sender's window), while the other side receiver contains only one window, which is required by the sender node. The sequence is mentioned in Figure 2.

In the proposed scheme we described the functional behavior of the proposed header verification method to prevent the network from DDoS attack. The objectives of research are to avoid flooding unwanted packets to consume limited bandwidth of wireless link and identified packets contain no useful information. The attacker sets the broadcast address as the receiver vehicle during the route decision process, so most vehicles that receive the route message are treated as receiver vehicles, and the intended receiver vehicle does not understand attacker behavior and is treated as a genuine sender node. During data transmission, the sender starts flooding the unwanted packet using any of the sliding window techniques, which are received by the all-broadcast receiver node. When the CVHB algorithm detects that the sequence number is frequently repeated and the sender node is the same, it calculates the inter frame space of the same sequence number by the attacker ($IFSS_{n,A}$), and if we get $IFSS_{n,A} \leq (\text{Average}(IFSS_{n,g})/2^k)$ (inter frame space of the same sequence number by a genuine node), it means the sender node is suspicious as a DDoS attack. It indicates that the source vehicle is a denial-of-service attacker, and the receiver is also a denial-of-service attacker. The receiver of the attacker's packet also initiates flooding and similar processes throughout the network, causing the overall network functioning disturbed by the DDoS attacker.

There is a large flood of unwanted data into the network during distributed denial of service. Figure 3 depicts an orange-colored field, indicating that it is a highly vulnerable field that has been modified by a DoS attacker. The attacker first creates the window based on KTH and sends the frame quickly (inter frame space is very low), setting URG, PSH flag as 1 (frame is higher priority than other frames and PSH 1 means frame sent immediately without waiting), and FIN as 0 (meaning that after that other frame is continued, it does not finish). In the optional field, frame segment size will change dynamically, timestamp is (∞) (which means round trip time cannot be calculated), and packet type is unknown. On the basis of these fields, we will be sure the message is a DDoS attack and detect the attacker node. While the packet reaches the network layer, the attacker sets the destination IP as a broadcast address (255.255.255.255) for receiving by all nodes and spreads a distributed denial of service attack into the network.

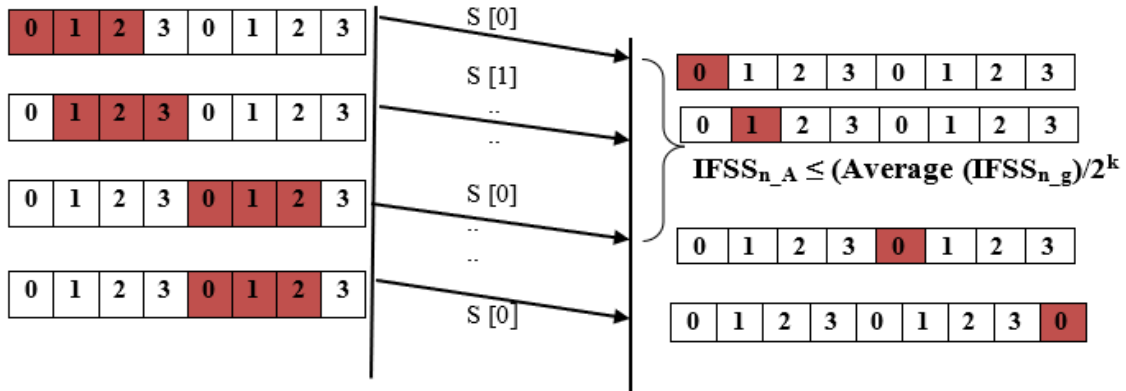


Figure 2. Inter frame space of same sequence number by attacker

$P_b > 0.9$ in T_s

Source Port				Destination Port				
Sequence Number (Frequently Generate)								
Acknowledgement Number								
Header length (4 bits)	Reserved bits (6 bits)	U	A	P	R	F	S	Window Size
		R	C	S	S	I	Y	
		G	K	H	T	N	S	
		(1)		(1)		(0)		
Checksum				Urgent Pointer				
Options								
(0-40Bytes) (Maximum Segment Size, Timestamp (∞), Window size extension, Padding)								
Data (Optional)								

Figure 3. DDoS attack time data header field

2.3. DDoS attack prevention

RSU determines whether the vehicle in the network is an attacker or not; for a DDoS attacker, if the misbehaving node's node ID and header contain unwanted information, block the node from future communication. RSU also sets their header information and sequence number, as well as broadcasts the block information to other vehicles in the network, so no more communication can take place from the attacker vehicle spoofing the network. RSUs also broadcast blocking information to other connected RSUs for complete network security purposes. The proposed CVHB would provide secure and safe communication to all vehicles in the network, as well as more dependable data communication between vehicles or RSUs. Finally, RSU determines whether the vehicle in the network is an attacker or not; for a DDoS attacker, if the misbehaving node's node ID and header contain unwanted information, block the node from future communication. RSU also sets their header information and sequence number, as well as broadcasts the block information to other vehicles in the network, so no more communication can take place from the attacker vehicle spoofing the network. RSUs also broadcast blocking information to other connected RSUs for complete network security purposes. The proposed CVHB would provide secure and safe communication to all vehicles in the network, as well as more dependable data communication between vehicles or RSUs.

3. METHOD

3.1. Comprehensive verification of the header format and bandwidth utilization (CVHB) architecture

In Figure 4, we explain the working architecture of CVHB, which starts from step 1 to develop the vehicular ad hoc network. In this step, the source node initiates the call routing protocol for searching the receiver node. In step 2, select the routing protocol as ad hoc on the demand distance vector (AODV), which provides the shortest path to the receiver node. Step 3 represents the use of the Floyd-Warshall algorithm to determine the shortest path through the route broadcasting method. During route broadcasting, there is a chance to get some malicious nodes that can start a denial-of-service attack, capture the identity of the receiver node, generate a high sequence number, and flood the attack packet into the network. In step 6, we execute the CVHB security technique, which takes the information of all intermediate nodes and calculates the bandwidth utilization, delay, and PDR. In step 7, we go back to step 6 to determine whether the node is an attacker or not. If the total probability exceeds 90%, proceed to step 8 for packet header format checking. In this step, if we receive URG = 1, PSH = 1, and Fin = 0, we identify the packet as an attacker node and block it; otherwise, we treat it as genuine and forward it to the receiver node, represented in step 11 of the block diagram.

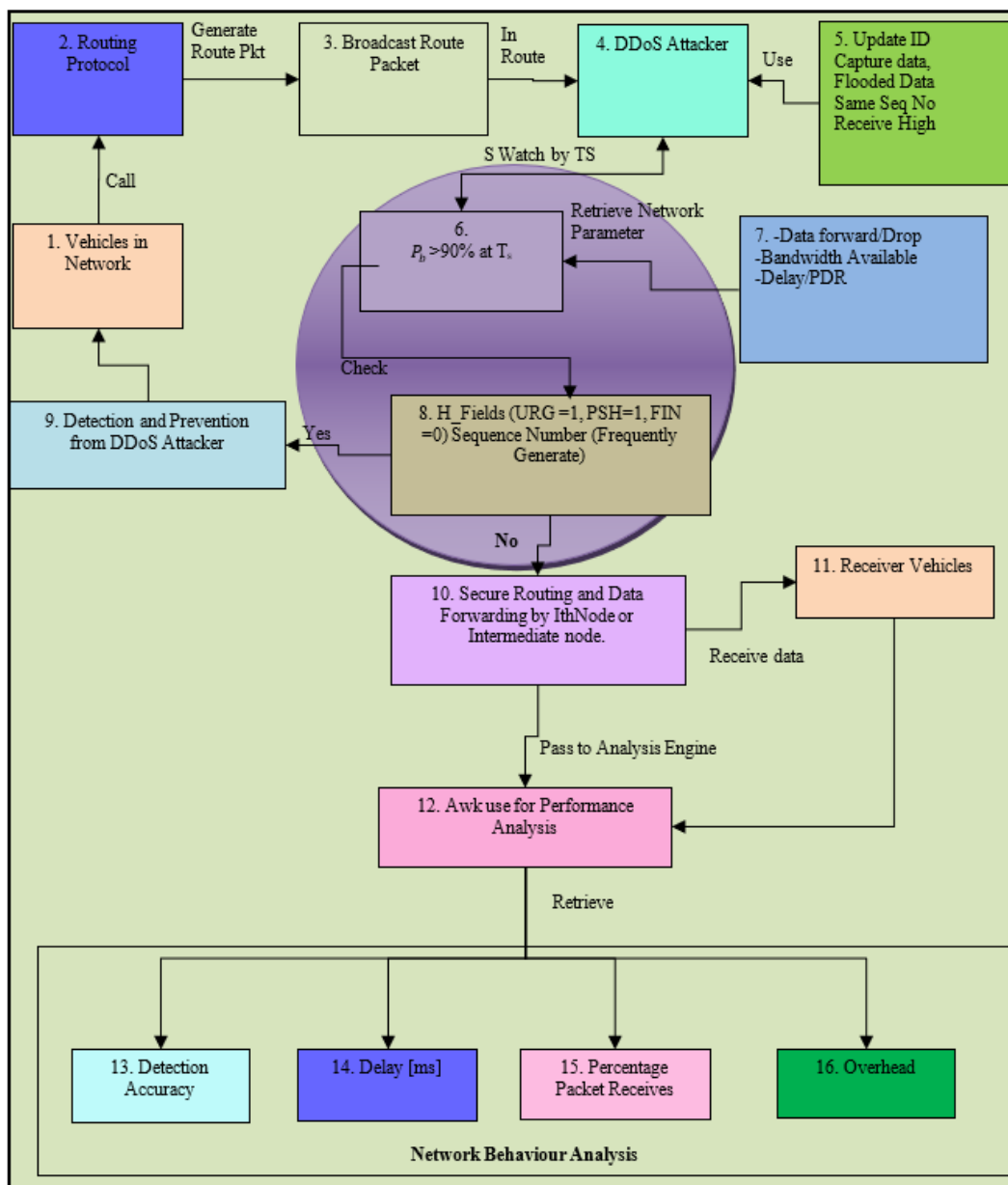


Figure 4. CVHB security system for VANET

Finally, get the receiver, and our network is identified as a secure network. At the end, simulator -2 generates the output file, which is passed into step 12 for data processing. Here, we use the awk script to get the output parameters, which are represented from step 13 to step 16. The analysis output includes attack detection accuracy, delay, percentage of data received, and overhead. The overall CVHB proposed system provides reliable and secure communication against the DDoS attack.

3.2. Simulation tool and simulation parameters

The simulation parameters considered for simulation are listed in Table 2. In VANET, nodes are vehicles, and vehicles in the network move with random velocities. The NS-2 simulator is used to create the different scenario in VANET [27]. The movement of vehicles is dependent on the traffic on the roads and the traffic status information forwarded by the leading and neighboring vehicles.

Table 2. Simulation parameter for deployment of VANET

Parameters	Configuration Value
Network simulator	NS-2.31
Routing protocols	DDoS-AODV, MSOM, CVHB
Area of simulation	1000*1000 m
Vehicle speed maximum velocity [m/s]	Random
Network type	VANET
Attack type	DDOS
Security technique	CVHB
Number of vehicles	100
Physical medium	Wireless, 802.11
Time for simulation (Sec)	550 Sec
Media access control (MAC) layer	802.11
Model of antenna	Omni antenna
Type of traffic	CBR, FTP
Propagation radio model	Two ray ground

3.3. Simulation experimental setup

In the experimental setup demonstration, first explain the traffic scenario of vehicles mentioned in Figures 5 and 6. In Figure 5 (showing network animator window of NS-2) vehicles are sensing for connection establishment or transfer traffic status request packets in network to leading vehicles. In Figure 6 vehicles start the movement with variable speeds and continuously forward or accept the traffic information. Figure 7 shows the demonstration of code run on NS-2 using Cygwin on windows. The attacker's role is to flood bulk of information, but proposed security scheme secures communication by applying CVHB scheme in VANET. For run the code use command "*ns CVHB.tcl*" and for change in the internal module run commands "*make clean*" for clear junk files then run "*./configure*", for patch localization distribution and run "*make*" command for add module with all external modules or for create object file of *cvhb.cc* files.

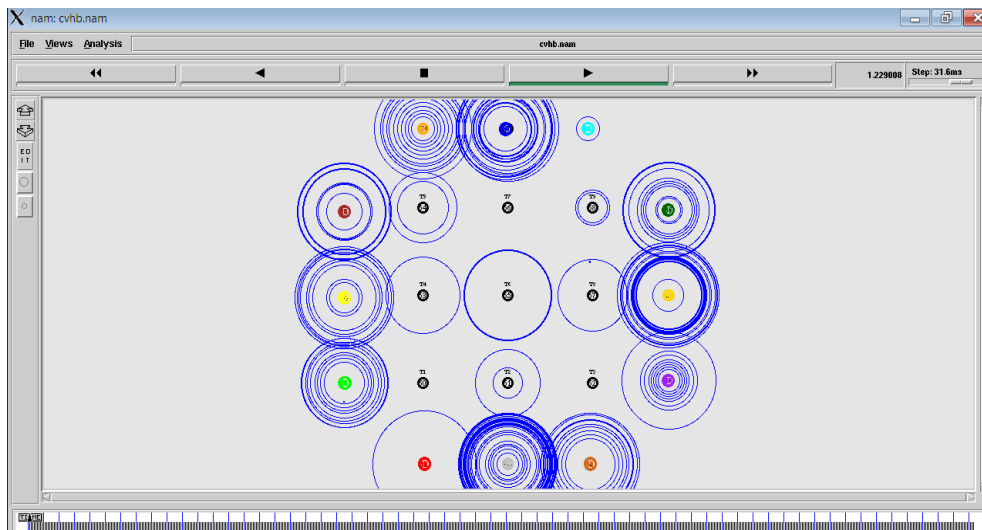


Figure 5. Vehicles are sensing for sending traffic status requests

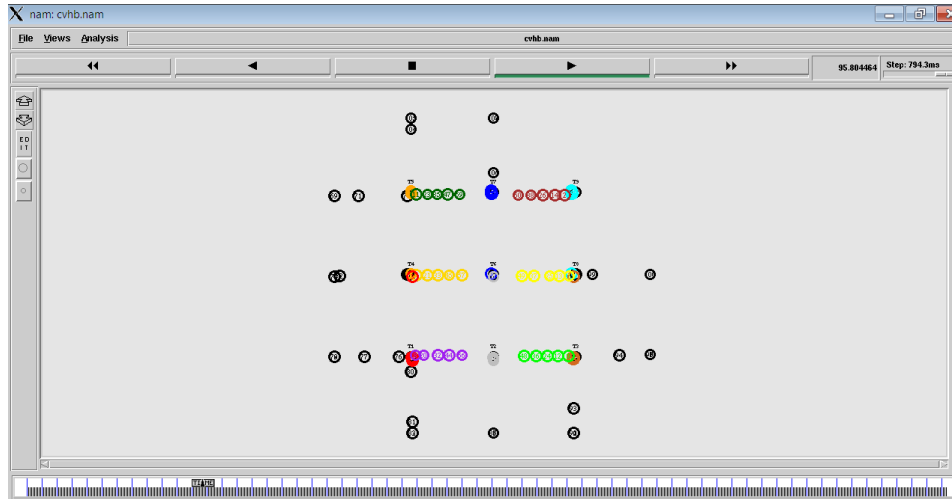


Figure 6. Vehicles movement and traffic information sharing

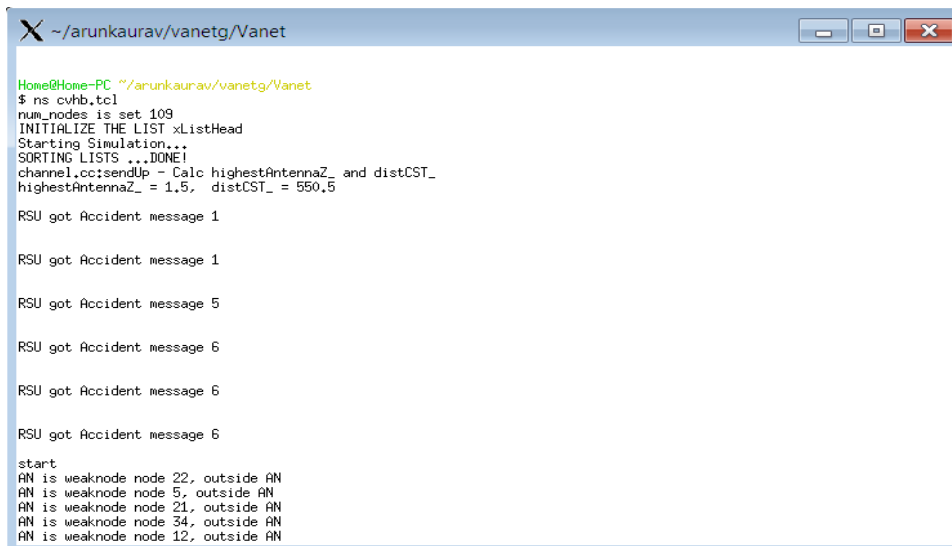


Figure 7. CVHB execution environment in NS-2.31

4. RESULTS AND DISCUSSION

Existing research analyzes the impact of DoS attacks using the supervised and unsupervised learning concept (MSOM), but it fails to accurately identify the flooding attacker node or the percentage of the attack. In our proposed CVHB approach, we accurately identify the attacker node, their behavior, the time of attack, and the percentage of the attack. Additionally, we ensure complete security through the use of a node blocking mechanism, resulting in an improved outcome for vehicular communication.

The performance evaluation of pure AODV, the previous MSOM, and the proposed CVHB shows that the CVHB is far better compared to existing scheme (MSOM) in VANET. The attacker only tries to reserve communication resources like bandwidth. The CVSB not only detects and prevents DDoS attacks in the network but also improves routing performance.

4.1. Throughput performance analysis

In VANET, the nodes or vehicles are continuously receiving traffic information from other vehicles and take the decision to follow the same route or move in another direction to avoid unnecessary delays in the network. The throughput is 22% at 500 seconds. The MSOM technique is able to block the attacker, but performance improvement is the major challenge. That is why throughput is only 40% at 500 seconds. The proposed CVHB approach's performance is better than the MSOM, and CVHB gives a better approach to

handling routing performance as well as attacker existence in the network. Its effect can be seen in performance at 55% at 500 ms mentioned in Figure 5 and delay analysis mentioned in Figure 8.

4.2. Average end to end delay analysis

Delays in the network can occur for a variety of reasons. Sometimes the sender is slow, and the receiver is fast, heavy traffic on a common route, collisions, and attacker presence are the main reason by that delay occurs in network. The average end to end delay of MSOM is about 30 ms. The proposed approach focuses not only on preventing DDOS attackers, but also on traffic status packet routing, which is the primary concern here. As a result, the proposed approach reduces flooding because the delay is only 25 ms (the maximum delay considered for all approaches) mentioned in Figure 9.

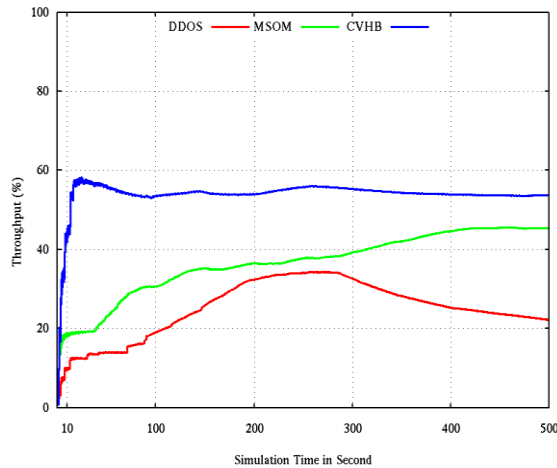


Figure 8. Throughput analysis

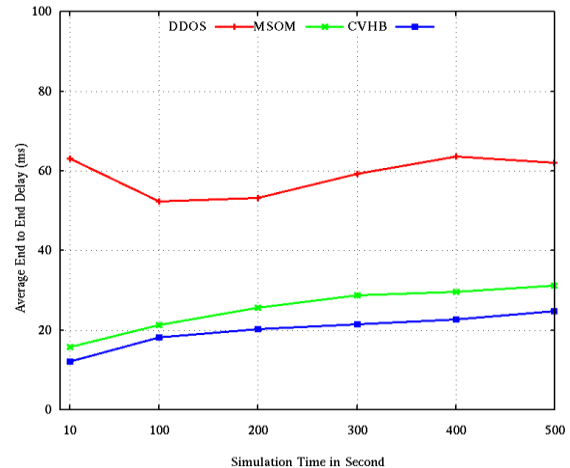


Figure 9. Delay analysis

4.3. PDR performance analysis

The number of packets sent and received in the form of a percentage is evaluated by packet delivery ratio (PDR) metrics. PDR measures the percentage of traffic status packets transmitted by sender vehicles versus packets accepted by the receiver. In this graph, the PDR is less than 50% in the presence of an attacker, and only a few packets reach their destination. The previous MSOM scheme gave an 80% success rate, but the CVHB scheme gave a 97% success rate. The meaning of "97% receiving" is minimum loss and smooth movement of vehicles in the network. Because the attacker is not active in the network, his presence is not affecting the performance of network mentioned in Figure 10.

4.4. Packet drop percentage analysis

The performance of the DDoS attacker, MSOM, and CVIB are evaluated, and it has been found that the proposed scheme gives better results mentioned in Figure 11. The dropping percentage is only 5% up to 500 seconds of simulation time. The dropping percentage in the presence of attackers is 38%, and the previous MSOM scheme blocked the attacker percentage, but the dropping percentage is only 25%. The proposed technique shows an improvement in performance that is 15% better than MSOM and 32% better than DDoS.

4.5. SDN controller utilization analysis

The software-defined networking (SDN) controller is responsible for traffic control in the presence of attackers in the network. The normal SDN network is the centralized controller for vehicle movement and traffic information generated by normal vehicles and attacker vehicles. The presence of the attacker means that the network will be inundated with unsolicited data. The MSOM utilization is minimal, but the performance of the network is satisfactory. The proposed CVHB performance improves the utilization of SDN and provides more than satisfactory performance mentioned in Figure 12.

4.6. DDoS packets flooding analysis

The presence of a DDoS attacker not only floods networks with unwanted packets, but it also has an impact on resource performance. If the resource requirements are not fulfilled by the RSU or SDN, it will

directly affect the delivery of traffic information and vehicle control on roads. The flooding of packets is measured in thousands, not hundreds, and will eventually be measured in lacks mentioned in the Figure 13.

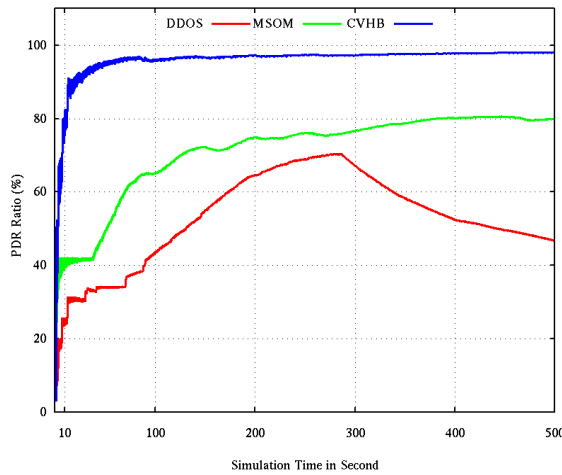


Figure 10. PDR analysis

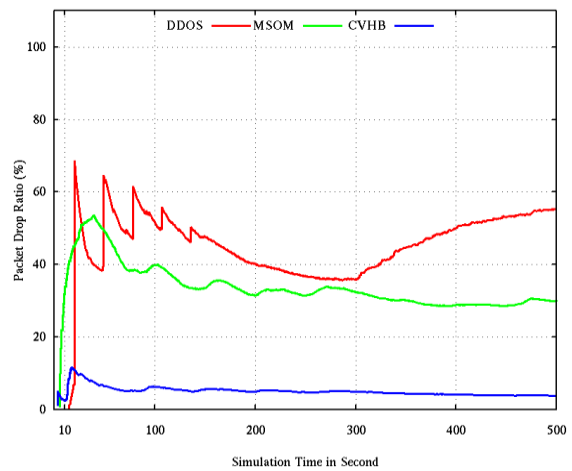


Figure 11. Drop percentage analysis

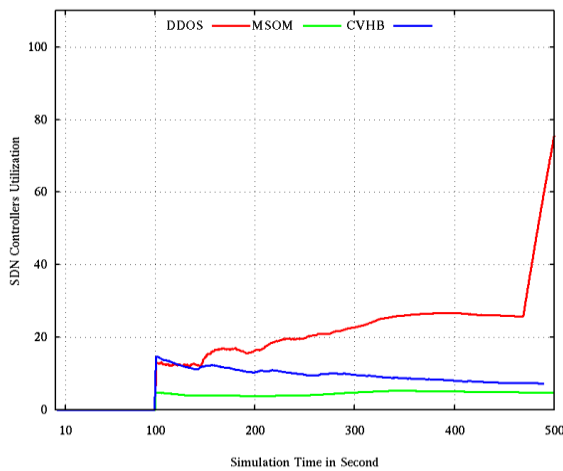


Figure 12. SDN controller analysis

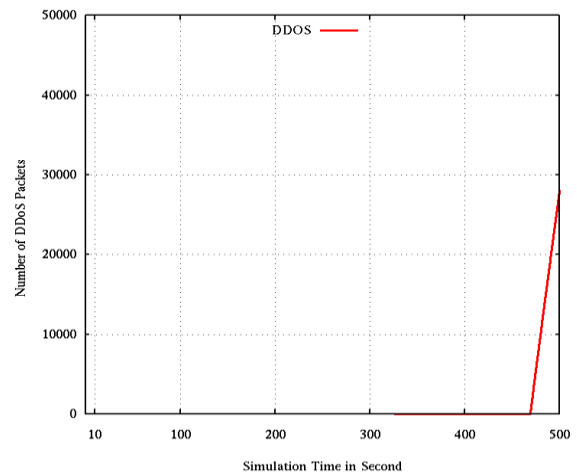


Figure 13. DDoS packets flooding capture

5. CONCLUSION

The vehicles on the road continuously exchange traffic information in VANET. Nowadays, traffic monitoring and control on roads is difficult because high vehicle densities affect vehicle performance, increase unnecessary road delays, and invite the possibility of traffic jams. A VANET is capable of controlling and managing traffic, but some issues, such as the detection of traffic information loss due to the presence of attackers, do not have immediate solutions. The proposed CVHB approach focuses on the header format changing during the communication of the attacker vehicle with normal vehicles. The sequence number field in the header changes frequently, and the rest of the fields' status is also not normal. The results show that there is an increment in packet loss and routing load in the network significantly if the DDoS attacker is present. The network is protected by the proposed CVHB technique through a self-organized, fully distributed, and localized procedure. The CVHB approach shows a 3 ms less delay as compared with the MSOM approach. Utilization: The attacker has infected 50% of the network performance, but it is also affected by the remaining performance. In the presence of attackers, the CVHB security scheme outperformed the MSOM approach in VANET, with a 17% improvement. The drop percentage is only 3% after detection and prevention. The DDoS attacker behavior is common for all connected vehicles. Due to the change in the header format, users frequently call the CVHB to resolve that problem. So, in the future, it proposes a fuzzy technique to detect the attacker. We

will use fuzzy rules to detect presence of attackers in the VANET and consider some important measurements when developing fuzzy rules for a secure VANET.

APPENDIX

Table 1. Previous work description with limitations and further enhancement

Ref. No.	Author and year	Work done	Limitations	Performance evaluated	Further enhancement or suggestions
[16]	Al-Mehdhara and Ruan	Proposed a multi-layered self-organizing map (SOM) by using supervised and an unsupervised learning technique in this module. The proposed model is a distributed, real-time VANET-SDN-based detection and mitigation method.	DDoS attacker vehicle flooding detection is missing and datasets are used to train the network, but for communication record of VANET, nodes continuously change location and want traffic status information.	PDR, throughput, delay, drop ratio, attacker reaction time and CPU utilization.	Attacker Infection gives information of unwanted packets in network. No need to evaluate reaction time in case of active attackers
[17]	Karthikeyan and Usha	Proposed security scheme for low-rate and high-rate DDoS attacks.	Similar types of behavior are detected only and reinforcement learning rules are not clear for normal and malicious packets.	Only attacker detection mentioned no new prevention technique proposed.	It is possible to improve detection rate by fixed the resource consumption. It is better for focus on packets receiving.
[18]	Turkoglu <i>et al.</i>	Machine learning classifier was proposed for detecting DDoS attacks in SD-VANETs that is supported by selection of features from the dataset and hyperparameter tuning of classifier models	Efficient traffic information related improvements are missing and the performance of the maximum relevance — minimum redundancy (MRMR) with Bayesian optimization cannot be compared with other techniques.	Measure Accuracy (%) Sensitivity (%) Specificity (%) F1-Score (%) of support vector machine (SVM), K-nearest neighbor (KNN) and decision tree (DT). Evaluated	If we run simulation then a large file creates and use other Aho Weinberger Kernighan (AWK) for required performance. If possible, to evaluate the receiving percentage.
[19]	Soni and Chandravanshi	Proposed a mechanism for security to locate an attacker's vehicles, which depends on network traffic statistics and focus on traffic status packets dropping.	The power protect data manager (PPDM) scheme enhances overhead due to checking high sequence number entries continuously in network and an attacker/s dropped information that was missing in the research.	Throughput, PDR, packets drop percentage and delay.	Black hole attacker detection at the receiving end gives better security. It can be possible to evaluate only attacker infected packets.
[20]	Palaniswamy <i>et al.</i>	Proposed a protocol suite includes protocols for driver authentication, vehicle to infrastructure (V-to-I) and vehicle to vehicle (V-to-V) key exchanges, information exchange, offline password reset, and vehicle complaint.	How possible to separate groups of vehicles which are moving in different directions and Vehicles performance is judged by their average speed, not by actual speed. why?	Evaluated protocol exchanging messages (PEM), and average key dissemination time (AKD) in different scenarios.	It can be possible to evaluate packets receiving at receiver end. Apply two checks on suspicious vehicles.
[21]	Wang <i>et al.</i>	Proposed a hybrid device to device message authentication (HDMA) technique for 5G-enabled VANETs that employs a one-of-a-kind group signature-based technique for mutual authentication between vehicle-to-vehicle (V2V) communication.	A large proportion of traffic information packets are dropped. So how to distinguish that the packet drop is because of attacker drop measured is due to other reason and if the platoon fails at the initial level, further security will be ineffective against attackers.	Multiple request Overhead, Loss ratio, OBU overhead.	They can evaluate the flooding information of the attacker. 5G utilization is not clear in attacker detection.
[22]	Krudyshchev <i>et al.</i>	Proposed a swarm-based technique for identifying routing assaults on VANET networks. This technique is based on the intelligent water droplets (IWD), and also the confidence model is employed.	The bandwidth and delay of a trust-based method are important considerations. Trust is based of set limits but reason behind the limits may be attacker or may not be. So, test probability of success.	PDR, Throughput and delay is evaluated. Use of swan intelligence utilization is not clear.	The number of malicious nodes is fixed and compare the performance with any existing scheme.

Table 1. Previous work description with limitations and further enhancement (*Continue*)

Ref. No.	Author and year	Work done	Limitations	Performance evaluated	Further enhancement or suggestions
[23]	Hu <i>et al.</i>	Proposed a hybrid architecture made up of autos, trust authority (TA), a server, RSUs, and a that allows for computation of integrity rating and feedback storage	Routing performances are not evaluated and trust-based scheme are very common.	PDR, trust score comparison of normal and malicious vehicles.	Worked on multiple attackers but behavior of both of the attackers is same. Work on different behavior attacker will be complex.
[24]	Karimireddy and Bakshi	Proposed a hybrid key cryptography technique for safety to protect communication of vehicles in ad hoc car networks. This security architecture uniquely built to defend a unique vehicle communications security approach.	Both methods are outdated and increase overhead in a dynamic network. There is no novelty in the work. Only a small comparison is proposed. Type of attacker information is missing. .	Mentioned comparison of Rivest-Shamir-Adleman (RSA) and advanced encryption standard (AES) algorithm. Evaluate success ratio also.	A new security scheme can develop for secure the network and which is based for node id and dropped data packets.
[25]	Bhoi <i>et al.</i>	Proposed a stable routing protocol multi-agent reinforcement learning based routing protocol (RRP) is used to secure messages between the source and destination from hole formation attacks. RRP consists of a recovery module, attacker node or normal node security to protect from malicious driver.	If the goal of the signature generation system is to make communication easier, then accurate message acceptance rules or standard communication rules should be used.	PDR and delay only evaluated.	PDR and delay show degradation when vehicle density increases. For improving performance fast detection mechanism required.
[26]	Tzeng <i>et al.</i>	Proposed an identity-based batch verification (IBV) scheme for V to V and V to RSU to assure message integrity, privacy, anonymous, authentication and traceability.	The multiple key exchange method multiple verifies the users means extra overhead in network.	Delay and packet receiving analysis measured.	Not focusing on malicious node header field information. By header information easily detection is possible.

REFERENCES




- [1] M. Rath, B. Pati, and B. K. Pattanayak, "An overview on social networking: Design, issues, emerging trends, and security," in *Social Network Analytics*, Elsevier, 2019, pp. 21–47.
- [2] Y. Qian and N. Moayeri, "Design of secure and application oriented VANETs," in *VTC Spring 2008 - IEEE Vehicular Technology Conference*, May 2008, pp. 2794–2799, doi: 10.1109/VETECS.2008.610.
- [3] G. Soni, K. Chandravanshi, A. S. Kaurav, and S. R. Dutta, "A bandwidth-efficient and quick response traffic congestion control QoS approach for VANET in 6G," In: *Saini, H.S., Sayal, R., Govardhan, A., Buyya, R. (eds) Innovations in Computer Science and Engineering*. Lecture Notes in Networks and Systems, Springer, Singapore, vol. 385, pp. 1–9, 2022, doi: 10.1007/978-981-16-8987-1_1
- [4] C. Sommer, A. Schmidt, Y. Chen, R. German, W. Koch, and F. Dressler, "On the feasibility of UMTS-based traffic information systems," *Ad Hoc Networks*, vol. 8, no. 5, pp. 506–517, Jul. 2010, doi: 10.1016/j.adhoc.2009.12.003.
- [5] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011, doi: 10.1109/JPROC.2011.2132790.
- [6] S. Malik and P. K. Sahu, "A comparative study on routing protocols for VANETs," *Heliyon*, vol. 5, no. 8, Aug. 2019, doi: 10.1016/j.heliyon.2019.e02340.
- [7] T. Nadia, A. Mourad, M. Hamouma, and K. Hamoudi, "A survey on vehicular ad-hoc networks routing protocols: classification and challenges," *Journal of Digital Information Management*, vol. 17, no. 4, pp. 227–244, Aug. 2019, doi: 10.6025/jdim/2019/17/4/227-244.
- [8] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2377–2396, 2015, doi: 10.1109/COMST.2015.2440103.
- [9] G. Soni and K. Chandravanshi, "A novel defence scheme against selfish node attack in MANET," *International Journal on Computational Science & Applications*, vol. 3, no. 3, pp. 51–63, Jun. 2013, doi: 10.5121/ijcsa.2013.3305.
- [10] G. Soni and K. Chandravanshi, "Security scheme to identify malicious maneuver of flooding attack for WSN in 6G," in *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, Aug. 2021, pp. 124–129, doi: 10.1109/SPIN52536.2021.9566066.
- [11] S. D. Kebede, B. Tiwari, V. Tiwari, and K. Chandravanshi, "Predictive machine learning-based integrated approach for DDoS detection and prevention," *Multimedia Tools and Applications*, vol. 81, no. 3, pp. 4185–4211, Jan. 2022, doi: 10.1007/s11042-021-11740-z.
- [12] A. S. Kaurav and S. R. Dutta, "Detection and prevention from different attacks in VANET: A survey," *Journal of Physics: Conference Series*, vol. 2040, no. 1, Oct. 2021, doi: 10.1088/1742-6596/2040/1/012017.
- [13] S. Kumar, K. D. Narayan, and J. Kumar, "Qualitative based comparison of routing protocols for VANET," *Journal of Information Engineering and Applications*, vol. 1, no. 4, pp. 13–17, 2011.
- [14] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, "Classification of security attacks in VANET: A review of requirements and perspectives," *MATEC Web of Conferences*, vol. 150, Feb. 2018, doi:

A comprehensive verification of the header format and bandwidth utilization ... (Arun Singh Kaurav)




- 10.1051/mateconf/201815006038.
- [15] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security analysis of vehicular Ad Hoc networks (VANET)," in *2010 Second International Conference on Network Applications, Protocols and Services*, Sep. 2010, pp. 55–60, doi: 10.1109/NETAPPS.2010.17.
- [16] M. Al-Mehdhar and N. Ruan, "MSOM: Efficient mechanism for defense against DDoS attacks in VANET," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/8891758.
- [17] H. Karthikeyan and G. Usha, "Real-time DDoS flooding attack detection in intelligent transportation systems," *Computers and Electrical Engineering*, vol. 101, Jul. 2022, doi: 10.1016/j.compeleceng.2022.107995.
- [18] M. Türkoğlu, H. Polat, C. Koçak, and O. Polat, "Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection," *Expert Systems with Applications*, vol. 203, no. 3–4, p. 117500, Oct. 2022, doi: 10.1016/j.eswa.2022.117500.
- [19] G. Soni and K. Chandravanshi, "A novel privacy-preserving and denser traffic management system in 6G-VANET routing against black hole attack," in *Sustainable Communication Networks and Application*, 2022, pp. 649–663.
- [20] B. Palaniswamy, S. Camepe, E. Foo, L. Simpson, M. A. Rezazadeh Bae, and J. Pieprzyk, "Continuous authentication for VANET," *Vehicular Communications*, vol. 25, Oct. 2020, doi: 10.1016/j.vehcom.2020.100255.
- [21] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5071–5080, Aug. 2021, doi: 10.1109/TITS.2020.3013928.
- [22] V. Krundyshev, M. Kalinin, and P. Zegzhda, "Artificial swarm algorithm for VANET protection against routing attacks," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, May 2018, pp. 795–800, doi: 10.1109/ICPHYS.2018.8390808.
- [23] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017, doi: 10.1109/TVT.2016.2565001.
- [24] T. Karimireddy and A. G. A. Bakshi, "A hybrid security framework for the vehicular communications in VANET," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar. 2016, pp. 1929–1934, doi: 10.1109/WiSPNET.2016.7566479.
- [25] S. K. Bhoi, R. P. Nayak, D. Dash, and J. P. Rout, "RRP: A robust routing protocol for vehicular ad hoc network against hole generation attack," in *2013 International Conference on Communication and Signal Processing*, Apr. 2013, pp. 1175–1179, doi: 10.1109/iccsp.2013.6577241.
- [26] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017, doi: 10.1109/TVT.2015.2406877.
- [27] M. Greis, "Tutorial for the network simulator 'ns'," *isi.edu*, accessed Oct. 01, 2023. [Online], Available: <http://www.isi.edu/nsnam/ns/tutorial/index.html>. ()

BIOGRAPHIES OF AUTHORS



Arun Singh Kaurav    is a research scholar in the Department of CSE, Koneru Lakshmaiah Education Foundation, Hyderabad. He obtained bachelor's degree from Sriram College of Engineering and Management, Gwalior and a master's degree from RKDF IST Bhopal. He has published articles in Scopus indexed journals. He can be contacted at email: arunsingh@klh.edu.in.



K. Srinivas    currently working as professor in the Department of CSE KL University Hyderabad Campus. He has about 22 years of experience in teaching and research. He obtained bachelor's and master's degrees from Osmania University Hyderabad. He obtained a doctoral degree from Rayalaseema University, Govt of Andhra Pradesh. He is an accredited faculty for AWS academy and CISCO networking academy. He has published research articles in various reputed journals like Springer IEEE and Elsevier with Q1 rank. His interested research areas are MANETS, cloud computing, artificial intelligence (AI), and machine learning (ML). He can be contacted at email: srirecw9@klh.edu.in.