Securing VANET from Sybil Attack using ECC, DSA, SAD and Detecting using Hybrid Model

[1] K. Madhushri, [2] Dr.R.Arockia Xavier Annie

[1]Assistant Professor, [2]Associate Professor
[1]Computer Science and Engineering,
[1]Sathyabama Institute of Science and Technology, Chennai, India
[1]karunagaranmadhushri@gmail.com, [2]annie@annauniv.edu

Abstract— **In VANETs keeping communications safe matters for transport systems to work well. The Sybil attack may cause many problems, such as spreading false traffic details, unauthorized use of important services and even car crashes. This study tries to build a strong way to spot such attacks by using the Elliptic Curve Cryptosystem, Digital Signature Algorithm and Sybil Attack Detection (SAD) Algorithm to reduce this risk. The main aim is to design a system to handle Sybil attacks in VANET. The Elliptic Curve Cryptosystem will make separate identities for each vehicle and the Digital Signature Algorithm will mark messages moreover check if they are real. Detect Sybil attack from VANET Dataset using hybrid model. We propose a method that pairs CNNs with a pre-trained VGG16 architecture to catch Sybil attacks in VANETs. The approach uses a set of features that covers vehicle ID, fake messages, geographical ID, attack type along with attack source to identify Sybil assaults in the network. VGG16 and transfer learning take advantage of the pre-trained model's ability to show deep details, which helps with both feature extraction moreover classification. The procedure helps adjust model settings to improve training accuracy and lower loss. To speed up learning moreover boost performance, it uses Particle Swarm Optimizer (PSO) to change network weights. Testing shows that the combined CNN-VGG16 and PSO method can reliably spot Sybil attacks in VANETs, which strengthens the security and reliability of vehicle communication systems.**

Index Terms— **VANET,ECC,DSA,SAD,VGG16,CNN,PSO,Sybil,Omnet IDE.**

I. Introduction

Vehicular Ad-Hoc Networks (VANETs) are a type of Mobile Ad-Hoc Networks (MANETs). They let vehicles and road structures talk to each other. VANETs help make roads safer, control traffic better next to offer different services for drivers furthermore passengers. Elliptic curves over finite fields have a math framework. This framework forms the base of the Elliptic Curve Cryptosystem (ECC), a method that uses public keys to hide data. ECC gives strong protection while using small keys. It fits well in settings that have few resources, like small computer systems and mobile tools. VANETs use different ways to send messages. One way is through cell networks and DSRC. DSRC is a short-range wireless tool made for cars. In a Sybil attack, a bad node acts as if it were several good ones by making up multiple false identities.

Convolutional Neural Nets (CNNs) are specifically designed to handle organized, grid-like input, including spatial data and images. Their ability to automatically learn hierarchical feature representations straight from raw input data has revolutionized a number of industries, most notably computer vision jobs. Convolutional, pooling, and fully linked layers are the three main components of a CNN. Even while VANET data may not seem like traditional photographs, the hierarchical feature extraction capabilities of VGG16 can still be useful in extracting relevant properties from your input data. This technique allows you to fine-tune the deep representations that VGG16 has acquired to better suit your specific detection objective.

In PSO, the search space is scanned by a population of possible solutions called particles in an attempt to find the optimal solution. Every particle, which represents a potential resolution to the optimization problem, is described by its position and velocity inside the search space. Every particle, which represents a potential resolution to the optimization problem, is described by its position and velocity inside the search space.

II. Related works

A. ELLIPTIC CURVE CRYTOSYSTEM

An NERA Scheme which is proposed for secure vehicle communication by Hongyuan Cheng and Yining Liu [1] but for some attacks NERA Scheme is not sufficient so the author suggests an improved RSU based authentication scheme with Elliptic Curve Cryptosystem(ECC) to make the System more Secure and more Efficient. In this paper they proposed tamper- proof based technique that generates pseudonyms and signatures using the system master key stored in the vehicle's tamper-proof device (TPD). Regular updates to the system master key are necessary for communication security. Recently, the NERA system for secure vehicle communications has been proposed to update the master key more efficiently. Nonetheless, the NERA program is susceptible to some security risks, including identity theft and impersonation assaults. Consequently, an enhanced RSU-based authentication system utilizing an Elliptic Curve. For some Advanced Attacks The NERA Scheme is not Sufficient to provide the Authentication and Security to the System.

B. PROOF OF WORK METHOD

Proof of Work Method by Mohamed Baza , Mahmoud Nabil, Mohamed M.E.A. Mahmoud, Niclas Bewermeier, Kemel Fidan, Waleed Alasmary and Mohamed Abdallah [13] suggests this algorithm for signed time- stamped tag is provided by each roadside unit (RSU) as evidence of the vehicle's anonymous position. A trajectory is created using proofs transmitted by several consecutive RSUs, and this trajectory serves as the vehicle's anonymous identity. Furthermore, one RSU's contributions are insufficient to form trajectories. Multiple RSU contributions are required. In order to fabricate false information, attackers must compromise an impractical amount of RSUs paths. Additionally, after an RSU provides verification of position, the car needs to solve a computational challenge by running algorithm for proof of work (PoW). After that, before obtaining a proof of work, it must present a legitimate solution to the following RSU. The vehicle must provide the event management with the most recent trajectory. The event management then use a matching method to determine the routes transmitted by Sybil automobiles. The plan is predicated on the Sybil trajectories being physically restricted to a single vehicle.

C. SESSION KEY APPROACH

A Session Key Approach is Suggested by Ravi Prakash, Kamal Soni [3] where the technique is used to detect Sybil attack in VANET. The Author Suggest the Session key approach to detect the ID of the Vehicles so that they can be tracked easily and the attack could possibly avoid. The Improved Session key requires less number of arithmetic calculations so that the response time of the vehicles and the server is reduced. It provides privacy to the drivers by using anonymous identity. So it is reliable for the Safety driving with reliable information. The enhanced session key approach described in the study dynamically creates the local certificate needed for the cars to communicate within VANET. In this Paper researcher used Session key based certificate algorithm where it only checks the Vehicle ID from the Vehicle ID the Corresponding Authority of VANET will issue the Key to the Vehicles. While Generating the Session Keys for the Sender will slow down the response times and reduce the performance of the System because, after creating a session key, you must always send the keys to the sender and wait for their acknowledgement.

D. SUPERVISED ML MODELS

Supervised ML Models Suggested by Prinkle Sharma, Hong Liu to detect the Sybil Attack in VANET. The author used Supervised ML Models like Support Vector Machine (SVM), Random Forest Classifier (RF), Naïve Bayes , K Means to detect the sybil attack where they used all the ML Models combined to detect the Sybil attack in the VANET where the author gets the detection accuracy as 87%. This Model finds difficult to detect the multiple attacks at a time so author suggests to implement some other Unsupervised Model for Multiple Attack detection.

E. DEEP LEARNING BASED HUMAN COGNITIVE PRIVACY FRAMEWORK

Deep Learning based Human Cognitive Privacy Framework by Francesco Schiliro, Nour Moustafa, Imran Razzak and Amin Beheshti [16] it is used to detect the attack from the network. DeepCog, a unique deep learning- based human cognitive privacy framework that protects users' privacy by utilizing feature transforming normalization. The encoded data is further processed using a deep MLP model to categorize samples based on an integer-based subject ID, allowing the framework to choose the appropriate secondary deep MLP model to detect eye activity (one for each person). This model achieves the accuracy of 93.8% .

F. HYBRID DEEP LEARNING MODEL

Hybrid Deep Learning Model like CNN with Bidirectional LSTM by Ankita Sharma, Shalli Rani, Syed Hassan Shah, Rohit Sharma and Mohammad Mehedi Hassan [17] where it shows an issue of detecting only the specific attack. This proposed system is used to detect DOS attack from VANET. Based on the crucial parameter security, this study addressed a fundamental component of intrusion detection systems (IDS) in light of the increased frequency of security and privacy threats in health care networks nowadays. The shortcomings of IDS in terms of implementing private controls and responding to cyberattacks in the context of smart health care have inspired this investigation . So the authors of this paper proposed an effective and portable deep learning-based CNN-Bidirectional LSTM is a suggested method for DDoS detection that classifies traffic flows as benign and malicious in this study using the properties of convolutional neural networks (CNNs).

G. LONG SHORT TERM MEMORY (LSTM) MODEL

Received Signal Strength Indicator (RSSI) and Voice Print model for detecting Sybil attack in VANET by Izhar Ahmed Khan , Nour Moustafa, Dechang pi, Bentain Li [19]. In this research suggests to detect the Malicious Activities from Autonomous Vehicles in VANET where it uses the algorithm of LSTM (Long Short Term Memory) where it uses to detect the sybil attack from VANET it is used for Classifying the malicious activities from the vehicle and detect them from the VANET by Deep Learning technique. The proposed framework has real-time automatic intrusion detection capabilities. The proposed framework is built on a deep learning- centered normal state architecture. AVs use a bidirectional Long Short Term Memory (LSTM) architecture to effectively identify intrusions from their communication networks and basic network gateways. The UNSWNB-15 data source for external network communications and the car hacking data source for in-vehicle communications are the two benchmark data sources used to assess the developed framework. This model will detect the attack only under the small scale data so author suggests to work on with real world scenario to improve the system in detection of multiple attacks.

H. BROAD LEARNING SYSTEMS (BLS)

Broad Learning System (BLS) where it is used to detect the sybil attack from VANET by Xiao Wang , Yushan Zhu, Linyao Yang [18] authors Suggested the vehicle misbehavior detection system uses a novel approach by introducing the Broad Learning System (BLS). To optimize the utilization of vehicle data, essential characteristics are initially taken out of the gathered unprocessed data. In this paper they have used BLS method to effectively and efficiently compute the network's link weight using the ridge regression approximation. An incremental learning algorithm based on the freshly created data in IoV can update and improve the system.

By using BLS (Broad Learning System) for classifying the attack in VANET, this method works fine with small data and finds difficult is the data becomes large.

III. *ARCHITECTURE OF VANET*

On-Board Units (OBUs): OBUs, which are installed in individual cars and function as the main communication devices for sending and receiving data in the VANET, are shown in figure

(1). Typically, these units have computer power, wireless transceivers (such Wi-Fi or Dedicated Short-Range Communication, or DSRC), and GPS for location awareness.

Roadside Units (RSUs): RSUs are stationary components that are positioned alongside road infrastructure, including overhead signs, lampposts, and traffic lights (see figure 1). They give cars an extra degree of connectivity and communication support. Road condition monitoring, emergency alerts, traffic light control, and other services are made possible by RSUs' ability to convey information between vehicles and the infrastructure.

Communication Protocols: VANETs use communication protocols designed specifically for use in moving vehicles. Operating in the 5.9 GHz frequency spectrum, IEEE 802.11p is one of the most widely used protocols. Rapid and dependable short-range communication between neighboring cars and RSUs is made possible by this protocol.

Networking Layer: In VANET architecture, data packet routing between OBUs and RSUs is controlled by the networking layer. It contains protocols for route management, route discovery, and dynamic network construction. Routing algorithms must adjust to regularly changing network topologies since VANETs are very dynamic networks.

Vehicle to Vehicle Communication (V2V) : Vehicle-to-vehicle (V2V) communication is the exchange of information between moving automobiles on the road to improve safety, efficiency, and traffic management. Wireless communication technology, which typically simplifies this connection, allows vehicles to share data in real time.

Vehicle to Vehicle Infrastructure (V2I): Communication between cars and roadside infrastructure, such as traffic signals, signs, and sensors, further improves traffic management and safety.

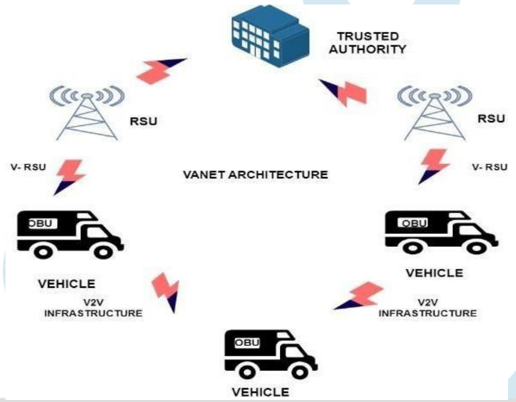

Fig 1. ARCHITECTURE OF VANET

IV. ATTACKS ON VANET

VANET features include high mobility, real-time guarantee, location awareness, privacy and authentication, and delay .VANET is under constant attack. Here are some descriptions of some of them:

Sybil Attack: A malicious node creates several false identities in order to pose as numerous genuine nodes in a Sybil attack. Numerous trust and security problems may result from this.

Denial of Service (DoS) Attack: A Denial of Service (DoS) attack seeks to stop the VANET from operating normally by flooding the network with bogus requests and traffic, making it inaccessible to authorized users.

Gray Hole Attack: A harmful node chooses to throw away certain packets while sending others in a gray hole attack. This action can upset the network's routes and messages.

Black Hole Attack: A harmful node throws away each packet it accepts when it performs a black hole attack, so it blocks nearby vehicles from talking to each other.

GPS Spoofing: Attackers can make vehicles believe they are elsewhere by sending false GPS signals. That may cause wrong directions in addition to unsafe situations.

Wormhole Attack: An attacker can make a quick, low-delay link between two far network sites with a wormhole attack. This method lets the attacker grab moreover change vehicle-to-vehicle messages.

Replay Attack: Replay attacks include an adversary intercepting legitimate messages and retransmitting them at a later period, which may result in network confusion or undesired behavior.

V. PROPOSED METHOD

In this approach, a method of locating the false identities is employed by examining the regular similarities in neighborhood data. In this work, a novel approach that relies on identifying rogue nodes from the network that initiate Sybil attacks has been developed.

Elliptical Curve Cryptosystem (ECC) : Elliptic curves over finite fields have an algebraic structure, which serves as the foundation for the Elliptic Curve Cryptosystem (ECC), a public-key encryption technique. Here it used to generate the Key for the Vehicle nodes . Individual Key is generated to all registered vehicle nodes in VANET.

The algorithm for Key Generation is given below:

Input: A Extracted Map setup with Vehicle nodes and Trusted Authority

Output: A Public and Private Key Generated

Algorithm:

1. **Choose an Elliptic Curve:**

   Select a specific elliptic curve over a finite field. The curve equation typically takes the form: $y^2 = x^3 + ax + b$, where a and b are coefficients that define the curve.

2. **Select a Base Point (Generator Point):** Choose a point G on the elliptic curve, often referred to as the generator point. G should have a large prime order (the number of times it can be added to itself before reaching the identity point). The order of G is denoted as n.

3. **Compute the Order of the Curve:**

   Calculate the total number of points (including the point at infinity) on the elliptic curve. This is denoted as N.

4. **Choose a Private Key:**

   Select a random integer d (private key) such that 1 <= d < n, where n is the order of the generator point G.

5. **Compute the Public Key:**

   Compute the corresponding public key point Q, which is the result of multiplying the generator point G by the private key d using elliptic curve scalar multiplication:

$$\mathbf{Q = d * G}$$

6. **Encode the Public Key:**

   Represent the public key point Q as an elliptic curve point (x, y), or in some cases, as a compressed form that only includes x along with a bit indicating the y-coordinate's parity.

7. **Save the Key Pair:**

   Store the private key (d) securely, and make the public key (Q) available for others to use. Key Length in size of 256 bits.

Digital Signature Algorithm (DSA): This Algorithm is used to generate the Certificate with Digital Signature to the Legitimate Vehicles to avoid the Malicious nodes in VANET.

The algorithm for Generation and Verification of Certificate is given below:

Input: A Legitimate Vehicle

Output: A Signature is Generated with pair of (r,s).

Algorithm:

Signature Generation:

Select two large prime numbers, p and q.

Compute g, a generator of a subgroup of integers modulo p.

Choose a private key x, a random integer, such that 1 < x < q-1.

Calculate the corresponding public key y, where y = (g^x) mod p.

Hashing:

Apply a cryptographic hash function to the message/document, producing a message digest.

Signing:

Generate a signature (r, s)

Choose a random integer k such that 1 < k < q-1.

Compute r as r = (g^kmod p) mod q.

Calculate s as s = (k^{-1}* (H(message) + x * r)) mod q, where H(message) is the hash of the message.

Signature Verification:

Key Acquisition:

Obtain the sender's public key (p, q, g, y).

Hashing:

Compute the hash of the received message/document.

Verification:

Verify the signature (r, s):

Check that 0 < r < q and 0 < s < q.

Calculate w as w = s^{-1} mod q.

Calculate u1 as u1 = (H(message) * w) mod q.

Calculate u2 as u2 = (r * w) mod q.

Compute v as v = ((g^{u1} * y^{u2}) mod p) mod q.

If v matches r, the signature is valid; otherwise, it's invalid.

VI. SYBIL ATTACK DETECTION MODEL

This model finds Sybil attacks in VANETs by checking if a vehicle gets false messages from a harmful node. If a Sybil node attacks a vehicle, it confirms the vehicle's identity with the RSU before sending the data packet.

The Sybil Attack Detection algorithm follows:

Input: False messages from the harmful node.

Output: A node is free from Sybil Attack

Algorithm:

Identify the location of vehicle from near by RSUs.

The malicious node will be verified by near by RSU by Distance based Verification.

```
Function distance_verification(vehicle_id, gps_location,signature):
if      verify_signature(vehicle_id, signature):
if calculate_distance_with_rsu(gps_locat ion) < threshold_distance:
return True return False
```

Verify the Neighboring nodes with particular RSUs.

```
function  neighbor_verification(vehicle_id, neighbor_list, signature):
if  verify_signature(vehicle_id, signature):
stored_neighbors = get_stored_neighbors(vehicle_id)
if compare_neighbor_lists(neighbor_list, stored_neighbors):

    update_stored_neighbors(vehicle_id, neighbor_list)
      return True return False
```

Timestamp and Signature Verification is done by the particular RSU.

```
function timestamp_and_signature_verification(messag e, signature):
if   verify_signature(message, signature) and is_valid_timestamp(message):
 return True
return False
```

By repeating these steps Malicious node is detected from the particular Range of the RSU .

VII. DEEP LEARNING MODELS

A. FUZZY LOGIC

Fuzzy logic is used for feature representation of VANET dataset for detecting Sybil attack where it is used for grouping the Attacks by using fuzzy inference system where it uses fuzzification for assigning Linguistic Variables and membership function, inference rule is used for aggregation.

B. VGG 16

VGG 16 used for Feature Extraction from feature represented by fuzzy logic . The hierarchical feature extraction capabilities of VGG16 can still be helpful in extracting pertinent characteristics from your input data, even though VANET data may differ from conventional photos. With this method, you can optimize the deep representations that VGG16 has learned to better fit your particular detection goal.

C. CONVOLUTIONAL NEURAL NETWORK (CNN)

CNN is used for detection of Sybil attack in VANET, it uses the data from the feature extracted from Transfer learning VGG 16 so CNN work as hybrid model with VGG16 to detect Sybil attacks in VANET.

D. PARTICLE SWARM OPTIMIZATION

Particle Swarm Optimization (PSO) , the Classification accuracy is fed into this module to improve the model and improve the robustness and performance of the model of high accuracy of malicious node detection.

VIII. IMPLEMENTATION

SYSTEM	DETAILS
Number of Vehicles	300
Number of Malicious Node	135
Number of Identities used by Malicious Node	128
Simulation Duration	250 Seconds
Vehicle Speed	30m/Second
Simulator	OMNET++
Area of Simulation	2500m*2500m

TABLE I : SIMULATION CONFIGURATION SETUP

IX. EXPERIMENTAL RESULTS

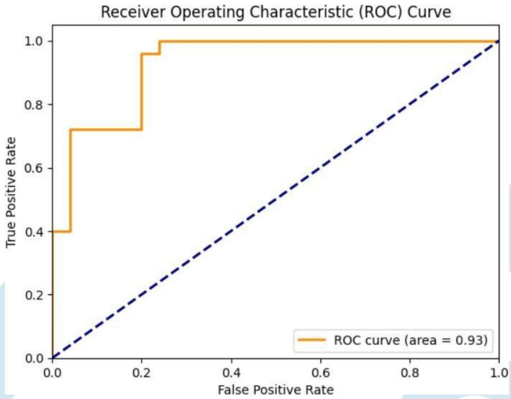

FIGURE I: ROC CURVE OF CNN

As showed in FIGURE I is ROC CURVE of CNN which gives 93% while detecting Sybil attack in VANET. After implementing Particle Swarm Optimization(PSO) with CNN then the ROC Curve increases to 99% it gives the higher accuracy in detecting the Sybil attack in VANET as it is shown in the FIGURE II.

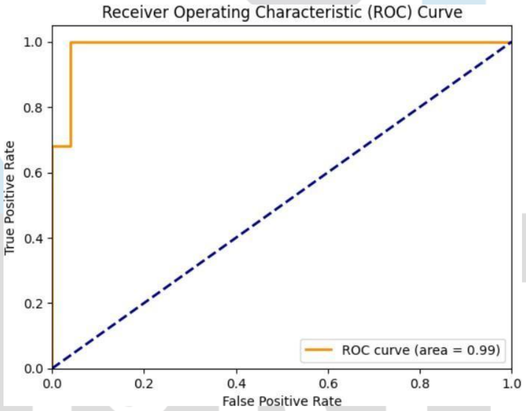

FIGURE II: ROC CURVE OF CNN with PSO

SYBIL NODE COUNT	CORRECTLY DETECTED	UNDETECTED	SYBIL ATTACK DETECTION RATIO (IN PERCENTAGE)
10	8	2	80
15	13	2	86.67
20	17	3	85
25	21	4	84

TABLE I: SYBIL ATTACK DETECTION RATIO IN SIMULATION SETUP

In Table I represents Sybil Attack Detection ratio which is carried out in Simulation setup, it shows the sybil attack detection ratio of increasing the sybil nodes from 10,15,20,25.

X. CONCLUSION

As a result, Maintaining the dependability and integrity of vehicle-to-vehicle communication requires the security of vehicular ad hoc networks, or VANETs in the application of Deep Learning Techniques into VANET dataset ,where it uses fuzzy logic for feature selection ,pretrained model VCG 16 is used for feature extraction and CNN is combined with VCG 16 as Hybrid model which is used as classification of Sybil attack which gives the accuracy of 94%.To improve the performance of the model ,it uses Particle Swarm Optimization which classify the Sybil attack with an accuracy of 97%. The ongoing development and integration of advanced security protocols will contribute to the overall safety and reliability of connected vehicles in Vehicular Ad Hoc Networks (VANET) .

XI. FUTURE WORK

On focusing on future directions, the Sybil attack detection from VANET include exploring enhanced feature representation techniques, such as advanced fuzzy logic methods and more sophisticated CNN architectures for feature extraction from VGG16.Integrating anomaly detection techniques, developing online learning mechanisms for model adaptation, and conducting extensive real-world evaluations will enhance the system's robustness and applicability.

REFERENCES

[1] Hongyuan Cheng and Yining Liu, “An Improved RSU-based Authentication Scheme for VANET” International Journal Of Internet Technology,2020, Vol. 21, No. 4,pp.1137-1150.

[2] Fan Li,Xiaoyu Song ,Huijie Chan,Xin Li,“Hierarchical Routing for Vehicular Ad Hoc Networks via Reinforcement Learning” IEEE Transactions on Vehicular Technology,2019, Vol. 68, No. 2, pp.1852-1865.

[3] Ravi Prakash, Kamal Soni, “Improved Session Key Based Certificate to Detect Sybil Attack in VANET” International Journal of Engineering Research and Technology,2014,Vol.3, pp. 117- 119.

[4] Shwetha M and Archana R A, “EMAP: Expedite Message Authentication Protocol For Vehicular Ad Hoc Networks” International Journal of Engineering of Research and Technology, 2014,ISSN:2278-0181, pp.517-522.

[5] Yasser Toor and Paul Muhlethaler,Inria Anis Laouiti, “Vehicle Ad Hoc Networks: Applications And Related Technical Issues”, IEEE communications Surveys,2008,Vol.10,No.3, pp.74-88.

[6] Rasha Al-Mutiri, Mznah Al-Rodhaan and Yuan Tian, “Improving Vehicular Authentication in VANET using Cryptography”, International Journal of Communication Networks and Information Security(April 2018),Vol.10,No.1,pp.248-255.

[7] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, Woong Cho, “A Security and Privacy Reviews of VANET ”, International IEEE Transactions on Intelligent Transportation Systems,2015, Vol.16, No.6 , pp.2986-2993.

[8] Anjia Yang, Jian Weng, Nan Cheng, “DeQOS Attack: Degrading Quality of Service in VANETs and its Mitigation”, International IEEE Transactions on Vehicular Technology,2019,Vol.68,No.5, pp.4838-4843.

[9] Khaled Rabieh, Mohamed M.E.A Mahmoud, Terry N.Guo and Mohamed Younis, “Cross-Layer Scheme for Detecting Large Scale Colluding Sybil Attacks in VANETs”, IEEE ICC 2015 – Communication and Information Systems Security Symposium, pp.1-6.

[10] Wenjia Li, Houbing Song, “An Attack- Resistant Trust Management Scheme for Securing Vehicular Ad-Hoc Networks ”, International IEEE Transactions on Intelligent Transportation Systems,2016, Vol.17, No.4 , pp.961-967.

[11] Pandi Vijayakumar, Maria Azees, Sergei A.Kozlov, “An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs International IEEE Transactions on Intelligent Transportation Systems,2022, Vol.23, No.2 , pp.1632-163.

[12] Pandi Vijayakumar, Maria Azees, Arputharaj Kannan and Lazarus Jegatha Deborah, “Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks”, International IEEE Transactions on Intelligent Transportation Systems,2016, Vol.17, No.4 , pp.1017-1026.

[13] Mohamed Baza , Mahmoud Nabil, Mohamed M.E.A. Mahmoud, Niclas Bewermeier, Kemel Fidan, Waleed Alasmary and Mohamed Abdallah, “Detecting Sybil Attacks using Proofs of Work and Location in VANETs” IEEE Transactions on Dependable and Secure Computing,2022,Vol. 19, No. 1, pp.39-51.

[14] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang and Xingshe Zhou, “Multi-Channel Based Sybil Attck Detection in Vehicular Ad Goc Networks using RSSI” International IEEE Transactions on Mobile Computing,2019,Vol.18, No.2, pp.362-374.

[15] Sohan Gyawali , Yi Qian, Rose Qingyang Hu, “Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks” International IEEE Transactions on Vehicular Technology,2020, Vol.69, No.8, pp.8871-8883.

[16] Francesco Schiliro, Nour Moustafa, Imran Razzak and Amin Beheshti, “DeepCog: A Trustworthy Deep Learning-Based Human Cognitive Privacy Framework in Industrail Policing” IEEE Transactions on Intelligent Transportation Systems,2023, Vol. 24, No. 7, pp.7485-7491.

[17] Ankita Sharma, Shalli Rani, Syed Hassan Shah, Rohit Sharma and Mohammad Mehedi Hassan, “An Efficient Hybrid Deep Learning Model for Denial of Service Detection in Cyber Physical Systems ” IEEE Transactions on Network Science and Engineering , 2023,Vol.10, No.5, pp.2419-2427.

[18] Xiao Wang , Yushan Zhu, Linyao Yang, “Fast and Progressive Misbehavior detection in Internet of Vehicles Based on Broad Learning and Incremental Learning Systems ” IEEE Internet of Thing Journal,2022,Vol.9, No.6, pp. 4788-4796.

[19] Izhar Ahmed Khan , Nour Moustafa, Dechang pi, Bentain Li, “An Enhanced Multi-Stage Deep Learning Framework for Detecting Malicious Activities From Autonomous Vehicles” IEEE Transactions on Intelligent Transportation Systems,2022, Vol.23, No.12, pp.25469-25477.

[20] Yingying Chen, Jie Yang, Wade Trappe, Richard P. Martin, “Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks”, IEEE Transactions on Vehicular Technology ,2010,Vol.59,No.5,pp.2418-2433.