Journal of Computer Science

Original Research Paper

Efficient Detection and Mitigation of Rushing Attacks in VANETs Using RAID: A Novel Intrusion Detection System

Vamshi Krishna Kapu and Ganesh Reddy Karri

School of Computer Science and Engineering, Faculty, VIT-AP University, Guntur, India

Article history
Received: 16-06-2023
Revised: 21-07-2023
Accepted: 01-08-2023

Corresponding Author:
Vamshi Krishna Kapu
School of Computer Science and Engineering, Faculty, VIT-AP University, Guntur, India
Email: vamshikrishna.20phd7088@vitap.ac.in

Abstract: The vehicle manufacturing hub has evolved over the last decade with the emergence of self-driving vehicles and human-driven vehicles that use the concept of Artificial Intelligence (AI). Vehicular Ad Hoc Network (VANET) is a subset of Mobile Ad Hoc Network (MANET) that allows vehicles to communicate with one another and the Road Side Unit (RSU). VANET has been a game changer with features such as accident prevention, real-time traffic, route predictions, discovering an alternate route, alert notifications, safety, and security. VANET systems are distinguished by their ability to transmit critical safety information in real-time, even when the network's topology is constantly changing. With the lifesaving features of VANET comes a disadvantage that can risk the drivers' security and privacy through various attacks on the network. Intruders can steal data, drop data packets and modify, insert, or delete data when it is transmitted between vehicles. To address the mentioned data communication issues as well as various attacks in the VANET network, the authors propose an Intrusion Detection System (IDS) Rushing Attack Intrusion Detection (RAID), a novel framework that performs the detection of rushing attacks in vehicular networks. According to the performance analysis, the proposed framework RAID meets a wide range of security requirements while requiring less communication and storage. The study's findings were found to be more efficient.

Keywords: VANET, V2V, V2X, Attacks, RAID

Introduction

Vehicles are proliferating on the roads at an alarming rate, with 8 out of 10 people owning one, resulting in an increase in the number of accidents year by year; every 25 seconds on average, one person's life is lost, with an estimated 1.2 million per year (Ibrahim *et al*., 2021). Accidents can occur for one of the following three reasons: (1) Malfunction of the vehicles; (2) Careless drivers; and (3) Intruders hacking the vehicle. As a result, the automobile industry has begun designing vehicles with advanced features embedded with Artificial Intelligence (AI). (Younas *et al*., 2022; Ma *et al*., 2020). VANETs are a type of wireless network that self-organizes and communicates between clusters of vehicles, with each vehicle acting as a node. VANETs are related to MANETs and are built using MANET principles (Sharma *et al*., 2022; Remya Krishnan and Arun Raj Kumar, 2022). For data transmission between vehicles, VANET uses three modes of transmission. (1) Vehicle-to-Vehicle (V2V) communication occurs when two or more vehicles communicate with one another. (2) Vehicle to Infrastructure (V2I), in which vehicles pass information to nearby Roadside Units (RSU) and from RSU to targeted vehicles; (3) Vehicle to Vehicle/RSU/Both (V2X), in which vehicles communicate directly to vehicles, through RSU, or both (Yogarayan *et al*., 2020; Tami *et al*., 2021). Vehicles must be equipped with the following hardware and software components to perform the above-mentioned modes of transmission: (1) Road Side Unit (RSU) (2) Application Unit (AU) (3) On Board Unit (OBU) (Al-Shareeda *et al*., 2020; Maria *et al*., 2021). Since communication between vehicles takes place over a wireless channel, privacy and security are critical, as there is a high risk of intruders disrupting the flow of communication, which can lead to substantial dangers such as car accidents, traffic jams, false information broadcasting, and communication data

theft by attackers. (Sharma *et al*., 2022; Aljabry and Al-Suhail, 2021). To counter intruder attacks before they steal or broadcast false information, a strong authentication scheme must be employed so that vehicles are authenticated before entering the network (Wang *et al*., 2021; Cheng *et al*., 2021). There is a possibility that an attacker will disguise himself as a validated vehicle and bypass the authentication scheme to get into the network; in such a scenario, intruders must be unable to read, insert, or modify the data (Di and Wu, 2022; Xu *et al*., 2019; Al-Shareeda and Manickam, 2022; Mei *et al*., 2022). To do so, all vehicles must encrypt the information before transmitting it so that only vehicles with the decryption key can access it, leaving the intruder roaming the network empty-handed (Ahmed *et al*., 2022; Khalid *et al*., 2021). An intruder in the network can pose a threat at any time; therefore, there should be a mechanism in place to detect the intruder and prevent him or her from roaming freely in the network (Azam *et al*., 2021; Jalali *et al*., 2017). Figure 1 depicts a VANET communication model wherein vehicles communicate with one another (V2V), with roadside infrastructure (V2I), and with any other vehicles (V2X).

Related Work

Many authors worked on and published frameworks for authentication, key management, and Intrusion Detection Systems (IDS), (Table 1) such as the authors (Kumar Pulligilla and Vanmathi, 2023), who presented the RBSLO framework based on RideNN that increased the precision and reduced the time required to identify the intruder. Authors (Ma *et al*., 2020) presented a decentralized key management mechanism that performs key registration, updating, and revocation and protects against well-known attacks. The proposed system improves storage, communication, computation, and latency performance. Authors (Paranjothi and Atiquzzaman, 2021) presented a technique where OBU was used to trace attacker vehicles using the F-rouND framework, which resulted in less data processing and an improved detection rate. The authors (Shawky *et al*., 2023) presented key management that improves network security and privacy. The work done makes use of the ML K Means algorithm to improve vehicle communication and performance. Authors (Ercan *et al*., 2021) proposed SP-CIDS that were trained using ML algorithms for data privacy and achieved 96.94% accuracy. The authors (Bangui *et al*., 2021a) presented a novel IDS for detecting false positions that resulted in better performance compared to previous models. Authors (Raja *et al*., 2020) proposed an IDS that is private and secure, for the development of IDS a distrusted ML and (ADMM) methods are used that detects malicious activity in the system and improves storage and performance of the proposed framework.

Routing in VANET

Accidents, traffic flow, the quickest routes, alternate routes, petrol stations, motels, and hospitals are all examples of critical information that is transmitted for safety and general needs (Lin *et al*., 2022; Alshudukhi *et al*., 2020). Routing is very critical and essential in VANET (Table 2) for vehicles to communicate with one another and RSUs. Establishing and maintaining routes between V2V, V2I, and V2X for data collection and information transmission requires VANET routing protocols that are distinct from MANET protocols (Rahnama *et al*., 2016; Rao *et al*., 2022; Bharti *et al*., 2022). Figure 2 depicts the classification of protocols used by VANET for routing information and (Fig. 3) depicts additional sub-classifications of routing protocols.

A. Geo-Based Routing

Geocast routing is essentially a type of location-based multicast routing that seeks to transmit information from an origin vehicle to every other vehicle within a defined geographical location known as a zone (Dutta and Thalore, 2017).

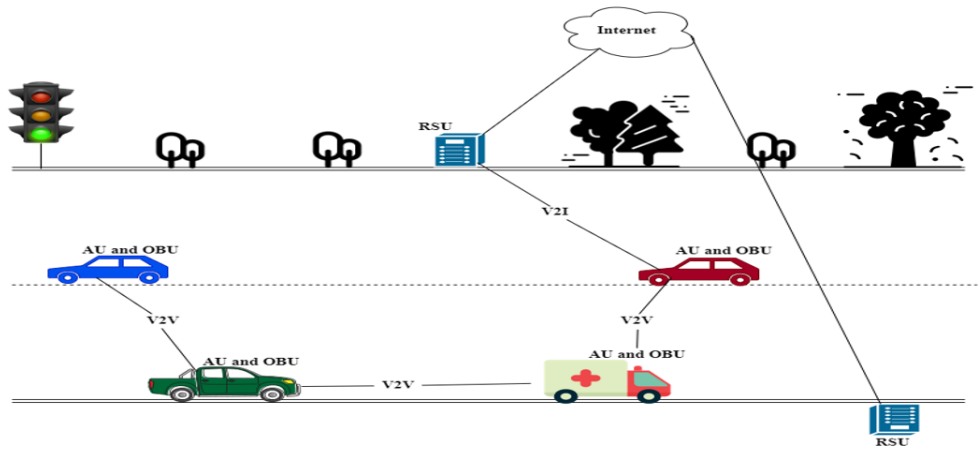


Fig. 1: VANET communication model

Table 1: A Summary of existing security systems

Citation	Algorithm/Technique used	Issue addressed	Limitations/Future research
Kumar Pulligilla and Vanmathi (2023)	Rider-based Neural Network (RideNN) and Rider-based Sea Lion Optimization (RBSLO)	Computation time and precision	Use of other datasets to decrease the time needed to compute
Ma *et al*. (2020)	DB-KMM	DDOS, internal attacks and collision attacks, storage	Need to address external attacks, and use of another key management methods
Paranjothi and Atiquzzaman (2021)	Fog computing-based on rogue node detection (F-RouND)	Detection of rouge vehicles	Need to address other attacks such as DDOS, Sybil using rouge method
Shawky *et al*. (2023)	Clustering, Cross layer scheme, RFID and K means	Security, privacy, and faster communication	Suspected vehicles can use fake credentials
Ercan *et al*. (2021)	ML-KNN, RF, and Ensemble Learning (EL)	Data privacy, position attacks, misbehavior vehicles	Does not support reaction method. Various other attacks are not covered
Bangui *et al*. (2021a)	RF, Posterior with corsets	False position and DOS attacks	Must use other methods to improve performances
Raja *et al*. (2020)	DML, ADMM, and DP	Privacy and security	Use of other classifiers to improve detection

Table 2: A summary of VANET routing protocols

Citation	Protocol/Technique used	Issue addressed	Disadvantages/Future research
Hota *et al*. (2022)	OLSR	Optimizes routing and propagation models for reliable packet dissemination	Testing Manhattan, Random-way point, gaussian, as well as of some modern routing protocols
Benmir *et al*. (2019)	GPSR	Reduce packet loss	Using other protocols to increase the packet delivery ratio
Yang *et al*. (2018)	Maxduration-Minangle GPSR (MM-GPSR)	Cumulative communication duration to select the next hop and minimum angle for optimal next hop	Path redundancy and performance increase
Cheng *et al*. (2010)	GeoDTN+Nav	Delivery of packets in divided networks	Moving destination, privacy issue
Shah and Kasbe (2021b)	AOMDV	Rushing attack	Use other protocols
Remya Krishnan and Arun Raj Kumar (2022)	AODV, OLSR	Gray hole, and black hole assaults	Hop count based gray hole and Black hole assaults
Sabbagh and Shcherbakov (2021a)	DSR, AODV	Most affected protocol when a black hole attack is performed	Compare other protocols

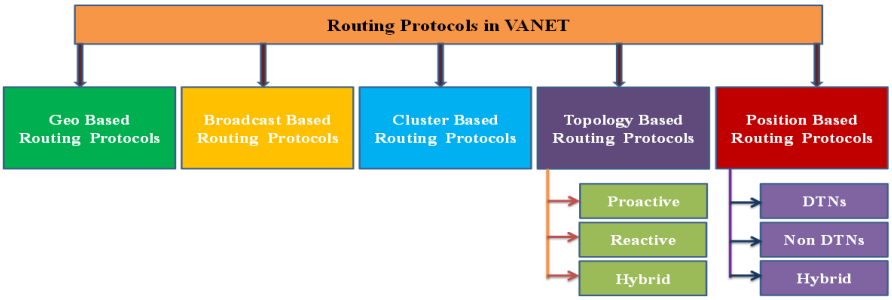


Fig. 2: Classification of VANET routing protocols

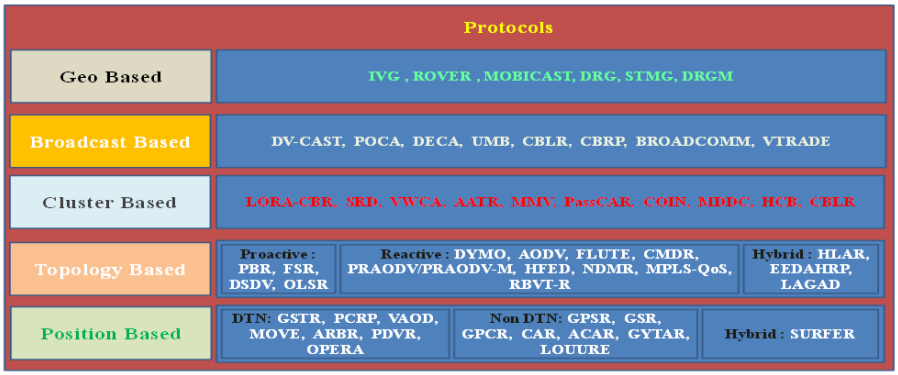


Fig. 3: Sub-classification of routing protocols in VANET

B. Broadcast-Based Routing

Broadcast routing is a straightforward method of flooding messages with other vehicles in groups. This procedure ensures that the message is delivered to all vehicles (Sarker *et al*., 2020; Kermani and Azarderakhsh, 2018). Flooding ensures packet delivery by ensuring that every node in the network receives the packet. The disadvantage of this routing scheme is that it is expensive (Shah and Kasbe, 2021b).

C. Cluster-Based Routing

Clustering-based routing selects one vehicle out of each cluster as the Cluster Head (CH), whose basic task is to manage other cluster members. A boundary node is a node that is located between two or more clusters (Sindhwani *et al*., 2022).

D. Topology Base Routing

To forward packets, topology-based routing employs link information. Prior to transmission, information is acquired and maintained in tables and the contents of the tables are used to establish the path (Stalin *et al*., 2018; Shah and Kasbe, 2021a). There are three types of topology protocols: Proactive, reactive, and hybrid.

E. Position-Based Routing

Geographic routing is another name for it and it uses the locations of the source vehicle, target vehicle, and neighboring vehicles; where each vehicle uses the GPS service to determine its location (Anastasova *et al*., 2021). Source vehicle (S) transmits packets to all of its neighbors and includes the Target vehicle's (T) location in the packet header to aid in information transmission to the target vehicle. There are additional classifications: Delay Tolerant Networks (Non-DTNs) and Delay Tolerant Networks (DTNs) (Shah and Kasbe, 2021a).

Detection Mechanisms in VANET

Nearly every industry is experiencing a trend toward privacy and security. It is a crucial VANET component that has a direct bearing on both financial and personal problems (Jiang *et al*., 2021). Minor breaches of privacy and security on the VANET could result in massive costs. (Ajjaj *et al*., 2022; Dhanaraj *et al*., 2022; Malik *et al*., 2022). Researchers worldwide focus much of their efforts on enhancing security and creating novel approaches and algorithms for identifying different known and unknown VANET attacks (Sajini *et al*., 2023; Bangui *et al*., 2021b; Bensaid and Boukli-Hacene, 2019; Theodore *et al*., 2021; Canto *et al*., 2023). The remaining paragraphs in this section provide a quick overview of the detection techniques proposed by the various authors who have worked to develop technologies that can detect security leaks in VANETs early on.

Materials

Our study makes use of Road Side Unit (RSU), Application Unit (AU), and On-Board Unit (OBU) devices, along with more than 50 vehicles moving in a random direction. We have extracted live traffic using OpenStreetMap, which creates an .osm file, for the purpose of rushing attack detection in VANET. This .osm file is used as the input for SUMO, an application that simulates traffic and creates trace files (.tcl files), which are used in the network simulator NS2 together with the necessary parameters (Fig. 5) and (Fig. 8). In co-labs, the output is produced using the generated trace files. (Table 3-4) summarizes the simulation parameters.

Table 3: A summary of existing VANET attacks detection technique

Citation	Technique used	Advantages	Disadvantages/Future research
Al-Shareeda *et al*. (2020)	Deep Q-learning network	Better performance and higher detection rate	Virtual simulation, classifier and father extraction
Liang *et al*. (2021)	Random Forest and posterior detection	Accuracy and Efficiency	Improve detection quality when compared to other ML-based IDS
Cheng and Liu, (2020)	Collaborative Trust Index (CTI)	Includes all potential attacks types	Extend the work in the direction of intrusion prevention systems
Bangui *et al*. (2021b)	The hybrid routing protocol (NIHR)	Improve the performance of network caches and content lookups	A predefined angle must be carefully set
Sabbagh and Shcherbakov (2021b)	DDOS detection based on fuzzy logic	90% precision and true negative rate	Improve accuracy using other advanced techniques
Mchergui *et al*. (2022)	Neural Network, Edge AI, Residual Convolutional	Automatic detection of the road irregularities and data transmission to surrounding vehicles	The future may bring about entirely new types of road irregularities and difficult roads
Bakkoury (2021)	Nearest neighbor and Parzen window method	Accuracy improved	Use of more ML techniques to improves accuracy
Xu *et al*. (2020)	IDS-based deep learning	Effectiveness and efficiency	Use of other advanced techniques
Aboelfottoh and Azer (2022)	EIDS. NSLKDD data, regression algorithm	Increase the efficiency and precision percentages by 84 and 90%	A novel feature selection strategies for the efficient forecasting framework of the machine learning method

Table 4: Parameters

No.	Parameters	Values
1	Simulation time (SUMO)	400 s
2	Simulation time (NS3)	60, 80, 120, 150 (s)
3	MAC	IEEE 802.11p
4	Routing protocols	AODV, DSR, DSDV, AOMDV
5	Vehicle speed	Random
6	Channel Type	Wireless
7	Number of vehicles	70-80
8	Packet size	200 bytes
9	Data packet type	CBR
10	Transmission range	250m
11	Speed	40 m/s
12	Number of RSUs	5
13	Simulation environment	1000×1000m
14	Frequency	2.4 GHz
15	Transmission power	33dbm

Methods

This section elaborates on the proposed framework, Rushing Attack Intrusion Detection (RAID) to identify the intruder in the network (the detection phase), which results in providing countermeasures to delay-sensitive attacks like rushing attacks by using AOMDV as a routing protocol. The RAID structure is comprised of two stages. (1) The primary stage (2) The detection stage (Fig. 4) depicts the entire framework of RAID.

The Primary Stage

The primary stage, also known as the storage stage, is where all data is collected and stored from numerous components. Updates are classified into two sorts. For periodic updates and event updates, we use the latter, which is an event update. The primary stage includes the following components.

A. Routing Table

A routing table is a set of rules that govern where data packets are routed. A routing table contains the information needed to transmit a packet via the most direct path to its destination. Each packet contains information about its destination and origin. When a packet is received, a vehicle analyses it and compares it to the routing table entries that best fit its destination (Mozaffari-Kermani and Reyhani-Masoleh, 2009). The table then informs the vehicle on how to transfer the packet to the next hop along the network's path.

B. Data Collection and Storage, or TA (Trust Authority)

All data acquired from RSUs and vehicles is saved here, along with updated information. When an event occurs and completes the authentication and detection stages, the modified data is transmitted to the primary stage for storing or updating existing data (Ali *et al*., 2016).

C. Roadside Unit (RSU)

RSUs are fixed hardware devices that are mounted on the roadside, these units incorporate sensors, antennas, CPUs, charging connectors, and storage systems (Mathur and Jain, 2018). The RSU communicates to vehicles or other RSUs via wired or wireless means.

D. Vehicles

A set of fast-moving network nodes that communicate with one another in V2V, or hybrid mode (Sundaram *et al*., 2021). All vehicles are outfitted with an Application Unit (AU) and an On Board Unit (OBU).

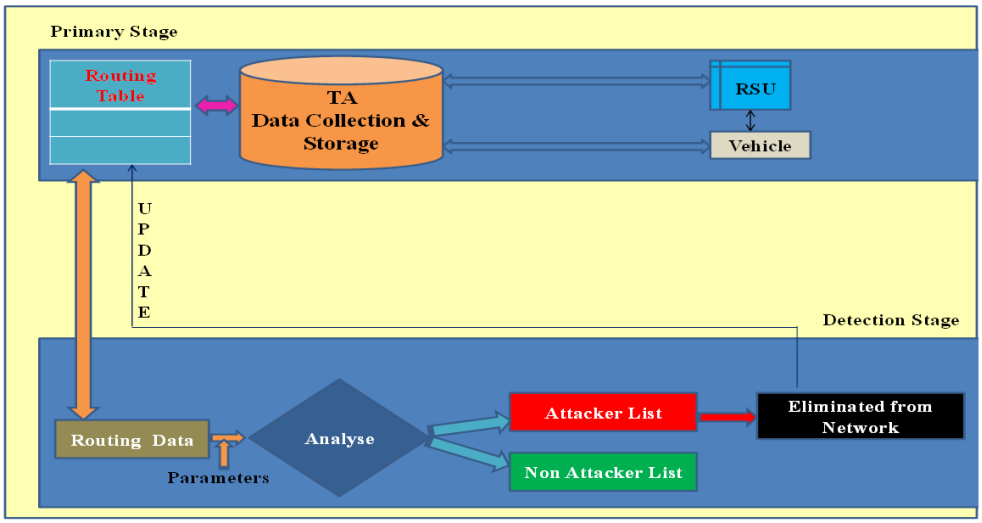


Fig. 4: RAID framework

Detection Stage

The detection step is for detecting malicious vehicles inside the network; these vehicles may have stolen or forged other vehicles' credentials and entered the network; (Fig. 5) while inside the network, these vehicles inflict damage to network operations (Malik *et al*., 2022; Sharma *et al*., 2022; Dubrova *et al*., 2023). The delay parameters listed below are considered and used as one of the basic inputs for each vehicle in our proposed algorithm, along with other inputs.

Basic Parameters

Total delay equation:

$$V_{delay} = v_{proc} + v_{queue} + v_{vrans} + v_{prop}$$

Processing delay equation:

$$V_{proc} = packet\ processing\ delay$$

Transmission delay equation:

$$v_{trans} = L / R$$

Queuing delay equation:

$$v_{queue} = v_{trans} * l_{queue}$$

Propagation delay equation:

$$v_{prop} = d / s$$

Generating Rushing Attack Scenario

A rushing attack is a type of advanced attack that employs the flood duplicate suppression strategy. In a rushing assault, the attacker receives the REEQ and does not wait for any form of delay; instead, the REEQ packet is transferred very quickly to the destination, fooling it into thinking it is the quickest path and ignoring the next incoming packets (Mozaffari-Kermani and Reyhani-Masoleh, 2011; Bayat-Sarmadi *et al*., 2013). To evaluate the performance of our RAID system, we simulate a rushing assault on the network and record the network transmission with and without a rushing attack. Our implementation is done in NS3, utilizing object-oriented programming and the object tool command language. Our simulation consists of five RSUs and 80 vehicles, four of which are attackers. Our RAID mission is to locate and remove vehicles that drop packets from the network.

Algorithm 1: Rushing attack detection algorithm

Input: Basic parameters, threshold, Timestamp(ts)

Step 1: When the Source Vehicle (SV) wishes to interact with a Destination Vehicle (DV), a path must be constructed from SV to DV. SV broadcasts a Route Request (RREQ) packet to discover the route to the DV.

Step 2: The reception of the RREQ packet is confirmed by neighboring vehicles. When an RREQ packet is received, intermediate vehicles (InVs) update the timestamp and geographical position of the packet for as long as the packet is valid.

Step 3: When the DV accepts the RREQ packet, it computes the i^{th} InVs delay along the path:

$$v^i_{delay} = timestamp\ at\ v^{i+1} - timestamp\ at\ v^i$$

i^{th} intermediate vehicle propagation delay:

$$v^i_{prop} = \frac{distance\ between\ v^i\ and\ v^{i+1}}{propagation\ speed}$$

Any vehicle minimum transmission delay:

$$v^i_{trans} = \frac{RREQ\ packet\ size}{handwidth}$$

//After calculation of $v^i_{delay}, v^i_{prop}, and\ v^i_{trans}\ delays$

```
for all paths at D
{
    p_t^i < 0          //Initially the trust in its path
  for all intermediate nodes in a pa<th
{
   if (v_delay^i ≤ v_prop^i + v_trans^i)
     {
       i^th vehicle Considered a rushing attacker
       p_t^i = −1          //path trust is negative
      Discard the path
     }
    else if (n_delay^1 ≤ d_pro + d_trns + d_pros)
      {
       p_t^i = 0.5 + p_t^i
      }
    else
      {
       p_t^i = 1 + p_t^i
     }
}
 p_tavg^i = p_t^i / number of InVs (intermediate vehicles)
}
```

Step 4: DV selects the two reverse paths which have a max of $\{p^i_{tavg}\}$ value among all different paths and sends Reroute reply (RREP) packets to SV. And does not send RREP packets through a path that has min delay and discards it.

Step 5: Out of two paths, SV selects any one of the paths randomly for data transmission

Step 6: Update the dropped path consisting of the attacker and attacker details back to the routing table

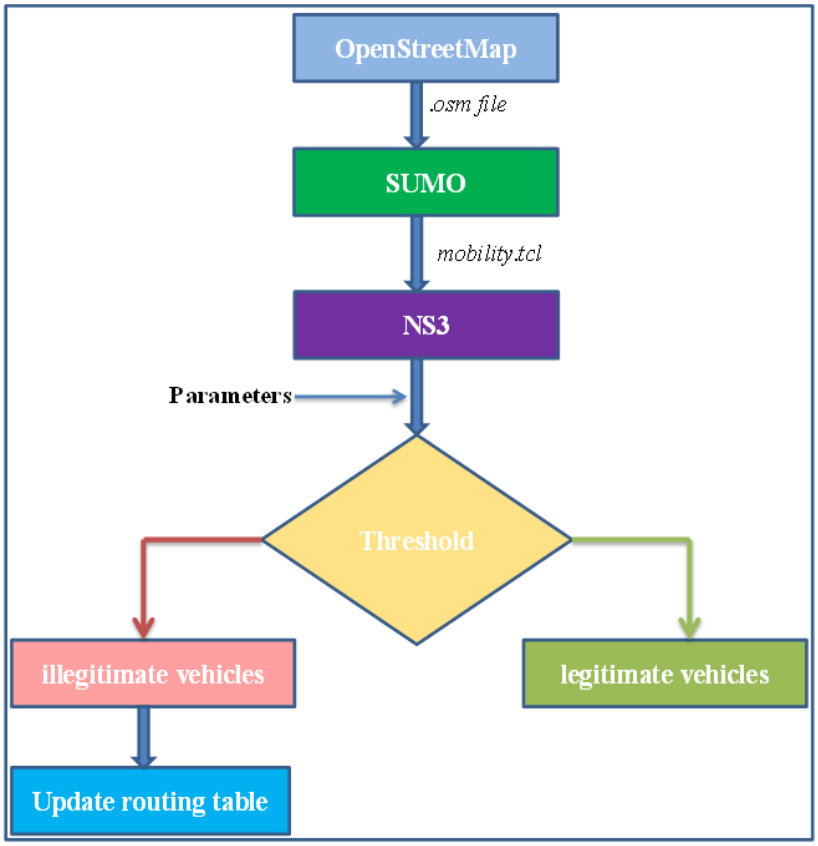


Fig. 5: Detection stage flow diagram

Dynamic Threshold

To counter the problem of a rushing attack, RAID employs a dynamic threshold value (α). An intermediate vehicle (I), when it receives a packet, is directed to verify and calculate the delays (5.2.1), update the REEQ, and retransmit to the next intermediate vehicle until it reaches the destination (Hota *et al*., 2022; Berzati *et al*., 2023). The illegitimate vehicle in the network, on receiving a REEQ packet, does not verify or update the delays; in fact, it does not follow any rules; the attacker immediately, without delaying, retransmits the packet to the next Intermediate Vehicle (Inv) to ensure that the destination vehicle receives this packet first and concludes that this is the shortest route and the destination vehicle acknowledges an RREP packet back to the source using this path. The calculation of α value is shown below:

1) After receiving acknowledgment of RREP packets from the Destination Vehicle (DV), the Source Vehicle (SV) sorts them in Sequential Order (SO) and stores them in the Routing Table (RT)
2) SV computes the average of all {RREP (SO)} packets with the difference of the last RREP (SO)
3) (α) is computed as follows:

$$\alpha=\begin{pmatrix} RREP_1(SO)-RREP_n(SO)-(RT) \\ +RREP_2(SO)-RREP_n(SO)-(RT) \\ +RREP_n(SO)-RREP_n(SO)-(RT) \end{pmatrix}+n$$
$$(SO(RREP_n))-(SO(RT))$$

$$\frac{\Sigma_{j=1(SO(RREP1))-(SO(RREPn))-(SO(RT))}^{i}}{n}+n \qquad (1)$$
$$(SO(RREP_n))-(SO(RT))$$

4) To determine the difference (Δ) between RREPn (SO) and RT:

$$\Delta=(SO(RREP_n))-(SO(RT)) \qquad (2)$$

5) Using the above Eqs. (1, 2) we simply the α shown in (Eq. 3):

$$\alpha=\mu(\Sigma_{j=1}^{i}SO(RREPj)-\Delta)+n\Delta \qquad (3)$$

6) SV compares each RREP (SO^n) to the calculated value (α). If the destination (SO) is greater than, the vehicle is regarded as an intruder vehicle

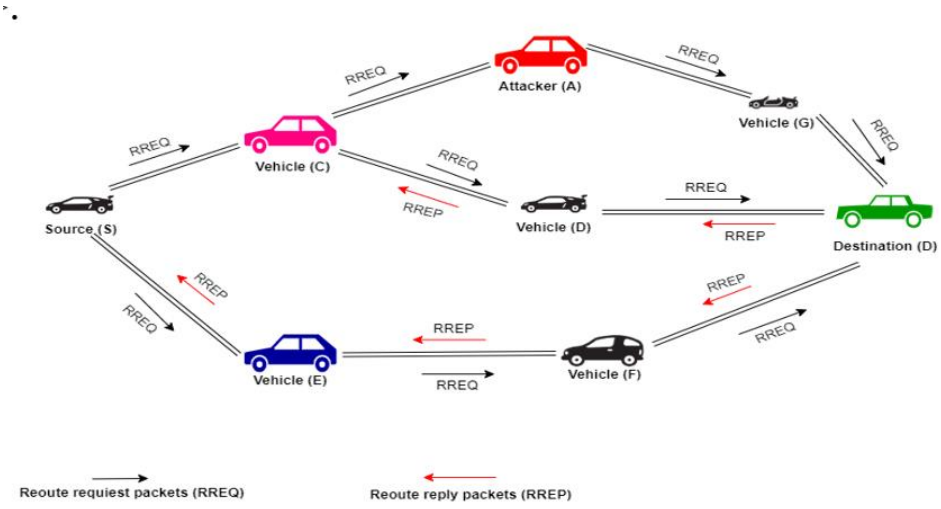


Fig. 6: Detection using AOMDV protocol

Scenario Illustration

As demonstrated in (Fig. 6) Making use of the AOMDV protocol, the Route Request (RREQ) packet is broadcasted from the Source Vehicle (SV) to the intermediate vehicles {C and E}. Intermediate vehicles {C, E} validate the Source Vehicle (SV) and Receiver Vehicle (RV) addresses, hop count, geographical locations, and timestamps and forward the packet to the next intermediate vehicle C → {A, D} and E → {F}, F → {R} A → {G}, G → {R} and D → {R}. To calculate the total delays of all vehicles, the Receiver Vehicle (RV) uses a delay rule-based algorithm the destination vehicle typically does not send Route Reply (RREP) packets through a path with the minimum delay to avoid selecting paths occupied by rushing attackers. This is because we set a dynamic threshold value, the path that falls above the threshold value are considered valid vehicles and which fall below the threshold value are considered attacker paths. By avoiding paths with the minimum delay and threshold value, the destination vehicle aims to minimize the chances of selecting paths that rushing attackers might have manipulated to make them appear more favorable. The ack (RREP) packets are then sent from those DV → SV. After SV receives the ack it selects any one of the paths randomly for data transmission. As a result, the route can now be secured, establishing a connection and transmitting data from one location to another {SV → DV}.

With the help of the delay rule-based technique we mitigate the risk of selecting compromised paths, in our work, we set the threshold value to the dynamic that keeps changing, so the rate of detecting the attacker paths is increased and the performance of detection rate is increased in comparison with the existing methods which can be clearly seen in (Fig. 10).

Results

Authentication techniques serve as the first line of defense in stopping intruders from entering the network (Yang *et al*., 2021). Even with strong authentication, intruders can still get access to the network by using forged credentials or stealing the credentials of legitimate and authenticated vehicles (Zhang *et al*., 2021; Zhou *et al*., 2022; Koziel *et al*. 2015). When an intruder joins the network using forged or stolen credentials and launches various attacks (Moni and Manivannan, 2022; Kaur *et al*., 2023), the RAID model starts to detect such unauthorized vehicles (Wang *et al*., 2019; Masruroh *et al*., 2020).

To evaluate, analyze and compare the effectiveness of the RAID, the model is built with a wide range of parameters and tools like OpenStreetMap, Sumo, and NS3 and compares the performance of the routing protocols AODV, AOMDV, DSR, and DSDV. The routing protocol employed in RAID is Ad hoc On-Demand Multipath Distance Vector (AOMDV). The advantages of AOMDV over other protocols are.

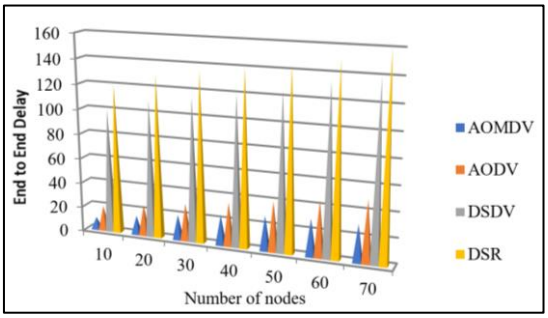
Optimal path length, multipath capability, higher throughput, the ability to search for alternate paths when a current link breaks down better routing performance; Reduced energy consumption.

Figures (7 a-c) compare routing protocols based on performance metrics.

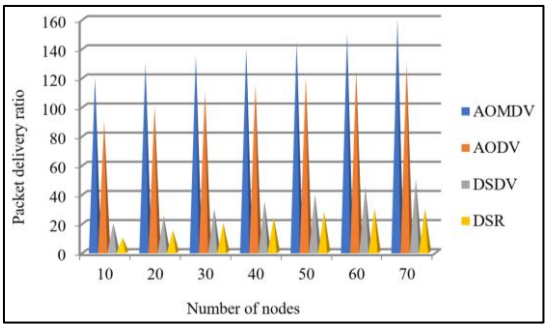
RAID Detection Probability

The main goal is to determine whether or not our RAID model can detect delay-sensitive attacks. Simulations are run to demonstrate the effect of the detection percentage. The RAID detection methodology was used for various numbers of vehicles and was monitored. Authors generate their own (self-generated) dataset that is given as input to RAID.

DOI: 10.3844/jcssp.2023.1143.1159



(a)



(b)

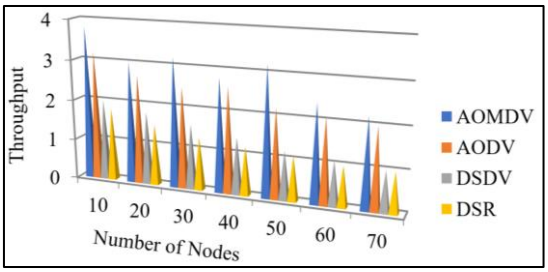


Fig. 7: (a) End-to-end delay; (b) Packet delivery ratio; (c) Throughput

Dataset Creation Steps

There are various processes involved in generating a dataset by capturing real-time traffic from OpenStreetMap, SUMO, and NS3.

A. Data Collection

Get up-to-date information on the road network from dependable sources, such as OpenStreetMap (OSM), which offers crowd-sourced traffic data. Access the relevant area or area of interest in OSM to gather data on the road network, including information on the road topology, intersections, lanes, and traffic flow.

B. Data Extraction from. OSM File

Utilize the existing APIs and tools, such as the Overpass API, OSMNX, or custom scripts, to extract the appropriate road network information from the OSM database. Obtain information on lane information, road categories, speed limits, and intersections from the road network.

C. Convert to SUMO Format

Create the necessary format for SUMO using the retrieved OSM data. To convert OSM data into a SUMO-compatible format (like.net.xml), use converters provided in SUMO or third-party libraries (Fig. 8).

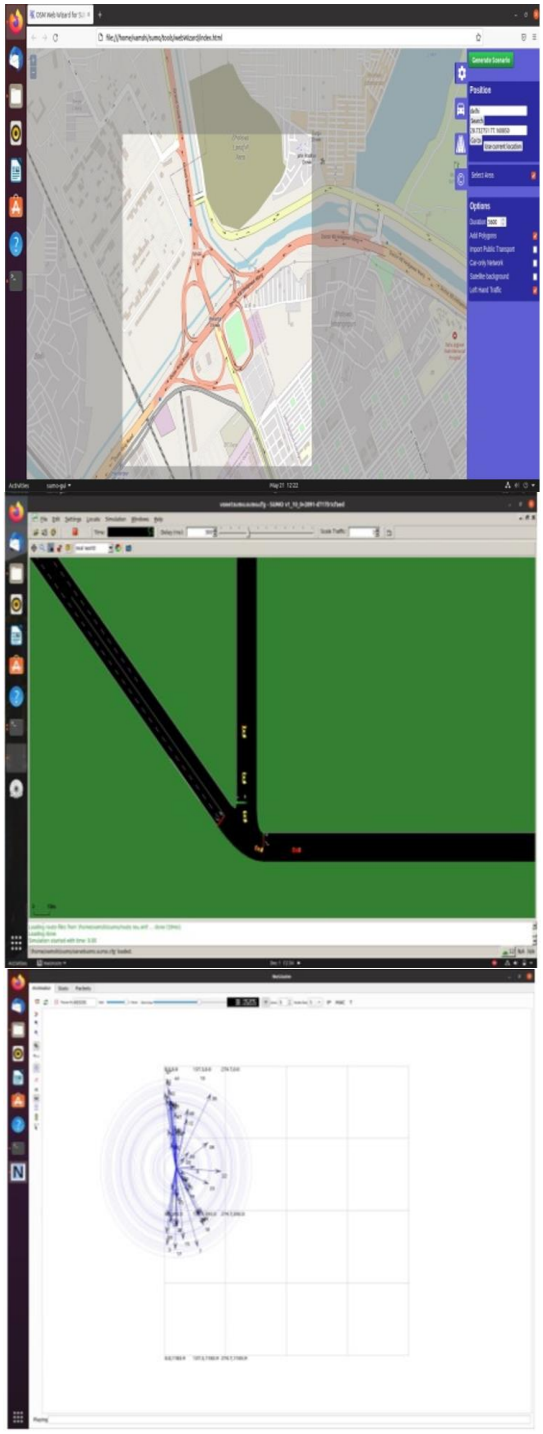


Fig. 8: A realistic scenario generated by OpenStreetMap, Sumo and NS3

DOI: 10.3844/jcssp.2023.1143.1159

D. Traffic Generation

Define the simulation's traffic demand and characteristics. For this purpose, traffic flows, vehicle categories, departure times, and paths may be generated using actual traffic patterns. Consider the supplied departure times, routes, and vehicle characteristics when you assign the generated traffic to the road network.

E. Extraction in SUMO and NS3

Use SUMO to run the simulation or the Network Simulator 3 (NS3) framework to incorporate the generated road network and traffic demand. Run the simulation to produce accurate traffic behavior and vehicle interactions based on the specified road network and traffic demand.

F. Output and Storage

The appropriate simulation output data should be captured and recorded, such as vehicle trajectory data, traffic flow rates, congestion levels, or other pertinent metrics. Save the simulation results in an appropriate format (such as a database, CSV, XML, or JSON) for further investigation or use in more experiments.

G. Analysis and Post Processing

Make use of the simulation output data analysis to gain valuable insights, assess traffic patterns, gauge the effectiveness of actions, or confirm research ideas. Process, display, and analyze the simulation results using data analysis tools or programming languages (such as Python and R) (Fig. 9)

A. Packet Delivery Ratio (PDR)

PDR is referred to as the ratio of the total received data packets to the total sent data packets:

$$PDR = \frac{\Sigma PKT\ received}{\Sigma PKT\ send} \tag{4}$$

B. End-to-End Delay (E2E)

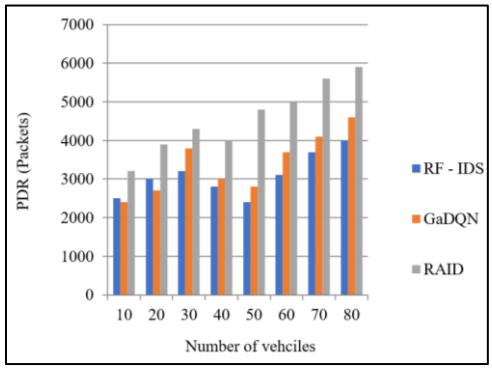
Average time spent transporting information packets from the source vehicle to the destination vehicle:

$$E2E = \frac{\Sigma\left(Arrival\ Time - Send\ Time\right)}{\Sigma\ No.of\ Vehicles} \tag{5}$$

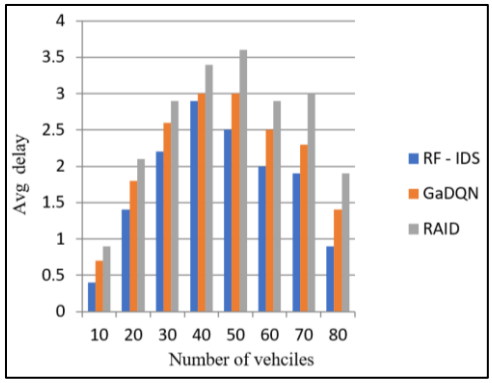
C. Throughput

Throughput is calculated by averaging the number of information packets successfully delivered to the target vehicle:

$$Throughput = \frac{Number\ of\ packets\ delivered * packets\ size * 8}{Total\ simulation\ time} \tag{6}$$



(a)



(b)

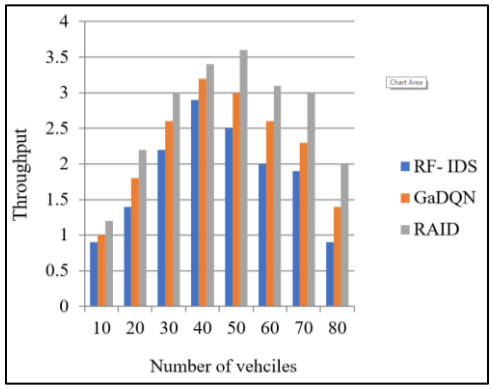


Fig. 9: (a) PDR; (b) End-to-End Delay; (c) Throughput

D. Accuracy

The suggested RAID's accuracy can be estimated using the following equation:

$$Acc = \frac{Tp + Tn}{Tp + Tn + Fp + Fn} \tag{7}$$

E. Detection Rate

Detection rate is the rate of identifying attacker vehicles correctly:

$$DR = \frac{Tp}{Tp + Fn} * 100 \tag{8}$$

The specific detection rate equation may vary depending on the security mechanisms employed in the VANET. The calculation of each probability term (*Tp* and *Fn*) in the detection rate equation requires considering the specific security mechanisms and protocols implemented in the VANET (Subramanian *et al*., 2017). This can involve techniques such as digital signatures, certificate-based authentication, message authentication codes, or other cryptographic methods. The detection rate formula can provide a clear and normalized measure of detection performance, allowing researchers and practitioners to assess the accuracy and reliability of their detection approaches.

F. Calculating i^{th} Intermediate Vehicle Propagation Delay

The amount of time it takes for the message to travel from the source to the destination is referred to as the intermediate vehicle's propagation delay:

$$Pr_{delay}^{i^{th}} = \frac{D}{S} \tag{9}$$

where, *D* is the vehicle's distance from the transmitting vehicle to the i^{th} intermediate vehicle and *S* indicates the average speed of the vehicles via which communication is taking place.

G. Minimum Transmission Delay of Vehicle

The amount of time it takes for a message or data packet to travel through a wireless medium This latency is affected by things like the VANET's channel access mechanism, data throughput, and packet size:

$$V_{t\,delay}^{\min} = \frac{packet\ size}{Data\ rate} \tag{10}$$

H. Range of i^{th} Vehicle

Depending on the type of technology and communication protocols being used, the range of vehicles in VANETs can vary. For V2V communication where vehicles communicate with each other directly, the range can be several hundred meters to a few kilometers (Bisheh-Niasar *et al*., 2021). For V2I communication where vehicles communicate via RSU will have a longer range than the V2V, the range can extend up to several kilometers, depending on the deployment and coverage area of RSU.

The results show (Fig. 10) how well the RAID structure performs overall. It was found that RAID performs better in terms of detection rate, throughput, PDR, and E2E delay. The dataset used to evaluate the performance of RAID was generated by running the simulation over a long period of time. On the other hand, we also evaluated the performance of protocols (Figs. 7a-c) that are compatible with our RAID framework. To determine which routing protocol provides optimal results, tests were conducted using DSR, AODV, DSDV, and AOMDV. According to the results of our simulation, AOMDV performs better in terms of PDF, throughput, and E2E delay.

Comparison with Existing Approaches

A. Problem Statement

Rushing attacks are malicious behaviors that occur when certain vehicles purposefully alter their behavior to gain an unfair advantage in network operations, such as accessing resources, creating communication channels, or receiving preferential treatment. The creation of efficient detection techniques, mitigation tactics, and security protocols is necessary to address the issue of rushing assaults in VANETs.

B. Approach Used

In our, we have used a novel detection technique known as RAID that detects the rushing attack in VANET by considering delay rules, dynamic threshold, vehicle timestamps, resource utilization, and others.

C. Key Findings

The key findings from the work are: Identifying rushing attacks, knowing the behavioral patterns of the network, dynamic threshold collaborative detection, and tradeoff between detection accuracy and overhead.

D. Novelty

The novelty of this study is Delay-based detection, Dynamic threshold, Incorporation of contextual data, Novel algorithm design, Real-time response, and mitigation. The dataset used in our work is self-generated that is created by extracting the live traffic using appropriate tools (refer to data creation section).

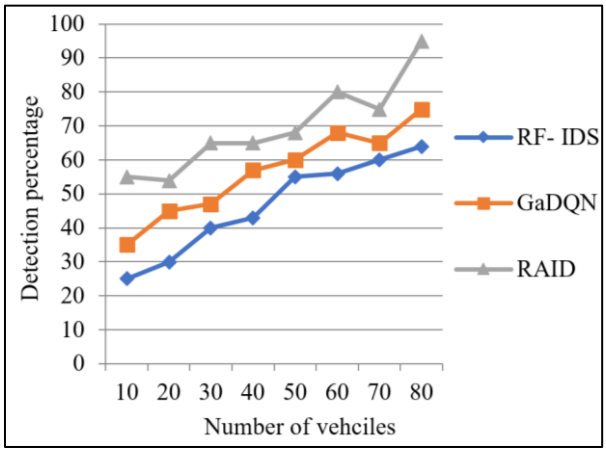


Fig. 10: RAID Overall detection rate

E. Limitations and Future Work

The proposed work was successful in detecting rushing attacks with delay rule and other parameters. The authors would like to consider the following attributes as limitations and future work: Dynamic Resource Allocation, Game-Theoretic Approaches, Improve QoS (Quality of Service), and Hybrid algorithm.

Discussion

Rushing attacks present serious security risks in VANETs as they may disrupt connectivity, communication, and resource allocation between vehicles as well as interfere with the network's normal operation. Here are some discussion-worthy points.

A. Vulnerabilities Exploited by Rushing Attacks

Rushing attacks take advantage of VANETs' fundamental qualities, such as the allocation of resources and the decentralized nature of communication. The lack of centralized control, the constrained communication range and the possibility for information imbalance between vehicles are just a few of the network vulnerabilities they take use of.

B. Attack Scenarios and Techniques

Examine various rushing attack situations and strategies that attackers may use. This can entail falsifying beacon signals, altering location data, or taking advantage of flaws in resource allocation systems. Discuss the unfair advantage rushing attackers may have over other vehicles.

C. Real-World Deployments and Challenges

Discuss the difficulties of implementing rushing attack defenses in actual VANETs. Take into account elements like scalability, interoperability, complexity of implementation, and the requirement for cooperation between numerous parties, including infrastructure providers, automobile manufacturers, and standardization agencies.

Future Research Work

Future research in the field of Vehicle Ad-Hoc Networks (VANETs) can concentrate on creating stronger and more effective defenses to lessen and stop such attacks.

A. Dynamic Resource Allocation

Create algorithms for dynamic and adaptive resource allocation that can change the distribution of resources in response to demand and network circumstances in real-time. By maintaining a fair and efficient distribution of resources among vehicles while taking into account elements like traffic circumstances, vehicle priority, and fairness limitations, such algorithms should be able to stop attacks.

B. Game-Theoretic Approaches

To examine and fully understand the defensive behavior of oncoming attackers and authorized vehicles, look into game-theoretic models. Create reward systems and techniques that discourage our attacks and encourage vehicle cooperation when using resources.

C. Quality of Service (*QoS*)

Various assaults on the vehicular network, such as rushing attacks, DOS and DDOS attacks, sinkhole attacks, and others, can have an impact on the QoS provided by the vehicular network. VANET requires modeling, designing, and implementation methods that will provide a legitimate message flow that can deliver data promptly and accurately to guarantee that emergency and safety-related information is secured against such assaults and maintains a high level of service quality across the network.

D. Advanced Routing Techniques

Traditional routing methods are worthless in a VANET because the involved transport vehicles are mobile and can change routing protocols in just a couple of seconds. Furthermore, in order to provide improved bandwidth, enhanced client service, and a greater packet delivery ratio, automobiles must be connected, data shared between both input and output vehicles, and data propagated to other vehicles.

E. Power Management

Transmission-related power management is a challenging issue that must be addressed to achieve effective vehicular communication. In a tightly packed vehicular network, maximum power may cause interferences that disrupt an ongoing transmission with some other transmission at a distant vehicle. As a result, in a higher-density network, lower power should be used to achieve reliable and efficient transmission (Mchergui *et al*., 2022).

F. Data Administration and Storage

Vehicles need to communicate in order to exchange data. The intruder uses vehicle storage capabilities and opportunistic conversations that can occur once one vehicle joins the communication range of another. The attackers use a variety of approaches to steal the information shared, including DOS, DDOS, Black Holes, Rushing, and others. Analyzing, storing, and keeping such huge amounts of data continues to be a challenge for researchers. Even while tools like Big Data can alleviate this issue, further research is needed to completely grasp the merging of two concepts.

G. Bandwidth and Connectivity

Vehicles nowadays are equipped with audio/video devices that play music and high-definition videos,

display 3D maps for navigation, and a variety of other apps; these apps must be updated regularly, which necessitates a large amount of bandwidth. VANET developers must ensure that adequate bandwidth for vehicle communication is provided. High bandwidth is useless if vehicle connectivity is poor; to communicate information (especially emergency information), connectivity is almost as important as bandwidth (Mchergui *et al*., 2022).

H. Standardization and Implementation

Develop standardized protocols and security measures in partnership with industry and standardization organizations that are especially suited to preventing attacks in VANETs. As a result, practical VANET systems would have interoperability, adoption, and implementation of efficient rushing attack countermeasures.

Conclusion

A rushing attack is an advanced attack that significantly impacts one of the security goals' *availability* resulting in a Denial of Service (DOS) attack. The rushing attack has received considerable attention in the field of MANET, but very little attention in the field of VANET. In this research work, we have shown that existing models such as RF-IDS and GaDQN have low accuracy in detecting rushing attacks, which makes the network vulnerable. With the RAID technique, we overcome this problem and improve the accuracy of detecting attacks.

RAID, a unique and effective method that could detect and prevent rushing attacks, is presented to safeguard and enhance the overall performance of VANETs. The approach was to compute a threshold value and generated a fake RREQ packet. The proposed RAID was built with OpenStreetMap and SUMO, tested in the NS-3 simulator and its performance and effectiveness were compared to the benchmark systems. Finally, the authors demonstrated that the RAID surpassed the benchmark techniques in terms of higher PDR, increased throughput, decreased end-to-end delay, and a maximum detection rate of 97.66%.

Future studies will focus on identifying and preventing different types of DOS and DDOS assaults.

Acknowledgment

The authors are thankful to "The Center of Excellence in Cyber Security", VIT-University, AP Campus for providing the necessary technical assistance and software to accomplish this research work.

Funding Information

No funding has been received from any agency in the public, commercial, or non-funding profit sectors.

Author's Contributions

Vamshi Krishna Kapu: Write up abstract, introduction, related work, proposed work, simulation and results.

Ganesh Reddy Karri: Drafted proposed work, data analysis, experiential setup and results.

Ethics

The article is original and contains unpublished data. The corresponding author confirms that all of the other authors have read and approved the manuscript and that no ethical issues are involved.

Availability of Data

Real-time traffic data is taken from OpenStreetMap, SUMO and NS3.

Competing Interests

"Not applicable" We, as authors, have no conflicts of interest to declare that are relevant to the content of this research article.

References

Aboelfottoh, A. A., & Azer, M. A. (2022, May). Intrusion Detection in VANETs and ACVs using Deep Learning. In *2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)* (pp. 241-245). IEEE. https://doi.org/10.1109/miucc55081.2022.9781691

Ahmed, W., Di, W., & Mukathe, D. (2022). Privacy-preserving blockchain-based authentication and trust management in VANETs. *IET Networks*, *11*(3-4), 89-111. https://doi.org/10.1049/ntw2.12036

Ajjaj, S., El Houssaini, S., Hain, M., & El Houssaini, M. A. (2022). A new multivariate approach for real time detection of routing security attacks in VANETs. *Information*, *13*(6), 282. https://doi.org/10.3390/info13060282

Ali, S., Guo, X., Karri, R., & Mukhopadhyay, D. (2016). Fault attacks on AES and their countermeasures. *Secure System Design and Trustable Computing*, 163-208. https://doi.org/10.1007/978-3-319-14971-4_5

Aljabry, I. A., & Al-Suhail, G. A. (2021). A survey on network simulators for vehicular ad-hoc networks (VANETS). *Int. J. Comput. Appl*, *174*(11), 1-9. https://faculty.uobasrah.edu.iq/uploads/publications/1631546206.pdf

Al-Shareeda, M. A., & Manickam, S. (2022). Security methods in internet of vehicles. arXiv preprint arXiv:2207.05269. https://doi.org/10.48550/arxiv.2207.05269

Al-Shareeda, M. A., Anbar, M., Hasbullah, I. H., & Manickam, S. (2020). Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sensors Journal*, *21*(2), 2422-2433. https://doi.org/10.1109/jsen.2020.3021731

Alshudukhi, J. S., Mohammed, B. A., & Al-Mekhlafi, Z. G. (2020). Conditional privacy-preserving authentication scheme without using point multiplication operations based on Elliptic Curve Cryptography (ECC). IEEE Access, 8, 222032-222040. https://doi.org/10.1109/access.2020.3044961

Anastasova, M., Azarderakhsh, R., & Kermani, M. M. (2021). Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *68*(10), 4129-4141. https://doi.org/10.1109/TCSI.2021.3096916

Azam, F., Yadav, S. K., Priyadarshi, N., Padmanaban, S., & Bansal, R. C. (2021). A comprehensive review of authentication schemes in vehicular ad-hoc network. *IEEE Access*, *9*, 31309-31321. https://doi.org/10.1109/ACCESS.2021.3060046

Bakkoury, S. O. S. B. Z. (2021), New Machine Learning Solution Based on Clustering for Delay-Sensitive Application in VANET. *International Journal on "Technical and Physical Problems of Engineering*" (IJTPE).

Bangui, H., Ge, M., & Buhnova, B. (2021a). A hybrid data-driven model for intrusion detection in VANET. *Procedia Computer Science*, *184*, 516-523. https://doi.org/10.1016/j.procs.2021.03.065

Bangui, H., Ge, M., & Buhnova, B. (2021b). A hybrid machine learning model for intrusion detection in VANET. *Computing*, *104*(3), 503-531. https://doi.org/10.1007/s00607-021-01001-0

Bayat-Sarmadi, S., Kermani, M. M., Azarderakhsh, R., & Lee, C. Y. (2013). Dual-basis superserial multipliers for secure applications and lightweight cryptographic architectures. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *61*(2), 125-129. https://doi.org/10.1109/TCSII.2013.2291075

Benmir, A., Korichi, A., Bourouis, A., Alreshoodi, M., & Al-Jobouri, L. (2019, September). An enhanced gpsr protocol for vehicular ad hoc networks. In *2019 11th Computer Science and Electronic Engineering (CEEC)* (pp. 85-89). IEEE. https://doi.org/10.1109/ceec47804.2019.8974321

Bensaid, C., & Boukli-Hacene, S. (2019). AODV-based Key Management in VANET Network. *Advances in Systems Science and Applications*, *19*(2), 80-89. https://doi.org/10.25728/assa.2019.19.2.707

Berzati, A., Viera, A. C., Chartouni, M., Madec, S., Vergnaud, D., & Vigilant, D. (2023). A Practical Template Attack on CRYSTALS-Dilithium. *Cryptology ePrint Archive*. https://eprint.iacr.org/2023/050

Bharti, M., Rani, S., & Singh, P. (2022). RTBSAD: RSSI AND TRUST-BASED SYBIL ATTACK DETECTION IN MANET. *Indian Journal of Computer Science and Engineering*. https://doi.org/10.21817/indjcse/2022/v13i3/221303128

Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021). Cryptographic accelerators for digital signature based on Ed25519. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *29*(7), 1297-1305. https://doi.org/10.1109/TVLSI.2021.3077885

Cheng, H., & Liu, Y. (2020). An improved RSU-based authentication scheme for VANET. *Journal of Internet Technology*, *21*(4), 1137-1150. https://jit.ndhu.edu.tw/article/view/2341

Cheng, P., Lee, K., Gerla, M., & Härri, J. (2010). GeoDTN+Nav: Geographic DTN Routing with Navigator Prediction for Urban Vehicular Environments. *Mobile Networks and Applications*, *15*(1), 61-82. https://doi.org/10.1007/s11036-009-0181-6

Cheng, Y., Xu, S., Zang, M., Jiang, S., & Zhang, Y. (2021, December). Secure authentication scheme for VANET based on blockchain. In *2021 7th International Conference on Computer and Communications (ICCC)* (pp. 1526-1531). IEEE. https://doi.org/10.1109/ICCC54389.2021.9674693

Canto, A. C., Kaur, J., Kermani, M. M., & Azarderakhsh, R. (2023). Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security. *arXiv preprint arXiv*:2305.13544. https://doi.org/10.36227/techrxiv.23071079.v1

Dhanaraj, R. K., Islam, S. H., & Rajasekar, V. (2022). A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments. *Wireless Networks*, *28*(7), 3127-3142. https://doi.org/10.1007/s11276-022-03017-6

Di, C., & Wu, W. (2022). A novel identity-based mutual authentication scheme for vehicle ad hoc networks. *Wireless Communications and Mobile Computing*, 2022. https://doi.org/10.1155/2022/7881079

Dubrova, E., Ngo, K., Gärtner, J., & Wang, R. (2023, July). Breaking a fifth-order masked implementation of crystals-kyber by copy-paste. In Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop (pp. 10-20). https://doi.org/10.1145/3591866.3593072

Dutta, R., & Thalore, R. (2017). A review of various routing protocols in VANET. *International Journal of Advanced Engineering Research and Science*, *4*(4), 237143. https://dx.doi.org/10.22161/ijaers.4.4.34

Ercan, S., Ayaida, M., & Messai, N. (2021). Misbehavior detection for position falsification attacks in VANETs using machine learning. *IEEE Access*, *10*, 1893-1904., https://doi.org/10.1109/access.2021.3136706

Hota, L., Nayak, B. P., Kumar, A., Sahoo, B., & Ali, G. M. N. (2022). A performance analysis of VANETs propagation models and routing protocols. *Sustainability*, *14*(3), 1379. https://doi.org/10.3390/su14031379

Ibrahim, H. A., Sundaram, B. B., Ahmed, A. S., & Karthika, P. (2021, December). Prevention of Rushing Attack in AOMDV using Random Route Selection Technique in Mobile Ad-hoc Network. In *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 626-633). IEEE. https://doi.org/10.1109/iceca52323.2021.9676089

Jalali, A., Azarderakhsh, R., Kermani, M. M., & Jao, D. (2017). Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM. *IEEE Transactions on Dependable and Secure Computing*, *16*(5), 902-912. https://doi.org/ 10.1109/TDSC.2017.2723891

Jiang, H., Hua, L., & Wahab, L. (2021). SAES: A self-checking authentication scheme with higher efficiency and security for VANET. *Peer-to-Peer Networking and Applications*, *14*, 528-540. https://doi.org/10.1007/s12083-020-00997-0

Kaur, J., Canto, A. C., Kermani, M. M., & Azarderakhsh, R. (2023). A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard. *arXiv Preprint arXiv*:2304.06222. https://doi.org/10.48550/arXiv.2304.06222

Kermani, M. M., & Azarderakhsh, R. (2018). Reliable architecture-oblivious error detection schemes for secure cryptographic GCM structures. *IEEE Transactions on Reliability*, *68*(4), 1347-1355. https://doi.org/10.1109/TR.2018.2882484

Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). A lightweight and secure online/offline cross-domain authentication scheme for VANET systems in Industrial IoT. *PeerJ Computer Science*, *7*, e714. https://doi.org/10.7717/peerj-cs.714

Koziel, B., Azarderakhsh, R., & Mozaffari-Kermani, M. (2015). Low-resource and fast binary edwards curves cryptography. *In Progress in Cryptology--INDOCRYPT 2015: 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings 16* (pp. 347-369). Springer International Publishing. https://doi.org/10.1007/978-3-319-26617-6_19

Kumar Pulligilla, M., & Vanmathi, C. (2023). An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection. *Internet of Things*, 22, 100723. https://doi.org/10.2139/ssrn.4204646

Liang, J., Ma, M., & Tan, X. (2021). Gadqn-ids: A novel self-adaptive ids for vanets based on bayesian game theory and deep reinforcement learning. *IEEE Transactions on Intelligent Transportation Systems*, *23*(8), 12724-12737. https://doi.org/10.1109/tits.2021.3117028

Lin, C., Huang, X., & He, D. (2022). EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/tdsc.2022.3164740

Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X., & He, W. (2020). An efficient decentralized key management mechanism for VANET with blockchain. *IEEE Transactions on Vehicular Technology*, *69*(6), 5836-5849. https://doi.org/10.1109/tvt.2020.2972923

Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J. T. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in vanets. *Sensors*, *22*(5), 1897. https://doi.org/10.3390/s22051897

Maria, A., Pandi, V., Lazarus, J. D., Karuppiah, M., & Christo, M. S. (2021). BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs. *Security and Communication Networks*, *2021*, 1-11. https://doi.org/10.1155/2021/6679882

Masruroh, S. U., Iqbal, M. I., & Hakiem, N. (2020). Performance Evaluation of AODV and AOMDV Routing Protocol on Rushing Attack for Wireless Mesh Network. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *12*(4), 51-55. https://jtec.utem.edu.my/jtec/article/view/5537

Mathur, B., & Jain, A. (2018). AOMDV protocol: A literature review. *International Journal of New Technology and Research*, *4*(7), 263027.

Mchergui, A., Moulahi, T., & Zeadally, S. (2022). Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs). *Vehicular Communications*, *34*, 100403. https://doi.org/10.1016/j.vehcom.2021.100403

Mei, S., Yuyan, G., Juan, Z., & Mingming, J. (2022). An Authentication and Key Agreement Scheme Based on Roadside Unit Cache for VANET. *Security and Communication Networks*, 2022. https://doi.org/10.1155/2022/3116682

Moni, S. S., & Manivannan, D. (2022, January). A lightweight privacy-preserving V2I mutual authentication scheme using Cuckoo filter in VANETs. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 815-820). IEEE. https://doi.org/10.1109/CCNC49033.2022.9700538

Mozaffari-Kermani, M., & Reyhani-Masoleh, A. (2009). Fault Detection Structures of the S-boxes and the Inverse S-boxes for the Advanced Encryption Standard. *Journal of Electronic Testing*, *25*, 225-245. https://doi.org/10.1007/s10836-009-5108-4

Mozaffari-Kermani, M., & Reyhani-Masoleh, A. (2011, September). A high-performance fault diagnosis approach for the AES SubBytes utilizing mixed bases. In *2011 Workshop On Fault Diagnosis and Tolerance In Cryptography* (pp. 80-87). IEEE. https://doi.org/10.1109/FDTC.2011.11

Paranjothi, A., & Atiquzzaman, M. (2021). A statistical approach for enhancing security in VANETs with efficient rogue node detection using fog computing. *Digital Communications and Networks*, *8*(5), 814-824. https://doi.org/10.1016/j.dcan.2021.09.010.

Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA vulnerabilities and its replacement by ECC: Elliptic curve cryptographic scheme for key generation. In *Network Security Attacks and Countermeasures* (pp. 270-312). IGI Global. https://doi.org/10.4018/978-1-4666-8761-5.ch012

Raja, G., Anbalagan, S., Vijayaraghavan, G., Theerthagiri, S., Suryanarayan, S. V., & Wu, X. W. (2020). SP-CIDS: Secure and private collaborative IDS for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4385-4393. https://doi.org/10.1109/tits.2020.3036071

Rao, R. S., Seema, Singh, P. K., & Khan, S. A. (2022). State of the Art VANETs Routing Protocols: A Literature Review. *International Journal of Mathematical, Engineering and Management Sciences*, *7*(3), 380-398. https://doi.org/10.33889/ijmems.2022.7.3.026

Remya Krishnan, P., & Arun Raj Kumar, P. (2022). Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping. *Wireless Personal Communications*, 1-36. https://doi.org/10.1007/s11277-021-09390-3

Sajini, S., Anita, E. M., & Janet, J. (2023). Improved security of the data communication in VANET environment using ASCII-ECC algorithm. *Wireless Personal Communications*, *128*(2), 759-776. https://doi.org/10.1007/s11277-022-09974-7

Shawky, M. A., Bottarelli, M., Epiphaniou, G., & Karadimas, P. (2023). An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks. IEEE Transactions on Vehicular Technology.

Sundaram, B. B., Kedir, T., Sorsa, T. T., Geleta, R., Srinivas, N., & Genale, A. H. (2020). An Approach for rushing attack resolution in AOMDV using arbitrary ID in MANET. *Palarch's Journal of Archaeology of Egypt/Egyptology*.

Sabbagh, A. A., & Shcherbakov, M. V. (2021a). A Secure and Stable Routing Protocol for VANET Under Malicious Attacks. In *Creativity in Intelligent Technologies and Data Science: 4th International Conference, CIT&DS 2021, Volgograd, Russia, September 20–23, 2021, Proceedings 4* (pp. 421-435). Springer International Publishing. https://doi.org/10.1007/978-3-030-87034-8_30

Sabbagh, A. A., & Shcherbakov, M. V. (2021b). Evaluation of reactive routing protocols performance under malicious attacks in VANET. *Distributed Computer and Communication Networks: Control, Computation, Communications: 24th International Conference*, DCCN 2021, Moscow, Russia.

Sarker, A., Kermani, M. M., & Azarderakhsh, R. (2020). Error Detection Architectures for Ring Polynomial Multiplication and Modular Reduction of Ring-LWE in $\boldsymbol {\frac {\mathbb {Z}/p\mathbb {Z}[x]}{x^{n}+ 1}} $ Benchmarked on ASIC. *IEEE Transactions on Reliability*, *70*(1), 362-370. https://doi.org/10.1109/TR.2020.2991671

Shah, P., & Kasbe, T. (2021a, May). Detecting sybil attack, black hole attack and DoS attack in VANET using RSA algorithm. In *2021 Emerging Trends in Industry 4.0* (ETI 4.0) (pp. 1-7). IEEE. https://doi.org/10.1109/eti4.051663.2021.9619414

Shah, P. A., & Kasbe, T. (2021b). A review on specification evaluation of broadcasting routing protocols in VANET. *Computer Science Review*, *41*, 100418. https://doi.org/10.1016/j.cosrev.2021.100418

Sharma, P., Pandey, S., & Jain, S. (2022). Implementation of efficient security algorithm and performance improvement through ODMRP protocol in VANET environment. *Wireless Personal Communications*, *123*(3), 2555-2579. https://doi.org/10.1007/s11277-021-09253-x

Sindhwani, M., Sachdeva, S., Arora, K., Yoon, T., Yoo, D., Joshi, G. P., & Cho, W. (2022). Soft Computing Techniques Aware Clustering-Based Routing Protocols in Vehicular Ad Hoc Networks: A Review. *Applied Sciences*, *12*(15), 7922. https://doi.org/10.3390/app12157922

Stalin, J., Rajesh, R. S., & Selvi, S. S. A. M. (2018). A survey on topology and geography-based routing protocols in VANETs. *International Journal of Applied Engineering Research*, *13*(20), 14813-14822.

Subramanian, S., Mozaffari-Kermani, M., Azarderakhsh, R., & Nojoumian, M. (2017). Reliable hardware architectures for cryptographic block ciphers LED and HIGHT. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *36*(10), 1750-1758. https://doi.org/10.1109/TCAD.2017.2661811

Tami, A., Boukli Hacene, S., & Ali Cherif, M. (2021). Detection and prevention of blackhole attack in the AOMDV routing protocol. *Journal of Communications Software and Systems*, *17*(1), 1-12. https://doi.org/10.24138/jcomss.v17i1.945

Theodore, S. K., Gandhi, K. R., & Palanisamy, V. (2021). A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks. *Complex & Intelligent Systems*, 1-11. https://doi.org/10.1007/s40747-021-00562-z

Wang, B., Wang, Y., & Chen, R. (2019). A Practical Authentication Framework for VANETs. *Security and Communication Networks*, *2019*, 1-11. https://doi.org/10.1155/2019/4752612

Wang, Y., Zhang, W., Wang, X., Khan, M. K., & Fan, P. (2021). Efficient privacy-preserving authentication scheme with fine-grained error location for cloud-based VANET. *IEEE Transactions on Vehicular Technology*, *70*(10), 10436-10449. https://doi.org/10.1109/TVT.2021.3107524

Xu, H., Mengjia, Z., Hu, W., & Wang, J. (2019). Authentication-Based Vehicle-to-Vehicle Secure Communication for VANETs. *Mobile Information Systems*, *2019*, 1-9. https://doi.org/10.1155/2019/7016460

Xu, W., Ji, X., Zhang, C., & Liu, B. (2020, May). NIHR: name/ID hybrid routing in information-centric VANET. In *2020 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-7). IEEE. https://doi.org/10.1109/wcnc45663.2020.9120459

Yang, M., Chen, J., Chen, Y., Ma, R., & Kumar, S. (2021). Strong key-insulated secure and energy-aware certificateless authentication scheme for VANETs. *Computers and Electrical Engineering*, *95*, 107417. https://doi.org/10.1016/j.compeleceng.2021.107417

Yang, X., Li, M., Qian, Z., & Di, T. (2018). Improvement of GPSR Protocol in Vehicular Ad Hoc Network. *IEEE Access*, *6*, 39515-39524. https://doi.org/10.1109/access.2018.2853112

Yogarayan, S., Razak, S. F. A., Azman, A., Abdullah, M. Z., Ibrahim, S. F., & Raman, K. J. (2020). A Review of Routing Protocols for Vehicular Ad-Hoc Networks (VANETs). In *International Conference on Information and Communication Technology*. https://doi.org/10.1109/icoict49345.2020.9166174

Younas, S., Rehman, F., Maqsood, T., Mustafa, S., Akhunzada, A., & Gani, A. (2022). Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs. *Applied Sciences*, *12*(23), 12448. https://doi.org/10.3390/app122312448

Zhang, J., Zhang, Q., Lu, X., & Gan, Y. (2021). A Novel Privacy-Preserving Authentication Protocol Using Bilinear Pairings for the VANET Environment. *Wireless Communications and Mobile Computing*, *2021*, 1-13. https://doi.org/10.1155/2021/6692568

Zhou, X., Luo, M., Vijayakumar, P., Peng, C., & He, D. (2022). Efficient Certificateless Conditional Privacy-Preserving Authentication for VANETs. *IEEE Transactions on Vehicular Technology*, *71*(7), 7863-7875. https://doi.org/10.1109/tvt.2022.3169948