Enhancing VANET Security: Efficient Communication and Wormhole Attack Detection using VDTN Protocol and TD3 Algorithm

Vamshi Krishna. K[1] and Ganesh Reddy K[2*]
[1] School of Computer Science and Engineering, VIT-AP University
Guntur, AP 522237 INDIA
[e-mail: vamshikrishna.20phd7088@vitap.ac.in]
[2] School of Computer Science and Engineering, VIT-AP University
Guntur, AP 522237 INDIA
[e-mail: ganesh.reddy@vitap.ac.in]
[*]Corresponding author: Vamshi Krishna. K

Abstract

Due to the rapid evolution of vehicular ad hoc networks (VANETs), effective communication and security are now essential components in providing secure and reliable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. However, due to their dynamic nature and potential threats, VANETs need to have strong security mechanisms. This paper presents a novel approach to improve VANET security by combining the Vehicular Delay-Tolerant Network (VDTN) protocol with the Deep Reinforcement Learning (DRL) technique known as the Twin Delayed Deep Deterministic Policy Gradient (TD3) algorithm. A store-carry-forward method is used by the VDTN protocol to resolve the problems caused by inconsistent connectivity and disturbances in VANETs. The TD3 algorithm is employed for capturing and detecting Worm Hole Attack (WHA) behaviors in VANETs, thereby enhancing security measures. By combining these components, it is possible to create trustworthy and effective communication channels as well as successfully detect and stop rushing attacks inside the VANET. Extensive evaluations and simulations demonstrate the effectiveness of the proposed approach, enhancing both security and communication efficiency.

Keywords: VANET Security, Communication, Worm Hole Attack, VDTN, TD3.

1. Introduction

With the goal of facilitating effective and dependable communication between infrastructure and vehicles in Intelligent Transportation Systems (ITS), VANETs have emerged as a potential technology. By enabling the exchange of real-time information, these networks help to improve traffic management, safety, and the overall driving experience [7]. However, because vehicular surroundings are dynamic and unpredictable, VANETs encounter few difficulties. Some of the most significant difficulties VANETs face are connectivity and security threats, such as restricted communication range, high mobility of vehicles, unpredictable network conditions, and attacks (WHA) [11]. These elements may affect the ability of VANETs to support crucial applications by causing communication breakdowns, longer delays, and decreased network coverage. Since VANETs are dynamic in nature, efficient communication and the detection of wormhole attacks are two fundamental aspects of enhancing VANET security [25]. Efficient communication mechanisms are essential to establish reliable and timely information dissemination among vehicles, ensuring the smooth flow of critical data such as traffic updates, collision warnings, and emergency notifications [10]. On the other hand, detecting and mitigating WHA is essential to maintain traffic safety and prevent disruptions within the VANET environment. The wormhole attack is a highly dangerous threat that requires two hostile nodes to establish a fast tunnel and secretly pass packets back and forth [30]. The significant network routing and communication disturbance caused by this malicious tunnel may lead to traffic accidents, the transmission of false information, and possible panic on the roads. In VANET, vehicles communicate with one another using three components and three methods [15]. The first of these three components is the AU (Application unit), which is a physical device built into the vehicle to display the necessary information. The second component is the OBU (On-board unit), a type of antenna mounted outside the car, typically in the front or rear; this OBU is used to send and receive messages from other vehicles and RSU. The third component is RSU, which is installed along the roadside and is primarily utilized for data transfer, authentication, and validation. RSUs are used to transmit data between two or more vehicles that want to communicate but are out of range of one another [1] [9]. The three most common communication techniques are V2V (Vehicle to Vehicle), V2I (Vehicle2Infrastructure), and V2X (Hybrid - V2V / V2I) [9]. **Fig. 1** depicts the fundamental design of the VANET communication modes discussed above.
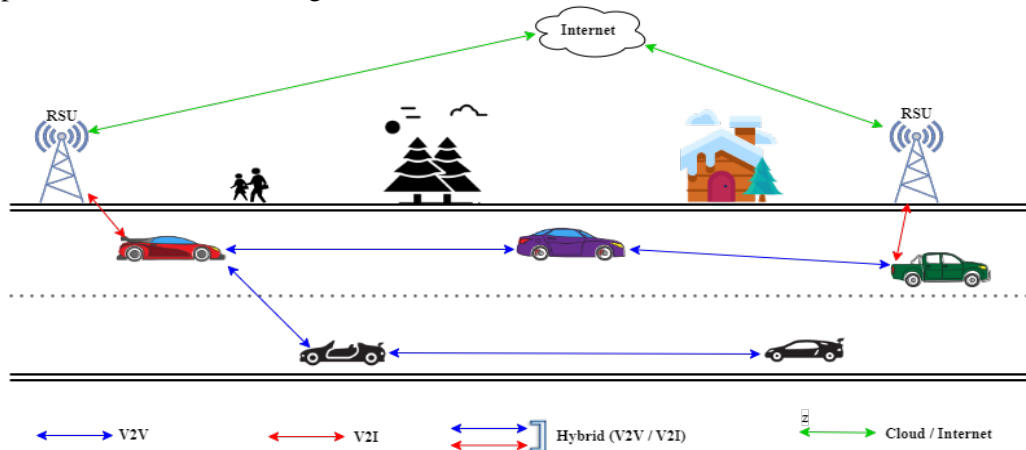

Fig. 1. VANET Communication Modes

The article's remaining sections are organized as follows: A review of related research on VANET security and recent communication protocols is provided in Section 2. In Section 3, we concentrate on the communication issues and vulnerabilities of the VANET, emphasizing the importance of the proposed strategy. The VDTN Protocol's design and workings are described in Section 4, along with how it supports effective communication in VANETs. In Section 5, we explore wormhole attacks in brief and look at how the TD3 algorithm works and what role it plays in detecting wormhole attacks. The performance assessment of our proposed approach is provided in depth in Section 6, which also analyses the outcomes of numerous simulations. In Section 7, we undertake a thorough security study, evaluating the durability of the VDTN Protocol and TD3. Finally, Section 8 offers a thorough analysis of the results, highlighting the contributions of our study, and brings the work to a close by summarizing the main ideas of the proposed technique and future research.

Table 1. List of Abbreviations

S.no	Abbreviation	Full form
1	AI	Artificial Intelligence
2	AODV	Ad-hoc On-demand Distance Vector
3	AU	Application Unit
4	CPM	Contact Prediction Module
5	DDPG	Deep Deterministic Policy Gradient
6	DNN	Deep neural networks
7	DRL	Deep Reinforcement Learning
8	DTN	Delay-Tolerant Networking
9	E2E	End-to-End
10	IDS	Intrusion Detection System
11	ITS	Intelligent Transportation Systems
12	KNN	K-Nearest Neighbours
13	ML	Machine Learning
14	OBU	On Board Unit
15	PPKS	Proactive Prevention Key Solution
16	RF	Random Forest
17	RSU	Road Side Unit
18	SVM	Support Vector Machine
19	TD3	Twin Delayed Deep Deterministic Policy Gradient
20	V2I	Vehicle-to-Infrastructure
21	V2V	Vehicle-to-Vehicle
22	V2X	Hybrid (V2V or V2I or Both)
23	VANET	
24	VDTN	Vehicular Delay-Tolerant Network
25	WHA	Wormhole Attack

2. Related Work

Providing WHA countermeasures is a difficult task, and many authors have proposed various techniques and algorithms. In this section, we will look at the existing countermeasures.

Authors [25] presented an ML approach with Preventive Scheme that uses an AODV routing protocol and an NS3 simulator that generates statistics, and then KNN and RF

algorithms are applied to detect WHA. The parameters considered here are packet lease and cryptographic. Authors [32] presented an ML approach using KNN and SVM that detected wormhole attacks using NS3 and a generated dataset. The parameters extracted for detection are source and destination IP, lost packets, received and transmitted packets, bytes dropped, delay sum, jitter sum, and packet dropped. Authors [31] propose an IDS to detect a malicious vehicle in the network using the DNN algorithm. Data is extracted using vector and value information; using this, the IDS is built for detecting malicious vehicles in the network. Authors [30] proposed the ESWI technique that optimizes the energy during the wormhole attack; this proposed method increases the performance and security of the wireless network while under attack. Authors [23] presented a review of various ML-AI techniques for detecting wormholes in wireless sensor networks that can produce a state-of-the-art solution to the existing problem. Authors [24] presented a routing technique using the AODV protocol that prevented the wormhole attack and provided security for IEEE 802.11 networks. Along with the DAPS technique, the authors also presented the *Proactive Prevention Key Solution* (PPKS) algorithm, which uses the timestamp of the nodes to determine its validity. Authors [26] proposed a new routing technique that uses LCNA and i-AOMDV methods for the detection of wormhole attacks in clustered wireless sensor networks and the proposed models were compared with EEHRCP and AD-PSO to achieve the desired results. Authors [27] dual schemes using active trust and a Cuckoo search algorithm that safeguards the network from various assaults such as a black hole and selective forwarding attacks that result in providing network lifespan and a secure routing path in WSN. Authors [28] proposed a novel self-adaptive framework for detecting black hole and wormhole attacks in WSN using a modified AODV protocol for *6LoWPAN* (low-power wireless personal area networks). Authors [29] proposed a novel SPAS algorithm using DDPG and HRM-SG for real-time audio and video generation and used this for predating driver's comfort in lane changing, speed, and others to achieve accuracy in pothole avoidance.

Table 2. Correlation of Existing techniques

Reference No	Attack type	Technique / Algorithm	Achieved	Drawbacks or further work
[25]	Wormhole	KNN and RF with packet lease and cryptographic	High accuracy	Lacks continuous learning Generation of dynamic threshold in varying network
[32]	Wormhole	KNN and SVM	High accuracy and low alarm	Detecting attacks at different layers
[31]	Malicious vehicle	DNN with a vector comprising value information extracted	Discriminate normal and hacking CAN packets with 98% accuracy	Real-time
[30]	Wormhole	ESWI technique	Minimize overheads and energy waste in its operations.	explore the metaheuristic approaches for the optimization of resources
[23]	Wormhole	ML-AI	Optimal solution	More optimal algorithms

[24]	Wormhole	DAPS technique and PPKS algorithm	safeguard IEEE 802.11 networks	Extend using different techniques and algorithms
[26]	Wormhole	New routing technique for WSN, LNCA algorithm, and i-AOMDV	the delivery ratio of packets, energy efficiency, delay from end to end, throughput,	Extend with new protocols and techniques
[27]	WSN black holes and selective forwarding	Dual assurance scheme with an active trust and Cuckoo search algorithm	Lifespan and secure routing path	Real-time implantation
[28]	Black Hole and Wormhole Attacks in DQN and 6LoWPAN	self-adaptive framework	Improved overall performance	Implement dense nodes and new modification techniques
[29]	Lane change, speed, angle	SPAS, DDPG, HRM-SG	Pothole avoidance, accuracy, convergence	considering pedestrian movement using computer vision, image processing, and multi-agent DDPG

The existing approaches failed to address the following issues:
- Setting up communication is a challenging task in continuously changing network like VANET
- Generation of dynamic threshold is difficult where network size varies constantly
- Accuracy of wormhole detection
- Continues learning of varying network scenarios

Our proposed system overcomes the drawbacks encountered by the existing systems

3. Significance of Proposed Methodology

3.1 Vulnerabilities and Challenges

Due to their unique qualities and dynamic nature, VANETs encounter a variety of security issues and communication difficulties. Designing reliable and secure VANET systems that enhance network performance and identify WHA in vehicular networks requires understanding these security vulnerabilities and communication challenges [9], as you can see in **Table 3**.

Table 3. Vulnerabilities of VANET

Sl no	Communication challenges	Security vulnerabilities
1	Periodic Connectivity	Privacy Issues
2	High Mobility and Varying Speeds	Authentication and Authorization
3	Dynamic Topology	Data fabrication
4	Limited Bandwidth	DoS and DDoS attacks
5	Scalability	Sybil Attacks
6	Energy Efficiency	Physical Attacks

3.2 Significance

The VDTN Protocol and TD3 algorithm are used in the proposed technique to address the stated security vulnerabilities and communication challenges in VANETs. The significance of the TD3 algorithm and the VDTN Protocol is explained below.

To address the communication challenges, the VDTN Protocol is essential. Even when direct communication lines are broken, the VDTN Protocol's effective communication enables reliable data delivery [2]. Vehicles can now store and transmit data, with routing decisions and data delivery optimized to accommodate dynamic network topologies.

The TD3 Algorithm is essential in detecting and mitigating one of the critical security vulnerabilities of VANETs, the wormhole attack [13]. The TD3 Algorithm, through its reinforcement learning capabilities, intelligently identifies abnormal behavior patterns and detects the presence of the wormhole attack, ensuring the integrity of information shared among vehicles and mitigating the impact of malicious vehicles. The proposed methodology's collaborative nature, which involves the TD3 Algorithm and VDTN Protocol working together, improves the overall security of VANETs [8]. The technique provides a comprehensive approach to improving VANET security by integrating the VDTN Protocol for effective communication and the TD3 Algorithm for wormhole attack detection.

4. VDTN Protocol (Vehicular Delay-Tolerant Network)

The architecture of the VDTN Protocol aims to deliver effective communication even in challenging VANET scenarios with periodic connectivity and dynamic topology [14] [5]. The protocol improves data delivery dependability and aids in overcoming communication issues by utilizing the store-carry-forward mechanism and intelligent forwarding decisions [1][2].
The key components and operations of the VDTN protocol are:
Vehicle: A vehicle becomes the source (S) when it generates data, such as safety information, traffic updates, and sensor readings. The S tries to transfer the generated data directly to the destination (D) if a direct communication link exists between the S and D [4].
Roadside Units (RSUs): RSUs are physical devices that are deployed along the roadside. RSUs act as relays and data storage points to support communication in the vehicular network, enabling data exchange with vehicles passing within their communication range [6].
Message Buffer: The vehicular network's vehicles and RSUs are equipped with a message buffer. When there are no direct or intermediate paths between S and D, data is temporarily stored in these message buffers until a suitable opportunity for data forwarding occurs or the message's time-to-live (TTL) period expires [16].
Dynamic message management: Each vehicle's and RSU's message buffer is dynamically managed by the protocol, preventing data packets from being kept around forever. Each data

packet has time-to-live (ttl) values attached to it to set a storage time limit, preventing expired data from using up buffer space [22].

Data storage and forwarding: If no paths exist between S and D, the S vehicle stores the data packets in its own message buffer [11]. The S vehicle searches for a suitable vehicle or RSU that acts as a relay for the D vehicle and transfers the data packets to the identified relay vehicle or RSU.

Routing and Forwarding logic: To choose the optimal path for data transmission between S and D vehicles, the VDTN Protocol employs sophisticated routing and forwarding logic. To make intelligent routing decisions, it takes into account the vehicle's mobility, connectivity, and network topology [30].

Data forwarding decision: When there is no direct communication link to the destination due to periodic connectivity, the S decides how to proceed depending on the routing and forwarding logic [11]. It analyses the message buffer to determine if vehicles or RSUs with better connectivity to the D are nearby.

Contact Prediction Module (CPM): The CPM stage is an optional one that may be used in circumstances where vehicles and RSUs can plan data forwarding and make the best use of available communication windows using the projected contact opportunities [32].

Opportunistic Data forwarding: When vehicles move near one another and are within communication range of another vehicle or RSU, the VDTN Protocol opportunistically forwards data [6]. A vehicle or RSU that has stored data packets forwards the data when it comes across a vehicle or RSU with a better path to the D.

End2End Data Delivery: The VDTN protocol attempts to achieve E2E data delivery between the S and D vehicles even under challenging conditions of vehicular networks by integrating dynamic buffer management, contact prediction, and opportunistic data forwarding [18].

5. WHA in VANET (Worm Hole Attack)

A wormhole is one of the most popular and severe VANET attacks. The wormhole, like the Gray Hole attack, is a variant of the Black Hole attack [24][6] [8]. In this attack, two or more attacker vehicles create a tunnel and send packets from one end of the attacker vehicle to the other end of the attacker vehicle, then send them to the network [7]. The said tunnel between two attacking vehicles is known as a wormhole; the tunnel can even be created for unaddressed packets simply by overhearing them on the network [4]. **Fig. 2** depicts the classification of wormhole formation.
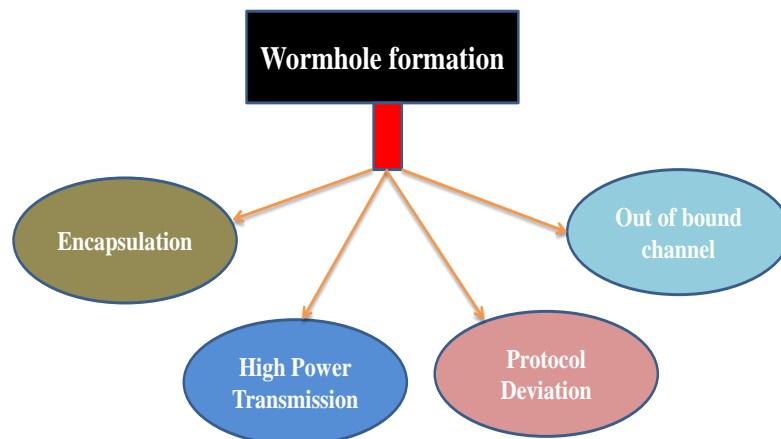

Fig. 2. Wormhole attack formation

The Wormhole attack endangers the VANET's availability, confidentiality, and integrity, potentially affecting the entire or a portion of the network [2]. The wormhole can be performed in two modes: hidden mode and participation mode, where encapsulation and protocol deviation belong to hidden mode and out-of-bound and high-power transmission fall under participation mode [3] [5].

5.1 TD3 (Twin Delayed Deep Deterministic Policy Gradient)

TD3 is an extension of the Deep Deterministic Policy Gradient (DDPG) algorithm and falls under the category of actor-critic methods. It is a powerful reinforcement learning technique used in various domains, including robotics, control systems, and anomaly detection [20]. It leverages deep neural networks to approximate both the policy (actor) and the value function (critic) to learn an optimal policy in a continuous action space. The "twin" in TD3 refers to the use of two critics to improve value estimation stability. In the context of VANETs (Vehicular Ad Hoc Networks), TD3 can be employed to detect and identify wormhole attacks, which are a significant security threat in vehicular networks [19].
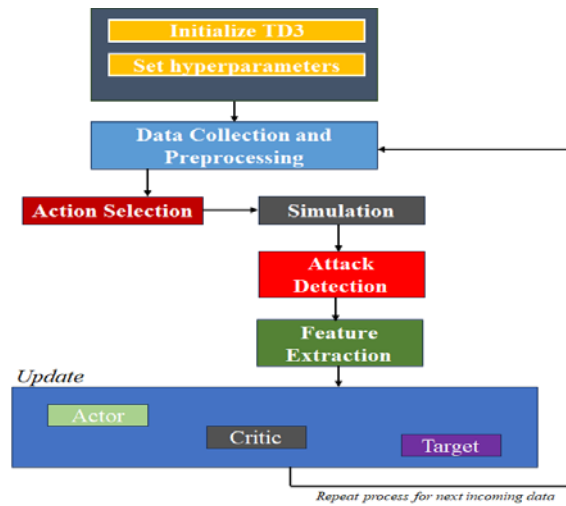

Fig. 3. Flow diagram of TD3 operation

5.2 Functions of TD3 in detecting wormhole attacks in VANET

In our proposed work, we employ the TD3 algorithm for the detection of wormhole attacks in the VANET. To do this, the TD3 algorithm is trained using both real-world VANET traffic data and simulated traffic data with wormhole attacks. The following steps show how it can be used to identify wormhole attacks:

Data collection: In VANETs, data is extracted from legitimate vehicles and RSUs to understand normal network behavior [1].

Attack Simulation: By inserting data packets between two malicious vehicles that have a high-speed data transfer tunnel, it is possible to simulate wormhole attack scenarios. This creates an artificial wormhole [24].

Training TD3: Using the legitimately collected data and the data from simulated wormhole attacks, the TD3 algorithm is trained. The objective is to discover the policy that maximizes the predicted cumulative reward while separating patterns of wormhole attack from normal behavior [17].

Classification and Detection: The TD3 method can be used to identify irregularities in VANET communication patterns after training. The algorithm issues an alert to warn of the possibility of a wormhole attack [24] if it notices behavior that differs significantly from the previously learned behavior.

Monitoring: The trained TD3 model can continually track network communication patterns in real-time VANET operations and identify potential wormhole attacks as they take place [3].

5.3 Equations

Table 4. List of Abbreviations

S.no	Abbreviation	Full form
1	ACC	Accuracy
2	AUC - ROC	Area Under the Receiver Operating Characteristic Curve
3	ET	Execution Time
4	$ETX_{i,j}$	Routing Metric
5	FNR	False Negative Rate
6	FPR	False Positive Rate
7	F1	F1-Score
8	L	Loss Function
9	LRU (i)	Dynamic Buffer Management
10	P	Precision
11	P_r	Communication Range
12	PL (d)	Path Loss Model
13	P(t)	Contact Prediction Module
14	Q_1 (s, a), Q_2 (s, a)	Bellman Equations
15	Rewards (s_t)	Cumulative discount reward
16	$TD3_{classifier}$	Wormhole classification
17	Threshold	Dynamic Threshold value
18	TPR	True Positive Rate

5.3.1 VDTN Based Equations

Communication Range: The Friis transmission equation, a widely used path loss model for wireless communication, can be used to represent the communication range of the VANET. The Friis transmission equation is provided by:

$$P_r = \frac{P_t \cdot G_t \cdot G_r \cdot \lambda^2}{(4\pi)^2 \cdot d^2 \cdot L}$$

(1)

where, P_r is the received power at the destination (D) in (watts), P_t is the transmitted power from the source (S), G_t , G_r are S and D's antenna gain, λ^2 is the wavelength of transmitted signal in (meters), d is the distance between S and D, and L is the system losses.

Path Loss Model: The signal loss and network quality between vehicles in a VANET are estimated using the path loss model. The Log-Normal Shadowing Model, often known as the Log-Distance route Loss Model, is one of the most widely used path loss models [16]. This formula can be used to calculate the path loss suffered by radio signals traveling between vehicles or between vehicles and Roadside Units (RSUs).

$$PL\ (d) = PL\ (d_o) + 10.n.\ log_{10}\ (\frac{d}{d_0}\ ) + X$$

$$(2)$$

where, PL (d) is the path loss at distance d in (dB), PL (d_o) is the reference path loss at a reference distance d_o in (dB), and n is the path loss exponent, that depends on the environment and frequency and X is a zero mean Gaussian random variable with standard deviation.

Routing Metric: The expected number of transmissions needed to successfully deliver a data packet from the (S to D) through a specific network link is measured using the expected transmission count (ETX), a routing metric that is frequently used in DTN (Delay-Tolerant Networking) protocols and can also be used in VDTN [12].

$$ETX_{i,\,j} = \frac{1}{Prob\ Success_{i,j}}$$

$$(3)$$

where, $ETX_{i,\,j}$ is the ETX metric between S (i) and D (j) through a specific intermediate vehicle, $Prob\ Success_{i,\,j}$ is the probability of successful transmission between vehicle i and vehicle j through the intermediate vehicle.

Contact Prediction Module (CPM): Based on previous mobility patterns, CPM is utilized in the Vehicular Delay-Tolerant Network (VDTN) protocol to estimate potential future contact possibilities between vehicles or Roadside Units (RSUs) [5]. To calculate the probability that two vehicles will make contact within a given time interval, the contact prediction model often uses probabilistic or statistical methodologies.

$$P(t) = \lambda.\ e^{-\lambda t}$$

$$(4)$$

where, P(t) is the probability of having a contact opportunity within a time t and λ is the rate parameter that determines the avg number of contacts per unit of time.

Dynamic Buffer Management: The LRU (Least Recently Used) technique is frequently used to decide which data packets to delete from the buffer when it reaches its limit, with the goal of dynamically managing buffer space allocation and handling data expiration based on Time-to-Live (TTL) values [2]. The data packet that has been in the buffer for the longest time without being transferred or forwarded is chosen by the LRU algorithm.

$$LRU\ (i) = min_{\,j}\ (arrival\ time\ (j))$$

$$(5)$$

where, LRU (i) is the index of the data packet that has been selected for removal from a buffer, j is the overall data packets in the buffer, and arrival time (j) is the arrival time of j th data packets in the buffer.

5.3.2 TD3 Based equations

Actor and Critic: The TD3 algorithm consists of two components: the actor network and the twin critic network. These components are used for approximating the policy (actor) and value functions (critics). The actor neural network takes the current state **s** as input and outputs the best action **a** to be taken in that state [9]. The critic neural networks, also known as twin critics, evaluate the quality of the chosen action by the actor network. They estimate the expected cumulative reward that can be obtained from following the actor's policy.

$$a = \text{Actor}(s)$$

(6)

where, a is the action output and s is the input state

$$Q_1(s,a) = \text{Critic}_1(s,a)$$
$$Q_2(s,a) = \text{Critic}_2(s,a)$$

(7)

where, $Q_1(s,a)$ and $Q_2(s,a)$ are the estimated Q values from the first and second critic networks , s is the input state and a is the input action

Bellman Equation: The Bellman equation for the Twin Delayed Deep Deterministic Policy Gradient (TD3) algorithm is used to update the value function estimates (Q-values) for the critic neural networks [21]. The Bellman equation is a fundamental concept in reinforcement learning and expresses the relationship between the value of a state-action pair and the expected cumulative reward that can be obtained by following a particular policy.

$$Q_1(s,a) = E_{s'\tau}[\,r + \gamma.\,min_{a'}\,Q_1(s',a')\,|\,s,a]$$
$$Q_2(s,a) = E_{s'\tau}[\,r + \gamma.\,min_{a'}\,Q_2(s',a')\,|\,s,a]$$

(8)

where, s' is the next state after taking action a, r is the immediate reward. a' represents the actions that the actor would take in the next state s' and γ represents the discount factor that determines the importance of future rewards compared to immediate rewards.

Loss function: It was a blow to the actor (political network). To compute the loss, sum the Q-values of all feasible states. We compute the Q values in the Critic network and then transfer that action to the Actor network [31]. To fulfill our goal of maximizing returns/Q-values, we must maximize this outcome. The Critic loss is a basic TD error that is used to determine Q-values for the next state. We must do everything possible to limit this loss.

$$L = \frac{1}{n}\sum_I (y_i - Q(s_i,\,a_i\,|\,\theta^Q))^{\,2}$$

(9)

Cumulative discount reward: In a reinforcement learning system, the cumulative reward (the sum of all rewards gained thus far) can be plotted as a function of the number of steps.

$$\text{Rewards}(s_t) \sim RE_t + \Upsilon\,RE_{t+1} + ... + \Upsilon^{\,T-t+1}\,RE_{T-1} + \Upsilon^{\,T-t}\,T^{Crt}(s_T,\,Act(\,s_T\,|\,\theta^{act}\,)\,|\,\theta T^{Crt}\,)$$

(10)

Noise: To encourage exploration of the action space, noise is added to the actor's output. In reinforcement learning, exploration is crucial to enabling the agent to identify potentially improved actions that result in higher rewards.

$$\text{Noise} = \theta.\,(\mu - \text{actor\_output}) + \sigma.\,N(0,1)$$

(11)

Where, Noise is the added to the actor's output, θ is a coefficient that determines the strength of mean reversion, μ is the mean value towards which the noise reverts, actor_output is the original action output, σ is the standard deviation and $N(0,1)$ is the random sample from a standard normal distribution.

Wormhole Classification: The TD3 algorithm is trained using both legitimate and malicious traffic data. After training, TD3 is used to identify whether a data packet received is a wormhole attack or a valid communication instance [15].

$$\text{TD3}_{\text{classifier}} = (\text{trained data \{parameters\}} + \text{received data packet})$$

(12)

where, parameters include Packet delay, Threshold, Packet Delivery Ratio (PDR), Hop count, Packet arrival time, and Received Signal Strength Indicator (RSSI).

Dynamic Threshold value: Dynamic threshold values are produced by a function that considers appropriate parameters and modifies the threshold in response to changing scenarios. Let threshold (t) be the dynamic threshold value at time (t)

$$Threshold = f(p1(t), p2(t)...pn(t)$$

(13)

where, p1(t), p2(t)...pn(t) are parameters of at time (t) and f () is the function that combines and processes parameters to generate threshold value.

Wormhole Detection: The binary indicator variable 1 indicates potential wormhole detected, o indicates normal traffic. Threshold values are defined to the respective features (parameters).

$$\text{flag} = 1 \begin{cases} Pkt_{delay} < Pkt_{delay} \ (Threshold_t) \\ \text{PDR} < \text{PDR} \ (Threshold_t) \\ Hop_{count} < Hop_{count} (\ Threshold_t) \\ Arrival\_time_{pkt} < Arrival\_time_{pkt}(Threshold_t) \\ \text{RSSI} < \text{RSSI} \ (\ Threshold_t) \end{cases}$$

(14)

flag = 0   // normal communication

5.3.3 Performance Metric Equations

Detection Accuracy: The accuracy of intrusion detection in VANET relates to how well the system can recognize and categorize intrusions within the network [31]. The accuracy metric is commonly used to measure an intrusion detection system's effectiveness and analyze its capacity to discriminate between expected network behavior and possible attacks.

$$\text{Acc} = \frac{(T_p + T_n)}{(T_p + T_n + F_p + F_n)} * 100$$

(15)

where, T_p (True positive) is the number of correctly detected intrusions, T_n (True negative) is the number of correctly identified normal instances, F_p (False positive) is the number of instances incorrectly identified as intrusions, and F_n (False negative) is the number of intrusions that were not detected.

False Positive Rate (FPR): is a metric used to evaluate the percentage of legitimate occurrences that intrusion detection systems mistakenly identify as intrusions. It is determined using the equation shown below:

$$\text{FPR} = \frac{F_p}{F_p + T_n}$$

(16)

False Negative Rate (FNR): is a performance indicator used to determine how well a classification system works in wormhole detection and distinguishes between positive occurrences (like wormhole attacks) and negative instances (like legitimate communication) [22].

$$\text{FNR} = \frac{Number\ of\ False\ Negative}{Number\ of\ Actual\ Positives}$$

(17)

Precision (P): is a performance indicator used to determine how well it comes to correctly recognizing positive occurrences (like wormhole attacks) out of all the cases it has categorized as positive.

$$\text{P} = \frac{Number\ of\ True\ Positives}{Number\ of\ True\ Positives + Number\ of\ False\ Positives}$$

(18)

True Positive Rate (TPR): is a performance metric used to evaluate the accuracy of identifying positive instances (e.g., wormhole attacks) out of all actual positive instances present in the dataset.

$$\text{TPR} = \frac{Number\ of\ True\ Positives}{Number\ of\ True\ Positives + Number\ of\ False\ Negatives}$$

(19)

F1-Score (F1): is a performance indicator that is employed to evaluate the overall effectiveness of a classification and detection system. To produce a balanced measurement, it combines Precision and Recall.

$$\text{F1-Score} = \frac{2\ X\ Precision\ X\ Recall\ (TPR)}{Percision + Recall\ (TPR)}$$

(20)

Area Under the Receiver Operating Characteristic Curve (AUC - ROC): is a performance metric used to evaluate the accuracy and discrimination ability of a classification system [11]. It measures the area under the ROC curve, which is a plot of the True Positive Rate (Recall) against the False Positive Rate as the classification system's discrimination threshold is varied.

$$\text{AUC-ROC} = \int_0^1 \text{TPR (FPR) d FPR}$$

(21)

Execution Time (ET): An algorithm's execution time is the overall amount of time it takes for it to run and finish all of its jobs.

$$\text{ET} = ET_{end} - ET_{start}$$

(22)

where, ET_{end} is the time when the algorithm finishes its execution and ET_{start} is the time when the algorithm starts its execution.

5.3.4 Proposed VDTH and TD3 Algorithm

Inputs:
Buffer size, Buffering thresholds, Prediction window size, Prediction accuracy thresholds, Hyperparameters for the TD3 algorithm (actor, critic, learning rate, action noise, noise decay, discount factor, reply buffer size, soft update rate), Network behavior patterns

Outputs:
Detected security threat wormhole attack in the active path
Response to security incidents creates a log indicating a wormhole attack
Take corrective actions: Transmit information related to the attack to all RSUs and Vehicles in the network

Step 1: Initialization
      Message_buffer (Msg_{buffer}), Contact_Prediction_Module (CPM),
      Dynamic_Buffer_Management parameters ($DBM_{parameters}$), TD3 parameters
($TD3_{parameters}$)
Step 2: Define a main loop to handle communication
      def main loop ( )
Step 3: Check if Source Vehicle (SV) generates data to be transmitted, Check if a direct path exists between Source Vehicle (SV) and Destination Vehicle (DV), if exist transmit packets directly, else find neighboring vehicles or RSUs with better connectivity to DV using VDTN routing and forwarding logic.
      $generated_{data}$ = generate_data ( )
      if $generated_{data}$:
            direct_link_avaiable = check_direct_link ( )
            if direct_link_avaiable:
                  transmit_data_directly ( )
      else
            $Suitable_{RSUs}^{vehciles}$ = find_vehicles/RSUs ( )
Step 4: Use Opportunistic data forwarding technique if neighboring vehicles or RSUs are found, if not store data in Msg_{buffer} and implement buffer_management_algorithm
      if $Suitable_{RSUs}^{vehciles}$:
            opportunistically_forward_data ( )
      else
            Msg_{buffer} = $generated_{data}$
            buffer_management_algorithm ( )
Step 5: Opportunistic forwarding and Data delivery
      for each $encountred_{RSUs}^{vehciles}$ // if any suitable vehicle or RSU is within the range
            if $Buffer_{data}$ & $Suitable_{RSUs}^{vehciles}$ // data in buffer and suitable vehicle or RSU available
                  opportunistically_forward_stored_data
                  update_routingtable_based_on_encounter   // routing table updated
Step 6: Implement Adaptive buffer management and energy efficiency
      Adaptive_buffer_management_algorithm ( )
Step 7: CPM
      if CPM
            forecast ( )   // function to forecast opportunities
            $schudle^{proactive}$ // proactively scheduling
Step 8: Data delivery
      $Check_D$ // continuously check if Destination(D) reached (r)
      if $Check_D$ == r   // D reached

$\qquad Delivered_D^{data}$ // data delivered to D

  else

    continue ( )   // continue to search for a path to D or D

Step 9: TD3 to detect wormhole attack

  if $Received_{pkt} == UE_{source}$ // data packet received from unexpected (UE) source

    features = $Extract_{features}^{received\ data}$ // received packets features

    action = $TD3_{features}$ // extract actions using TD3 algorithm

     if action == "wormhole_atatck"

      $raise_{log}^{alert}$ // log the incident and alert the network

      $handle_{WHA}$ // take corrective actions

Step 10: Go to Step 2   // continue further communication

6. Performance Evaluation

A comprehensive examination involves a systematic assessment of the proposed methodology's effectiveness, efficiency, and robustness in addressing VANET security through efficient communication and detecting wormhole attacks [17]. The evaluation aims to provide evidence of the proposed methodology's performance and validate its benefits in a realistic vehicular network environment.

6.1 Simulation Setup

To assess the effectiveness of our suggested strategy and compare it to current intrusion detection methods, we carried out comprehensive tests. The tools and parameters are listed in **Table 5** below

Table 5. Parameters

Slno	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	VDTH
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	6
13	Simulation Environment	1000m X 1000m
14	Frequency	2.4 GHz
15	Transmission Power	33dbm
16	Buffer size (Vehicle)	50 data packets
17	Buffer Size (RSU)	150 data packets
18	Battery Capacity	5000 watt-hours (wh)
19	Energy Threshold	1000 Joules

Our research employs a traffic simulator (SUMO) and a network simulator (NS3). Before using the abovementioned simulators, we produce a live traffic (.OSM) file using an OpenStreetMap where we have taken traffic from the Bangalore map. The .osm file is fed into SUMO, which generates mobility files for the network simulator. The NS3 generates the files listed below while executing the mobility file: Animation file (.XML), Routing table, Flow Monitor, Packet Statistics, etc.

7. Simulation Outcomes

7.1 Packet delivery ratio (PDR): PDR measures the proportion of data packets that are successfully delivered to their intended destination. This statistic is essential for evaluating communication dependability in VANETs.

Parameters used:
- Time: Time is often used as the x-axis in PDR graphs to show how performance varies over time. It allows for the observation of trends and fluctuations.
- Packet Types: Different types of packets may be used in the graph, such as data packets, control packets, or specific types of attack packets.
- Packet Delivery Ratio: This rate reflects the number of packets delivered successfully. It can be represented on the y-axis.
- Attack Simulations: When measuring PDR for attack detection, the graph may include attack scenarios, demonstrating how well the security solution can identify and mitigate attack traffic.

Analysis: The PDR graph allows researchers to draw several important conclusions:
- Performance over Time: Researchers can observe how PDR evolves, providing insights into network stability and responsiveness to changing conditions.
- Comparison: By comparing multiple algorithms or solutions, researchers can assess which one is more effective in maintaining high PDR levels or identifying and mitigating attacks.
- Impact of Scenarios: Different scenarios can reveal how the solutions perform under various conditions, such as high-density traffic or diverse mobility patterns.
- Security Evaluation: When assessing attack detection, the graph may indicate how well the TD3 Algorithm identifies and responds to wormhole attacks.
- Adaptability: Researchers can gauge how well the VDTN Protocol and TD3 Algorithm adapt to network challenges, making them more robust.
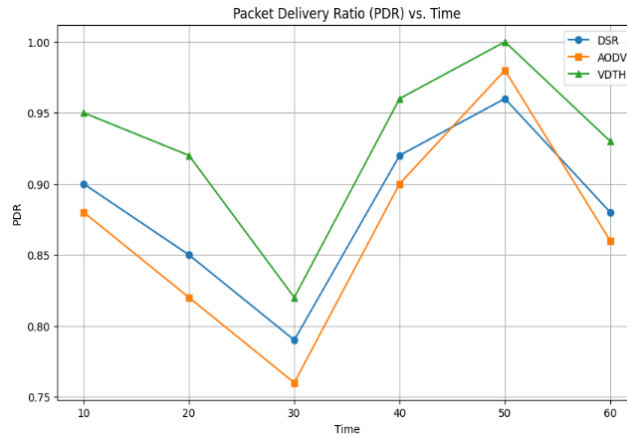
Fig. 4. PDR

7.2 End-to-end delay: The End-to-End Delay is a critical network performance metric that measures the time taken for a data packet to travel from its source to its destination. In the context of VANETs, it reflects the time it takes for a message to reach its intended recipient and plays a crucial role in assessing communication efficiency and reliability.

Parameters Used:
- ➢ Time: Time is typically plotted on the x-axis, representing the duration of the simulation or real-world observations. It allows for the observation of how End-to-End Delay varies over time.
- ➢ End-to-End Delay (ms): The End-to-End Delay, measured in milliseconds (or another appropriate time unit), is plotted on the y-axis. This value represents the average, minimum, or maximum delay experienced by data packets.
- ➢ Packet Types: Different types of packets may be used in the graph, such as data packets, control packets, or specific types of attack packets. Each type can have a separate line on the graph to distinguish their delay characteristics.

Analysis: The End-to-End Delay graph provides several key insights:
- ➢ Latency Patterns: Researchers can observe how End-to-End Delay evolves and assess any patterns or trends. High delays can indicate potential network congestion or inefficiencies.
- ➢ Comparison: By comparing multiple algorithms or solutions, researchers can assess which one provides lower End-to-End Delay, demonstrating its ability to expedite communication.
- ➢ Impact of Scenarios: Different scenarios can reveal how the solutions perform under various conditions, providing an understanding of how End-to-End Delay is affected by factors like traffic density and mobility patterns.
- ➢ Security Evaluation: When evaluating the detection of wormhole attacks using the TD3 Algorithm, the graph may indicate how the delay patterns change in the presence of attacks. Detecting anomalies in delay can be a sign of potential attacks.
- ➢ Efficiency: Researchers can gauge how efficiently the VDTN Protocol and TD3 Algorithm manage communication, leading to lower End-to-End Delay.
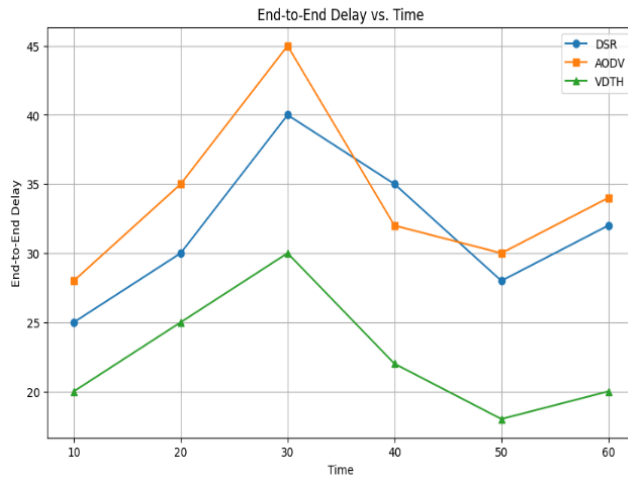
Fig. 5. End-to-end delay

7.3 Throughput: It represents the capacity of the network to transport data efficiently. In VANETs, throughput is a crucial metric for evaluating how well the network can handle data transmission under different conditions.

Parameters Used:

➢ Time: Time is usually represented on the x-axis, indicating the duration of the simulation or real-world observations. It helps in visualizing how throughput varies over time.

➢ Throughput (bits per second or packets per second): The throughput values, typically measured in bits per second (bps) or packets per second (pps), are plotted on the y-axis. These values indicate the rate at which data is successfully transmitted.

➢ Packet Types: Different types of packets may be used in the graph, such as data packets, control packets, or specific types of attack packets. Each type can have a separate line on the graph to distinguish their throughput characteristics.

Analysis: The Throughput graph provides several key insights:

➢ Capacity of the Network: It shows how well the network can handle data transmission, revealing its capacity in terms of bits or packets per unit of time.

➢ Comparison: Researchers can compare the throughput of different algorithms or solutions to identify which one can transmit data more efficiently. Higher throughput generally indicates more effective communication.

➢ Impact of Scenarios: By examining the graph for various scenarios, researchers can understand how changes in network conditions affect the network's throughput. This can include factors like traffic density and mobility patterns.

➢ Security Evaluation: When evaluating the detection of wormhole attacks using the TD3 Algorithm, the graph may show how attack detection influences network throughput. Anomalies in throughput can indicate the presence of attacks.

➢ Efficiency: Throughput graphs help gauge how efficiently the VDTN Protocol and TD3 Algorithm manage communication, leading to higher data transmission rates.
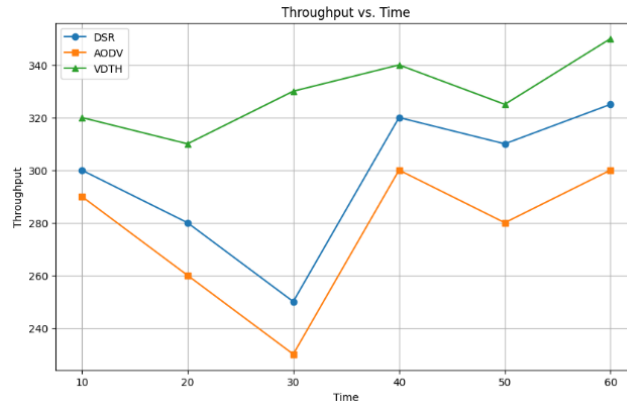
Fig. 6. Throughput

7.4 Efficiency and Overhead: Efficiency refers to how effectively a protocol or system achieves its intended goals while optimizing resource utilization. High efficiency indicates that the system accomplishes tasks with minimal waste and resource consumption, whereas overhead represents any additional data, processing, or resources required by a protocol or system beyond the essential data payload or task. It includes control messages, acknowledgments, error-checking mechanisms, and other auxiliary operations. Lower overhead is desirable as it indicates more efficient resource utilization.

Parameters Used:
  ➢ Time: Time is typically plotted on the x-axis, indicating the duration of the simulation or real-world observations. It allows for the observation of how efficiency and overhead vary over time. b. Efficiency (%): The efficiency values are usually plotted on the left y-axis. These values are expressed as percentages and indicate how well the system achieves its goals.
  ➢ Overhead (%): Overhead values are plotted on the right y-axis. They are also expressed as percentages, representing the additional resources the system consumes.

Analysis: The Efficiency and Overhead graph provide several key insights:
  ➢ Resource Utilization: The graph demonstrates how efficiently the VDTN Protocol and TD3 Algorithm utilize network resources. A higher efficiency with lower overhead indicates efficient resource management.
  ➢ Comparison: Researchers can compare the efficiency and overhead of different algorithms or solutions to identify which one balances the trade-off between resource utilization and task achievement effectively.
  ➢ Impact of Scenarios: The graph allows for an assessment of how changes in network conditions affect efficiency and overhead, such as variations in traffic density or mobility patterns.
  ➢ Security Evaluation: When evaluating the detection of wormhole attacks using the TD3 Algorithm, the graph may indicate how the security measures influence efficiency and introduce overhead.
  ➢ Adaptability: Researchers can gauge how well the VDTN Protocol and TD3 Algorithm adapt to network challenges, making them more efficient and reducing overhead.
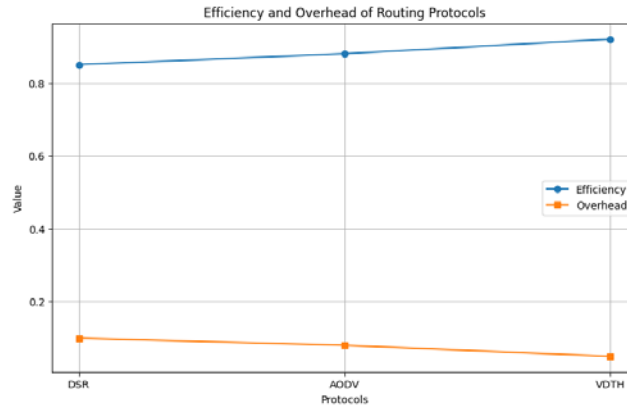
Fig. 7. Efficiency and Overhead

7.5 WHA Detection Rate: The WHA Detection Rate measures the ability of a security solution to identify and detect wormhole attacks in VANET. It is a crucial metric because wormhole attacks are a significant security threat in VANETs, and accurately detecting them is vital to network security.

Parameters Used:
- ➢ Time: Time is typically plotted on the x-axis, indicating the duration of the simulation or real-world observations. It allows for the observation of how the WHA Detection Rate varies over time.
- ➢ WHA Detection Rate (%): The WHA Detection Rate values are plotted on the y-axis, usually expressed as percentages. It represents the percentage of wormhole attacks successfully detected and mitigated by the proposed solution.

Analysis: The WHA Detection Rate graph provides several key insights:
- ➢ Detection Efficacy: It demonstrates how effective the proposed VDTN Protocol and TD3 Algorithm are at identifying and mitigating wormhole attacks. A higher WHA Detection Rate indicates a more effective security solution.
- ➢ Comparison with Existing Solutions: By comparing the proposed solution with existing methods, researchers can assess whether the new approach outperforms or matches the capabilities of established security measures.
- ➢ Impact of Scenarios: The graph allows for an evaluation of how different network conditions affect WHA detection. Researchers can understand how changes in traffic density or mobility patterns influence the solution's ability to detect attacks.
- ➢ Security Evaluation: WHA Detection Rate is a critical security metric, as it measures the system's ability to maintain the integrity and security of VANET communications in the presence of wormhole attacks.
- ➢ Adaptability: Researchers can gauge how well the proposed solution adapts to network challenges and maintains high detection rates under varying conditions.
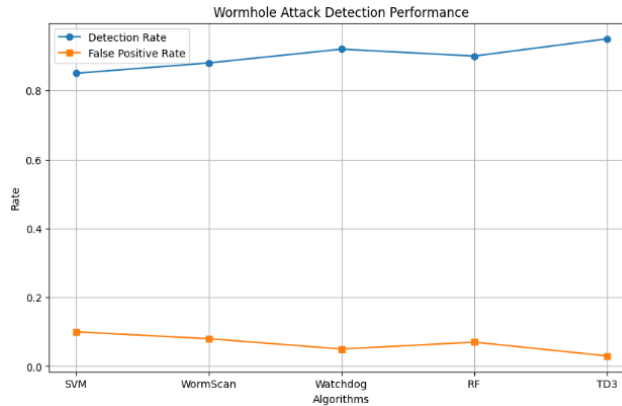
Fig. 8. WHA Detection Rate

7.6 Overall Attack Detection Performance: The Overall Attack Detection Performance graph assesses the effectiveness of a security solution, such as the proposed TD3 Algorithm, in identifying and mitigating a range of attack types in a VANET. This is a holistic measure of the system's security capabilities.

Parameters Used:
- ➢ Time: Time is typically plotted on the x-axis, indicating the duration of the simulation or real-world observations. It allows for the observation of how the Overall Attack Detection Performance varies over time.
- ➢ Detection Performance (%): The detection performance values are usually plotted on the y-axis and expressed as percentages. They represent the success rate of the system in identifying and mitigating attacks.
- ➢ Comparison with Proposed and Existing Solutions: The graph may include multiple lines or data points representing different approaches. This includes the proposed solution (VDTN Protocol and TD3 Algorithm) and existing security methods for VANETs. These lines enable a direct comparison.

Analysis: The Overall Attack Detection Performance graph provides several key insights:
- ➢ Comprehensive Security Assessment: It offers a holistic view of the system's security capabilities by measuring its effectiveness in detecting various types of attacks, both known and potential threats.
- ➢ Impact of Scenarios: The graph enables an evaluation of how different network conditions affect the system's ability to detect attacks. This includes changes in traffic density, mobility patterns, and the intensity of attacks.
- ➢ Security Evaluation: The graph helps researchers understand the system's ability to maintain the security and integrity of VANET communications in the presence of a wide range of security threats.
- ➢ Adaptability: Researchers can gauge how well the proposed solution adapts to different attack scenarios and maintains high detection performance under varying conditions.
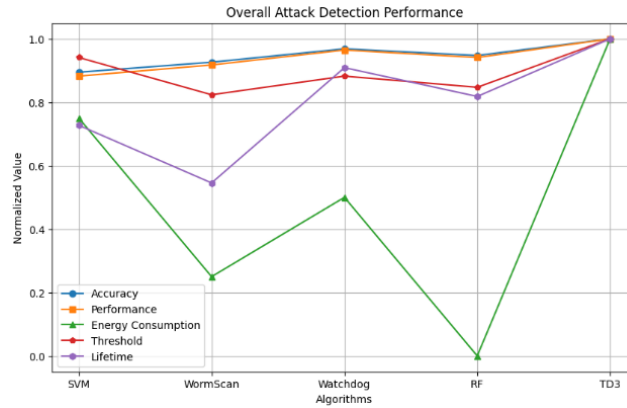
Fig. 9. Overall Attack Detection Performance

7.7 Performance improvements achieved:

Authors have used tools such as SUMO, NS3, and OpenStreetMap to extract live traffic to generate simulation scenario. First, we extract live traffic using OpenStreetMap which generates (.OSM) file the .osm file is fed into SUMO, which generates mobility files for the network simulator. The NS3 generates the files listed below while executing the mobility file: Animation file (.XML), Routing table, Flow Monitor, Packet Statistics, etc.

By integrating VDTN and TD3 authors have enhanced the communication and security where VDTN protocol is used to make sure critical messages reach their destination even when the target vehicle or RSU is not within the range of the source by employing store and forward technique, in case of attack detection TD3 algorithm which learning continuously, handles high dimensional data increases detection rate of attacks than the existing IDS.

The performance improvements achieved using simulations are:

An increase in PDR, improvement in WHA detection rates, a substantial reduction in overhead, an increase in efficiency and increase in throughput, reduction in end-to-end delay. These advancements collectively culminate in an overall enhancement of VANET performance.

8. Robustness of the Proposed Methodology

The proposed methodology's robustness is measured by its capacity to maintain efficiency and dependability regardless of the numerous kinds of difficult circumstances and variations that are frequent in VANET networks [6].

8.1 Advantages of the Proposed technique

The advantages of the proposed methodology in the VANET environment are discussed in the **Table 6** below.

Table 6. Robustness

Slno	Parameter	Description
1	Effectiveness in Dynamic VANET Environments	Even in dynamic VANET networks with constantly shifting vehicle positions, network topologies, and communication situations, the concept is still effective. It can adjust to the variations and uncertainties that come with vehicular networks.
2	Resilience to Network Disruptions	The proposed approach is capable of addressing network partitions and communication delays that result in periodic connectivity. Even in the face of disturbances, it guarantees that the VANET continues to be secure and functional.
3	Adaptive Wormhole Attack Detection	Given its adaptability, the TD3 Algorithm can recognize not only straightforward wormhole attacks but also more complex and evolving variations. It can modify its detection methods to recognize new attack patterns.
4	Managing Data Variability and Noise	The methodology demonstrates robustness against noise and data variability that may result from changes in the communication channel, vehicle motion, or environmental conditions. It is capable of effectively separating noise from actual communication.
5	Low False Positive Rate	The methodology aims to reduce the likelihood of incorrectly identifying lawful communication as a wormhole attack by maintaining a low false-positive rate. As a result, unneeded disruptions are reduced, and there is a high degree of confidence in the threats that have been detected.
6	Efficiency and Scalability	The proposed approach is made to be scalable, allowing it to handle bigger VANET deployments without suffering appreciable performance deterioration. Additionally, it is energy-efficient, thereby decreasing the additional pressure on vehicular networks.
7	Generalization Capability	The methodology is not constrained by particular circumstances or training data and can generalize its detection abilities to a variety of VANET scenarios. Across a variety of VANET techniques, it can reliably identify wormhole attacks.
8	Real-World Validation	Extensive testing and validation utilizing real-world VANET datasets or accurate simulation models show that the proposed methodology is robust. It goes through a comprehensive review process to guarantee its reliability and effectiveness in real-world circumstances.
9	Ability to Adjust to VANET Dynamics	The approach is flexible enough to adjust to VANET dynamics, including shifting vehicle density, communication ranges, and mobility patterns. It keeps working well even as network circumstances change.

8.2 Future Research Directions

The proposed technique uses the TD3 Algorithm and VDTN Protocol to improve VANET security, and it also offers several promising features and benefits. Its potential outcomes, and possibilities for further development are highlighted in this section [12]:

- *Efficient Communication:* Even in situations of infrequent connectivity and dynamic topology, the VDTN Protocol's integration allows for effective communication in VANETs. By utilizing store-and-forward procedures, communication problems common in vehicular networks are resolved, and message delivery is ensured.

- *Wormhole detection using TD3:* The TD3 Algorithm's ability to recognize both simple and complex wormhole variants is demonstrated by its use in the detection of wormhole attacks [8]. Due to the algorithm's adaptive nature, which allows it to change and modify its detection strategies, dynamic VANET scenarios are ideal for it.

- *Robustness and Resilience:* By continuing to function under a variety of VANET scenarios, tolerating disruptions, and successfully separating genuine communication from noisy data, the approach exhibits robustness [7]. Its suitability for VANET installations in the real world is improved by its robustness to network dynamics and uncertainty.

- *Balancing False Positive and False Negative Rates:* To ensure accurate wormhole attack detection and minimize unnecessary interference with legitimate communication, the technique seeks to establish a balance between false positive and false negative rates [15]. Its overall performance can be better understood using the F1-Score and AUC-ROC measurements.

- *Scalability and Energy Efficiency:* In VANETs with limited resources, scalability and energy efficiency must be taken into account. These issues are addressed in the methodology's design, which enables it to be used in larger network deployments without dramatically raising computing overhead.

- *Adaptability and Generalization:* Due to the TD3 Algorithm's capacity to learn and generalize from a variety of data, the methodology demonstrates adaptability to many VANET scenarios. Its practical value is increased by the fact that it may be used in numerous VANET implementations [10].

- *Real-World Validation:* Using VANET datasets or simulations, the proposed methodology is systematically validated and tested in the real world. Its dependability and efficiency in real-world scenarios are ensured by this experiential evaluation.

- *Future Research Opportunities:* Despite its advantages, more research is needed in several areas. Investigating machine learning methods for better feature extraction, optimizing threshold values, and resolving privacy and security issues in VANET communication are possible research areas.
  Example: Types of privacy and security challenges that need to be addressed
  o *Location Privacy:* One of the critical challenges is protecting the location privacy of vehicles. While it's essential for vehicles to share their positions for safety and traffic management, this information must be anonymized to prevent tracking of individual vehicles. Future research can focus on developing efficient pseudonym-changing strategies and location obfuscation techniques to preserve driver privacy.
  o *Message Authentication:* Ensuring the authenticity of messages in VANETs is a significant challenge. Vehicles need to be able to trust the information they receive from other vehicles and infrastructure. Research can explore advanced cryptographic techniques and secure authentication mechanisms to verify the integrity and origin of messages, preventing malicious actors from injecting false data.

    o *Privacy-Preserving Data Aggregation:* Research can focus on privacy-preserving techniques for data aggregation. This would allow for the collection and analysis of VANET data without revealing individual vehicles' sensitive information. Privacy-enhancing technologies like secure multi-party computation can be explored to enable data aggregation while protecting privacy.

    o *Denial of Service (DoS) Attacks:* DoS attacks can disrupt communication in VANETs, impacting safety-critical applications. Future research can focus on developing resilient communication protocols that can withstand DoS attacks and continue to operate effectively.

    o *Vulnerable Onboard Units (OBUs):* OBUs are potential weak points in VANET security. Researchers can explore techniques to secure these units against tampering and unauthorized access.

While the proposed technique offers several advantages, there are still areas where further research is needed

    o *Trustworthiness of legitimate users:* Only legitimate vehicles with valid credentials can enter the network. There is a possibility that these vehicles can turn into attackers; identifying such attackers is a challenging task in a dynamic environment such as VANET. A strong and trustworthy technique is required to identify such vehicles before they can turn into attackers and cause any damage.

    o *Interoperability:* Research is needed to address interoperability challenges, especially when VANETs interact with different communication technologies, such as 5G networks. Developing standards and protocols that allow seamless integration is essential.

    o *Cross-Border Communication:* Develop solutions that facilitate cross-border communication and cooperation, ensuring that vehicles can seamlessly communicate across different regions with varying standards and regulations.

    o *Reliability in Harsh Conditions:* Research solutions that enhance VANET reliability in challenging conditions, such as adverse weather, low visibility, and heavy traffic, to ensure the continuous flow of critical safety information.

- *Integration with Cross-Layer Security Approaches:* Collaboration and cross-layer security techniques may further improve VANET security as a whole. A thorough security framework could be developed by combining the proposed approach with other defense mechanisms in future studies.

- *Impact of Emerging VANET Technologies:* The methodology's flexibility and adaptability to new hardware and communication protocols should be taken into account as VANET technologies develop.

- *Real-World Deployment Challenges:* Real-world deployment issues for the proposed methodology could include hardware limits, network heterogeneity, and time constraints [20]. To ensure successful deployment, future research should address these issues.

8.3 Integration with Emerging Technologies

Improving the security, effectiveness, and functionality of VANETs requires integration with emerging technologies. Key integration aspects to think about are as follows:

- *Edge Computing:* Leveraging edge computing resources within vehicles and infrastructure can reduce latency in data processing and decision-making. Edge computing enables faster responses to critical situations, such as collision avoidance, and supports the deployment of AI-driven applications in VANETs.
- *Blockchain Technology:* Blockchain can provide a secure and immutable ledger for VANET communications and transactions. It can enhance data integrity, privacy, and the trustworthiness of information exchanged among vehicles.
- *Environmental Sensors:* Integration with environmental sensors can provide real-time data on air quality, temperature, and other environmental factors. This data can be used for route planning and to warn drivers of adverse conditions.
- *Augmented Reality (AR) and Virtual Reality (VR):* AR and VR technologies can enhance driver assistance systems by providing drivers with augmented views of their surroundings, real-time traffic data, and safety alerts.
- *Heterogeneous Networks:* VANETs should be able to adapt to various network types, including cellular, Wi-Fi, and ad-hoc networks. This adaptability ensures continuous communication even in areas with varying network infrastructures.
- *Drone Integration:* Drones can be used to collect traffic data and provide emergency response support. Integrating VANETs with drone technology enhances the network's capabilities for monitoring and managing traffic.

8.4 Critical challenges and their role in the broader transportation and communication landscape

VANETs are a critical component of the broader transportation and communication ecosystem, and their reliability and performance are integral to achieving privacy and security goals. By addressing, these challenges that are of paramount significance, as they have a direct impact on the ability of VANETs to enhance transportation safety, efficiency, and sustainability. The proposed VDTN Protocol and TD3 Algorithm offer solutions to these challenges, making them vital contributions to the field of VANET research.

1) Safety Enhancement: Vehicles communicate with each other and with infrastructure, facilitating real-time exchange of critical safety information. In our proposed technique we address this challenge by using the VDTH protocol that uses the store and forward method to ensure that this safety-enhancing communication remains reliable and resilient, reducing the risk of accidents and saving lives.

2) Cyber security: As VANETs become more interconnected, they become susceptible to cyber security threats, including attacks such as wormhole attacks or attacks on communication channels. The authors address these challenges by employing a DRL algorithm known as TD3, which detects the attacks performed on the network to safeguard against malicious activities that could compromise safety and data privacy.

3) Resource Efficiency: VANETs often involve resource-constrained devices. Ensuring the efficient use of limited communication bandwidth and computational resources is critical for scalability and sustainability. By integrating the features of VDTN and TD3 challenges such as optimizing resource usage and network performance are resolved.

4) Adaptive Traffic Management: VANETs enable adaptive traffic management that responds in real-time to changing traffic conditions. Employing the TD3 algorithm which learners continuously, handle high-dimensional data and adapt to the current environment will ensure

that these systems can adapt effectively and reduce congestion, minimize delays, and optimize traffic flow.

5) Scalability: As the number of vehicles on the road increases, addressing scalability challenges is vital. VANETs need to accommodate a growing number of vehicles while maintaining high performance and security. As mentioned in point no. (4) The TD3 adapts to the changing scenario in terms of growing and shrinking vehicles and surroundings like urban, highways, etc.

10. Conclusion

The integration of the Vehicular Delay-Tolerant Networking (VDTN) protocol with the Twin Deep Deterministic Policy Gradient (TD3) algorithm has produced promising advancements in strengthening the communication and security issues within Vehicular Ad Hoc Networks (VANETs). The fundamental premise of VDTN, rooted in its ability to navigate intermittent connectivity and communication delays inherent in vehicular environments, has proven crucial in ensuring reliable data transmission. The results of our experiments demonstrated how well the VDTN protocol handles communication breakdowns. VDTN successfully reduced the effects of network splits and sporadic connectivity by employing store-and-forward and opportunistic data forwarding strategies, making data distribution possible even in difficult VANET scenarios. Concurrently, the integration of the TD3 algorithm emerged as a potent defense mechanism against wormhole attacks, a prevalent threat in VANETs. TD3 adeptly detected and prevented these attacks by generating dynamic thresholds and identifying anomalous packet transmission patterns, thereby safeguarding the integrity and confidentiality of data exchanges among vehicular nodes. Our innovative technique outperforms existing systems with a superior increase in key stages, including an 8% increase in Packet Delivery Ratio (PDR), outstanding 10% WHA detection rates, an appreciable 11% reduction in overhead, and an exceptional 13% increase in overall operational efficiency. Furthermore, a commendable 7% increase in throughput is correlated with an 8% reduction in end-to-end delay, resulting in an extraordinary 9% enhancement in VANET performance.

Future research in this domain will focus on the incorporation of additional Deep Reinforcement Learning (DRL) algorithms to detect and mitigate Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, aiming to establish a comprehensive and robust security framework for vehicular networks.

Acknowledgment

References

[1]   B, Santhosh and Lohiya, Dr. Harsh and Rani, Dr. B. Kavitha, "Detection Technique in Delay Tolerant Networks Using Rid and VDTN Frame Work," *SSRN*, June 21, 2022. Article (CrossRef Link)

[2]   Z. Du et al., "A Routing Protocol for UAV-Assisted Vehicular Delay Tolerant Networks," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 85-98, 2021. Article (CrossRef Link).

[3] E. Khoza, C. Tu and P. A. Owolawi, "Comparative Study on Routing Protocols for Vehicular Ad-Hoc Networks (VANETs)," in *Proc. of International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, Durban, South Africa, pp. 1-6, 2018. Article (CrossRef Link)

[4] L. R. Gallego-Tercero, R. Menchaca-Mendez, M. E. Rivero-Angeles and R. Menchaca-Mendez, "Efficient Time-Stable Geocast Routing in Delay-Tolerant Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 8, pp. 171034-171048, 2020. Article (CrossRef Link).

[5] Ruiz, P.M., Cabrera, V., Martínez, J.A., & Ros, F.J., "BRAVE: Beacon-less routing algorithm for vehicular environments," in *Proc. of the 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010)*, 709-714, 2010. Article (CrossRef Link).

[6] Teixeira, L. H., & Huszák, Á, "Reinforcement Learning Environment for Advanced Vehicular Ad Hoc Networks Communication Systems," *Sensors*, 22(13), 4732, 2022. MDPI AG. Retrieved from Article (CrossRef Link).

[7] R. A. Nazib and S. Moh, "Reinforcement Learning-Based Routing Protocols for Vehicular Ad Hoc Networks: A Comparative Survey," *IEEE Access*, vol. 9, pp. 27552-27587, 2022. Article (CrossRef Link).

[8] V. K. K and G. Reddy, "A Delay Sensitive Multi-Path Selection to Prevent the Rushing Attack in VANET," in *Proc. of 5th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, pp. 1-7, 2021. Article (CrossRef Link).

[9] Krishna, K. V., & Reddy, K. G., "VANET Vulnerabilities Classification and Countermeasures: A Review," *Majlesi Journal of Electrical Engineering*, 16(3), 63-83, 2022. Article (CrossRef Link).

[10] Devi, T. K., Mohanakrishnan, R., & Karthick, T, "Secure Message Broadcasting in VANET Using RSU based Authentication and Cascade Encryption," *Webology*, 17(2), 706-716, 2020. Article (CrossRef Link).

[11] Vitalkar, R. S., Thorat, S. S., & Rojatkar, D. V, "Intrusion detection for vehicular ad hoc network based on deep belief network," in *Proc. of Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021*, pp. 853-865, 2022.

[12] Polat, H., Turkoglu, M., & Polat, O., "Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET," *IET Communications*, 14(22), pp. 4089-4100, 2020. Article (CrossRef Link).

[13] Almalki, S. A., Abdel-Rahim, A., & Sheldon, F. T, "Adaptive IDS for Cooperative Intelligent Transportation Systems Using Deep Belief Networks," *Algorithms*, 15(7), 251, 2020. Article (CrossRef Link).

[14] Kashyap, A. A., Raviraj, S., Devarakonda, A., Nayak K, S. R., KV, S., & Bhat, S. J, "Traffic flow prediction models–A review of deep learning techniques," *Cogent Engineering*, 9(1), 2022. Article (CrossRef Link).

[15] Azzoug, Y., & Boukra, A, "Bio-inspired Probabilistic Opportunistic Routing for Vehicular Delay-Tolerant Networks Using a Hybrid Swarm Approach," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 15(2), 17–27, 2023. Article (CrossRef Link).

[16] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, B. A. S. Al-Rimy, F. Saeed and T. Al-Hadhrami, "Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network," *IEEE Access*, vol. 7, pp. 159119-159140, 2019. Article (CrossRef Link).

[17] A. Haydari and Y. Yilmaz, "RSU-Based Online Intrusion Detection and Mitigation for VANET," *Sensors*, vol. 22, no. 19, p. 7612, Oct. 2022. Article (CrossRef Link).

[18] Bayat, Majid and Pournaghi, Morteza and Rahimi, Majid and Barmshoory, Mostafa, "NERA: A New and Efficient RSU Based Authentication Scheme for VANETs," *Wireless Networks*, vol. 26, pp. 3083-3098, 2020. Article (CrossRef Link).

[19] Jyothi, N., & Patil, R, "A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET," *Journal of Information and Telecommunication*, 6(3), 270-288, 2022. Article (CrossRef Link).

[20] Azam, F., Yadav, S. K., Priyadarshi, N., Padmanaban, S., & Bansal, R. C, "A comprehensive review of authentication schemes in vehicular ad-hoc network," *IEEE access*, 9, 31309-31321, 2021. Article (CrossRef Link)

[21] Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X., & Zeng, X, "A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network," *IEEE Access*, 7, 154560-154571, 2019. Article (CrossRef Link).

[22] Feng, X., & Tang, J, "Obfuscated RSUs vector based signature scheme for detecting conspiracy Sybil attack in VANETs," *Mobile Information Systems*, 2017. Article (CrossRef Link).

[23] M. Hanif et al., "AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks," *Electronics*, vol. 11(15), 2022. Article (CrossRef Link).

[24] Saini, P.K., Singh, A. & Sohal, J.S, "Proactive Prevention Key Solution for Wormhole Attack IEEE 802.11 Networks Using AODV," *Wireless Pers Communication*, vol. 128, pp. 89-108, 2023. Article (CrossRef Link).

[25] Ali, Shahjahan, and Nand, Parma and Tiwari, Shailesh, "Detection of Wormhole Attack in Vehicular Ad-hoc Network over Real Map using Machine Learning Approach with Preventive Scheme," *Journal of Information Technology Management*, vol. 14, pp. 159-179, 2022. Article (CrossRef Link).

[26] Singh, S., Saini, H.S, "Intelligent Ad-Hoc-On Demand Multipath Distance Vector for Wormhole Attack in Clustered WSN," *Wireless Personal Communication*, vol. 122, pp. 1305-1327, 2022. Article (CrossRef Link).

[27] Mehetre, D.C., Roslin, S.E. & Wagh, S.J., "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," *Cluster Computing*, vol. 22, pp. 1313-1328, 2019. Article (CrossRef Link).

[28] T. Kamaleshwar, R. Lakshminarayanan, Yuvaraja Teekaraman, Ramya Kuppusamy, Arun Radhakrishnan, "Self-Adaptive Framework for Rectification and Detection of Black Hole and Wormhole Attacks in 6LoWPAN," *Wireless Communications and Mobile Computing*, 2021. Article (CrossRef Link).

[29] G. Raja, S. Anbalagan, S. Senthilkumar, K. Dev, and N. M. F. Qureshi, "SPAS: Smart Pothole-Avoidance Strategy for Autonomous Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19827-19836, 2022. Article (CrossRef Link).

[30] Hafsa Shahid, Humaira Ashraf, Hafsa Javed, Mamoona Humayun, Nz Jhanjhi, Mohammed A. AlZain, "Energy Optimised Security against Wormhole Attack in IoT-Based Wireless Sensor Networks," *Computers, Materials & Continua*, vol. 68(2), pp. 1967-1981, 2021. Article (CrossRef Link).

[31] Kang, J., & Kang, W., "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security," *PLOS ONE*, 11(6), e0155781, 2016. Article (CrossRef Link).

[32] Singh, P.K., Gupta, R.R., Nandi, S.K., Nandi, S., "Machine Learning Based Approach to Detect Wormhole Attack in VANETs," in *Proc. of WAINA 2019: Web, Artificial Intelligence and Network Applications*, pp. 651-661, 2019. Article (CrossRef Link).

Mr. Vamshi Krishna K ⓘ received his B.Tech degree in Computer Science and Engineering from Rao Bahadur Y. Mahabaleswarappa Engineering College (RYME), Bellary affiliated with Visvesvaraya Technological University (VTU) in 2009, and his M.Tech degree in CSE from the Jain University Global campus Kanakapura, Bangalore, in 2012. At present, he is pursuing his PhD under the guidance of Dr. Ganesh Reddy K at VIT-AP University. He has published three papers on network security and one IEEE conference in the area of information security in VANET. His main research areas are information security and computer networks.

Dr. K. Ganesh Reddy ⓘ received his B.Tech degree in Information Technology from Andhra University, in 2007 and his M.Tech degree in Information Security from the National Institute of Technology Rourkela (NITR), Orissa, in 2010. He was awarded a Ph.D. degree in computer science and engineering from the National Institute of Technology Karnataka (NITK) Surathkal, in 2014. At present, he is working as an associate professor at VIT-AP University. He has published twenty international conference and journal articles and two national conferences in the area of wireless and information security. He is an editorial board member of the Journal of Information and has reviewed IEEE, Springer international conference articles, and Wiley, Hindawi, and Oxford journal articles. His main research areas are information security, cloud computing, algorithm design, and computer networks. He is an Associate Member of the National Cyber Safety and Security Standards (NCSSS) India, and a member of the Institution of Engineers (India). He is a certified security analyst by NCSSS.