International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Design a Process to Detect and Mitigate the Malicious Attacks in VANET Using Ml Approach

[1]Prakash V. Sontakke, [2]Nilkanth B. Chopade

Submitted: 11/01/2024 **Revised**: 17/02/2024 **Accepted**: 25/02/2024

Abstract: The research intends to detect suspicious behavior in VANETs and block the vehicles involved from using the network for its intended purpose of safe information exchange. To enhance traffic safety and efficiency, VANETs use wireless ad hoc communication between vehicles and roadside devices to share cooperative awareness data and event-based messaging. By considering the existence and condition of cars traveling within a set range, drivers can receive quick notifications about potentially hazardous scenarios, such as a vehicle suddenly braking in front of the back of traffic congestion up ahead or the hacking of shared information inside a network. Within a communication range of a few hundred meters, nodes in a VANET will often broadcast mobility-related data (i.e. absolute values for position, time, heading, and speed) to develop a communal knowledge of single-hop neighbors. The ability for network nodes to communicate ad hoc allows traffic safety software to run with little lag.

For the purpose of protecting VANETs from outside attackers, the suggested HCMNDA (Hybrid cooperative malicious node detection Approach) methods employ automated prediction. Only VANET-registered nodes have addresses that have been validated by a trusted certificate authority. Internal attackers with the right hardware, software, and valid certificates can be detected by analyzing stored data in a table using a clustering approach. I illustrate how the Attacker's single-hop or multi-hop communication range may be negatively affected by the processing of incorrect information on the traffic's overall security and performance. The majority of existing VANET misbehavior detection systems focus on data-centric plausibility and consistency criteria.

Most existing solutions are only tested via simulations. To the contrary, I employed a network-wide automated prediction of malicious activity to test how well VANET misbehavior detection stands up in the actual world. Long-term research in operational tests based on simulation, and dedicated trials employing test vehicles, yielded fresh insights that are presented here. Based on these findings, the cutting-edge HCMNDA (Hybrid cooperative malicious node detection Approach) method was developed. There are two main benefits to this approach: the ability to quickly pinpoint potential attackers within the cluster and the ability to spot irregular behavior in the immediate vicinity. Using this strategy, which can detect abnormal node behavior should be effective even against yet-to-be-developed attack methods.

Keywords: *VANET, HCMNDA (Hybrid cooperative malicious node detection Approach), attackers, security*.

1. Introduction

Given the rising number of vehicles on the road and the rapid progress being made in the field of autonomous vehicles, road safety is becoming increasingly important. The communication system of VANET can be utilised to disseminate data pertaining to highway security, traffic management, navigation, and maintenance. Since VANETs can be penetrated in a number of ways, from passive eavesdropping to direct interference [1], they are often viewed as a target for such attacks. A hacker may, for instance, look up and replay other vehicles' messages in order to gain access to tools like toll services. A malicious actor may tamper with a specific vehicle, imitate it, and issue a false warning, all of which would cause traffic problems [1].

[1]*Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune- 411044, India.*
prakashsontakke2122@gmail.com
[2]*Pimpri Chinchwad College of Engineering, Savitribai Phule Pune University, Pune- 411044, India.*

The term "machine learning" (ML) refers to the process of teaching a computer new information and the ability to make sound judgments. Almost every sector relies on ML, from production to robotics to the arts to biotechnology to intelligent autonomous transportation to automated systems. It has risen in popularity due to its low cost, availability of massive volumes of data, and high-powered computing machinery. It allows for fast, well-thought-out decision making, which improves the system's energy efficiency, QoS, and dependability [1]. Since the population and car industry have grown so rapidly, traffic and health have become pressing issues in many cities. Every year, automobile accidents kill about 1.25 million people around the world [2], making them the leading cause of mortality for people aged 15 to 29. Expensive delays, increased body temperature, increased pollution, and increased fuel consumption are all results of traffic congestion. In 2017, traffic jams in the United States cost $305 billion [3]. Increased productivity can be realized in the form of fewer traffic accidents, a cleaner environment, and more efficient traffic flow

through the implementation of an intelligent and efficient transportation network. Reduced journey times for passengers are one benefit of the Vehicular Ad Hoc Network's (VANET) efforts to enhance traffic flow and road safety, especially during peak periods. As the number of people using wireless devices continues to rise, the need for more spectrum to support excessive capacity allocation has become urgent. This has hampered the widespread adoption of cutting-edge switching technologies like those used in "smart cities," 3D video streaming services, AR/VR, the IoT, and VR, among others (VR).

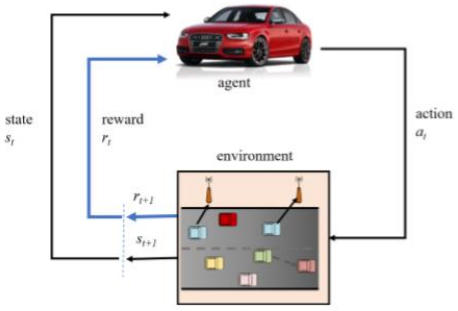

Fig 1: VANET architecture using intermediator

Intrusion detection, either on its own or in tandem with the prediction feature, can help uncover fraudulent and otherwise unusual activity in large, complex networks.

The goal is to investigate and analyze numerous VANET attacks and security vulnerabilities.

For careful data processing and spotting even the tiniest irregularities, it is necessary to design intrusion detection systems that provide end-to-end monitoring.

The goal of this ML-based system is twofold: 1) to enhance the effectiveness of intrusion detection systems, and 2) to prevent potentially damaging alerts due to false positives or negative variables.

This section discusses the remaining components. In Part II, we examine the previous research on intrusion detection and its limitations. The VANET system's technique is outlined in Section III. Part IV explains the VANET system's developed method for detecting and preventing intrusions. The findings are presented in Section V. In the final section, you will find the summary.

2. Related Works

This talk will review previous attempts at securing VANETs. The most important answers will be summed up for you. Numerous research efforts have explored different VANET-friendly intrusion detection system topologies [3]. Because of the interconnected nature of VANETs, MANETs, and Sensor Networks, it is important to reevaluate security practices in these areas. The second section will begin with an explanation of VANET.

After covering the extensive literature on VANETs, many studies have looked into MANET-specific intrusion detection systems [3].

Carlos H. O. O. Quevedo et al. [1] state that the vulnerabilities and limitations of VANETS are the most pressing problems in the field. VANETs are vulnerable to both traditional network attacks and newer, more sophisticated ones, such as Sybil's, which try to compromise authentication and disseminate false information. For this reason, our study created a SyDVEL M-based method for detecting Sybil attacks in VANETs. Services like road safety, reducing traffic congestion, digital entertainment, and others can all benefit from the system's foundation in advanced machine learning algorithms. SyDVELM proposes a methodology for understanding the dynamics of vehicular node movement in dense urban environments. Sybil node relocation error evaluation in light of actual vehicle dependability. They showed how SyDVELM may be used in VANETS to guarantee a high detection rate with low error rates and a versatile detection approach. SyDVELM's strengths over the present Sybil Attack Detection system are demonstrated by these features. The suggested method will be tried out in sparse environments, and the ELM solution will be integrated with other machine-learning techniques for possible implementation.

In [2], Stefan Mihai et al. detail the technological advancements that have led to a cooperative, wired, mobile transportation system. By analyzing the most serious threats posed by VANETs, the authors provide a comprehensive evaluation of the methods now in use for protecting users' privacy, the integrity of their communications, and their confidentiality. However, widespread adoption is required to tackle the outstanding issues related to safe automotive accessibility and road networks. The author also explains why unified policies and procedures are essential for ensuring flexibility and dependability without compromising on privacy or security. For this information to arrive unharmed, network security must also be improved.

By Fabio Gonc lves, et al. [3] A comprehensive SLR on the application of VANET Smart IDs is provided in this work. The most often used configuration of the network traffic simulator Ns-2 and the SUMO protocol has been used in the research. In terms of the most popular ML algorithm, it looks that NN (and its many variations) is the most popular option. The necessary datasets are often created from the simulation or the network simulator's trace file for each investigation. The SLR was made in part to help people find reliable, freely available data

collections. It appears that this was impossible. According to the evaluation of the studies, most of them do not specify the processes by which their databases and assaults are created.

One of the most rapidly evolving computational methods, machine learning (ML) is being utilized to solve pressing issues in a wide variety of disciplines, as explained by Mohammad Asif Hossain et al. [4]. We anticipate that VANETs, or ad hoc vehicle networks, will play a significant role in reducing traffic jams and car accidents. A massive amount of data must be transmitted in order to secure this area. Because of this, the current bandwidth allocated to VANET is incapable of handling these kinds of data loads. Therefore, VANET experiences a spectrum shortage. Cognitive radio (or CR) is an approach that has the potential to resolve problems of this nature. The performance of a VANET built on CR, sometimes known as a CR-VANET, could be significantly enhanced in a number of ways. CR-VANET can be made even smarter by incorporating ML techniques, which can help speed up the network's ability to adjust to new environments and boost its service's performance without wasting too much power. Their overview covers the fundamentals of CR, VANET, CR-VANET, and ML, such as their design, key functions, common challenges, and potential solutions. The scenarios of CR-VANET were used to assess the ML technique specifications and roles. In addition, it provides details on the application of ML in autonomous vehicles. They also explain the applications and cutting-edge research in ML approaches throughout CRVANETs' many fields of study, including routing, spectrum sensing, security, and resource management. Many facets of ML application to AVs have been identified, and its capabilities have been expanded to alleviate traffic congestion and road accidents. Since these disciplines are still developing, they are utilizing ML methods to reap the benefits of being studied at an early stage. In his thesis, he addressed some of these broader themes, along with open questions and potential future directions for the area.

Authors WANG TONG et al. [5], Better communication is just one of the many topics covered in this article on software-defined networking (SDN)-based virtual area network (VANET) architecture, components, and operations. We can lessen overall network strain by controlling it with a single remote. As an added bonus, SDN controllers can monitor potential vulnerabilities. In this piece, the authors highlight how modern vehicle technology helps a great deal with monitoring and controlling formerly difficult transportation networks.

Many SDN adoptions are still impeded by many security difficulties, as noted by the method's creator, A. Hussein et al. [7]. This paper examined current SDN security flaws, threats, and mitigation strategies. Inherent in the SDN's functionalities are a plethora of novel network issues. To meet the requirements of these networks, it is necessary to strengthen and optimize them. Since the strategies were developed in response to certain violent situations, they fare well in their wake but fall short when confronted with attacks that were not expected.

The security community is slow to adopt SDN technology despite increasing investments and research in the field. Finding studies that evaluate SDN-based network security technologies' usability, practicality, reliability, and efficacy is challenging. The ultimate goal of SDN security is to implement a multi fence safety policy that permeates every aspect of the network, providing comprehensive protection against both known and undiscovered threats.

R. This study by Boutaba et al. [8] provided a comprehensive analysis of the constraints, challenges, and risks posed by the SDN's design in a number of real-world use cases. The authors also used granular semantic analysis of the defensive network to create and protect SDN-based networks. In addition, you should seek to improve network security generally, and the SDN stack in particular, by implementing cutting-edge upgrades and a fortified network operating system. The technological hurdles it posed for SDN controllers and other communication devices in the SDN domain were substantial. A security framework with a legislative focus was also created. This application's function is to monitor and safeguard the SDN environment. It should be noted that ONOS SDN manager was responsible for developing this program and assessing potential security issues. Finally, they are indicative of the attack vectors against which our method is most effective. As part of the exhibition, we are also displaying our results from the examination.

DoS attacks are described in detail by S. Pouyanfar et al. [09], and the authors note that in order to provide a diagnosis, models for detecting such attacks must be built rapidly. One strategy suggested in this paper involves adjusting the packet propagation ratio. It will detect assaults like DoS as soon as they are successful. Also, they note that in the coming work, black list would be encrypted before being transferred to the RSU for distribution to network users, which should make it more difficult for attackers to steal packets from the network. To round out our discussion of learning's stochastic game, we will go through the DOS problem once again.

[10] Y. Gordienko et al. The literature of the Next Decade based on SDNs is available to the writers in a comprehensive format. We provide an introduction to SDN architecture and code for implementing SDN. The

characteristics of SDN are the focus. The many ways that SDN can be used to construct next-generation networks are being examined. Key issues can be addressed by integrating SDN with other technologies, such as those used in the smart home, smart buildings, smart mobility, optical networks, and handheld wireless sensor networks. Several issues need to be resolved before SDN can be applied to other, more advanced networks.

As stated by L. Liang et al. [11], It is crucial to building trustworthy protocols that adhere to the stringent requirements of this application sector if car networks are ever going to be commercially viable and appealing to consumers. To offer successful car identification while protecting driver privacy, the construction of secure protocols is difficult by the seemingly opposing requirements of consumers, automakers, and the government. There are a number of ways to address these issues, and we were able to develop some new primitives by drawing inspiration from features of vehicle networks. In laying out the issues and potential solutions inside vehicle networks, the authors of this paper aim to inspire other academics to dive into this promising but underexplored field. Different intrusion detection systems that are suitable for MANET have been the subject of a number of research efforts [3]. MANET architecture may be roughly divided into three classes, and each of them has its own set of advantages and disadvantages.

Multilevel clustering was utilized to build a complicated hierarchical IDS by H. Ye, L. Liang, and co-authors in [12]. The third design deploys a virtual agent with mobility to traverse the extensive network. One or more mobile agents are dispersed over the MANET and assigned to each node in order to carry out a certain activity. In prior research, such as that of Kachirski and Guha [13], multiple mobile agents were used to create decentralized intrusion detection systems; this approach allows for the workload to be distributed across a larger number of people because different agents are responsible for different aspects of the investigation. Research on ML and data processing can be found in published works. Using these methods, IDS can acquire expertise in security systems, learn how threats and their operations work, draw connections between seemingly unrelated occurrences and even predict assaults. Unattended learning in IDSs, such as the clustering process, and an unattended examination of trends, was the focus of the research.

To identify VANET intrusions, B. Khalfi et al. [13] created a game-theoretical model. This model predicts that the controlled nodes will likely be subject to a denial-of-service assault in the future. Numerous papers have been written about using differential privacy in machine learning. Here's an example: Kasiviswanathan et al. [29] successfully implemented a generic approach to approximate learning in a probabilistic setting. Since studying differential privacy theory, a growing body of work has investigated how privacy and performance relate to one another in ML. In addition, many specialists are concerned with the integrity of the transmitted differentials. Verification of the distributed difference protection was invented by Eigner and Maffei for use in developing crypto figure ic protocols and is now fully automated. They developed a differentially private approach for using simulated gradient descent to solve a distributed constrained optimization, protecting the confidentiality of the constraints collected [12].

Many different areas, including traffic modeling, filtering, and network categorization, have discussed possible applications of ML. At [26], it offered responses to a Deep Learning Survey. The fundamental idea behind reinforcement learning (a type of ML) was first introduced by Gosavi. In CR, researchers analyzed the various ML methods systematically. There are a number of CR systems that make use of AI. CRNs argued about a wide variety of ML uses. A wide range of topics relating to the application of AI in CRNs has been covered. Several machine learning (ML) approaches are discussed in context with their application to DSA. The newest developments and applications of ML in VANETs have been discussed. In [21], the numerous uses of VANET AI were reviewed, and a detailed analysis of the various ML techniques utilized in VANETs was provided. Quick feedback was gathered on CR via survey. Here, they addressed some of the CR's fundamentals as well as its other metrics, taxonomies, issues, and problems. Please consult for detailed CR data. The CR cycle was outlined, which comprises four stages: spectrum sensing, perception, reasoning, and adaptability (see Section II.C). It investigated how to sense the spectrum in different ways [13]. A discussion was held to address the issues surrounding spectrum variety and the knowledge that comes with it. Spectrum management has been reformed.

Open-loop solutions prevent interference from occurring in the former scenario. In contrast, closed-loop techniques reduce congestion once it has been recognized [28]. Congestion can be detected with the use of measuring techniques that take note of the number of messages in the queue, the amount of time the channel is in use, and the percentage of its capacity that is really in use. As was said in the introduction, VANET's congestion management solutions fall into two broad categories: hybrid strategies and strategies based on prices, resources, CSMA / CA, priority setting, and scheduling [17]. We'll talk about those strategies below.

Below, we will go over a number of distinct varieties of VN attacks [7][10].

A. False information; the test of the introspective, logical, and proactive square attacker. They will send inaccurate data within the network because it alters the activities of different drivers.

Attacker B. UN Company Undertakes Intentional manipulation of sensing-element data The assault When it comes to running a business, AN is an officer who is both fair and active. As a means of avoiding responsibility in the event of a failure, he employs this assault to alter the predicted location, distance, and course of many nodes.

An intruder with a C. identity theft speech act is a passive and dishonest corporate leader. It has the potential to follow a vehicle's path and utilize that information to determine what kind of car it is.

DOS Attacker is a local, hostile, physical threat. An attacker's attempt to knock down the network by means of unpleasant messages on the roadmap is possible. Dummy messages and the introduction of obvious automatic countermeasures are two examples of this type of attack.

Packet Relaying and Dropping It is possible for an attacker to cause good packets to be dropped. An invader might delete all alerts meant to notify responding vehicles, for instance. Also, an attacker may fake an accident by recovering the packets at the time of the mishap.

The F. Vehicle in the Shadows This type of assault is possible in any setting where vehicles can potentially seek to alleviate wireless channel congestion. A car, for instance, may send a warning to its neighbor and wait for a reply. The car will avoid alerting additional nodes if it receives a response, as it will know that its neighbor is in a better position to convey the warning message.

G. It is difficult to identify and prevent a wormhole attack. In this attack, a malicious node intercepts data packets at a single point in the network and sends them on to other nodes in the network over a dedicated network. If the rogue node just sent management messages via the channel, rather than data packets, the attack would be more successful [12].

Sybil Virus Assault, H. A vehicle commits this attack by assuming the identities of other cars. These names and numbers can be used to launch an attack inside the framework. In addition, the creation of these fictitious identities gives rise to the impression that there is a greater quantity of automobiles on the road than there actually are. If multiple attack variants use spoofing to impersonate various nodes in a network, the result is chaos [13].

Table 1: Approaches in ML algorithm use in VANET

Application Category	Task	Utilized ML algorithms	Core ML method utilized	Open challenges specific to V2X
Mobility management	Mobility prediction Handover optimization	Probabilistic models, NNs Q-learning, Fuzzy Q-learning,	Supervised Learning Supervised Learning RL	It is necessary to anticipate the future position of an object quickly and accurately in order to facilitate other predictive tasks, such as handover. Because of their movement, they need a smooth handoff, but they can't take too much time doing it.
Routing	Routing decision, user association	Q-learning, multi-armed bandits, Kernel-based learning NNs, K-nearest neighbours, and multi-armed bandits are all types of NNs.	RL	Differentiated quality of service routing in a vehicle heterogeneous network.
Resource Management	Channel, power, and joint radio	Q-learning, Convolutional NN	Supervised Learning RL	Spectrum efficiency through spectrum sharing; Resource allocation based on

	resource management Computation and storage	(CNN), Deep Q-learning Deep Q-learning		diversified QoS needs; System architecture design; Interference and power optimization;
Energy	resource management Base station switch-off	Q-learning,	RL	Centralized optimization of scheduling algorithms for the regional
efficiency	Infrastructure and/or Electric Vehicle (EV) energy efficiency through scheduling	Heuristic Q-learning, Deep Q-learning		command, or on a per-gateway-device basis; A large-scale solution that integrates EV hardware with readily deployable ML techniques

2.1 Research Gap

Extreme decentralization, in which hosts rather than a single server carries out the network's design and operations, is a hallmark of common VANETs. There are a lot of new services and protocols that VANETs can support now. This characteristic pinpoint many problems caused by a new kind of network's enhanced service provisioning, together with the network's sluggish reaction times and restricted mobility when confronted with hostile external forces [20].

Connectivity issues and the subsequent absence of VN authorization features make it more difficult to build a security line and classify nodes as trustworthy or untrusted.

Information security vulnerabilities in VANETs can be attributed to the following sources:

1. The lack of host defense equipment against intruders.

2. The potential for message substitution and wiretapping owing to shared access to the communication environment

3. The VANET architecture's peculiarities make it impossible to use a conventional security mechanism.

4. The necessity of using intricate routing algorithms that account for the likelihood of getting false information from compromised hosts due to altering the network's topology.

2.2 PROBLEM STATEMENT

In particular, VNs require extremely low latency and extreme flexibility to accommodate a wide variety of situations and applications. After that, the network must be redesigned to allow for more hardware accessibility and easier operation by piercing the rigid framework. Each node in a network can be isolated, hacked, and made to talk to the bad guys [21]. Another security issue for virtual networks is that it is possible to eavesdrop on communications sent between nodes and to inject and replay spoofed messages. When a network is attacked by hostile nodes, regular network operations are disrupted on purpose. These issues would have a major bearing on the spread of VN. This makes the job of defending VNs more challenging [22].

Wireless network performance issues between nodes lead to issues with source-destination connectivity and data connectivity. Therefore, VNs must be extremely flexible so that they can respond to any situation.

But there are still a lot of problems to be solved. a few of them are as follows:

- Performance and adaptability
- Scalability
- Interoperability

Since VN consists of a variety of hardware and some networks have resource-constrained nodes, the network's security must be guaranteed while minimizing overhead as much as possible.

3. Methodology

This section of the research details the suggested model architecture, which is constructed from several VANET building elements. Most VANET architectures consist of an application unit (AU), a mobile radio system unit (RSU), and an onboard unit (OBU). Contact between

OBUs (car to car) or an OBU and an RSU (vehicle to infrastructure) is based on vibration or wireless communication in the vehicle environment [3]. In addition to communicating with other RSUs and traffic control centers, RSUs can talk to other infrastructures via wireless networks (infrastructure to infrastructure). It's equipped with an OBU and a few AUs. Additionally, the OBU employs its array of sensors to exchange data with other RSUs and OBUs and to collect data on their surroundings. Readers interested in learning more about the fundamental building blocks of VANET architecture will find that information here [22]. As can be seen in the graphic below, each vehicle is equipped with a local PML-CIDS agent that keeps tabs on things like OBU and AU communications.

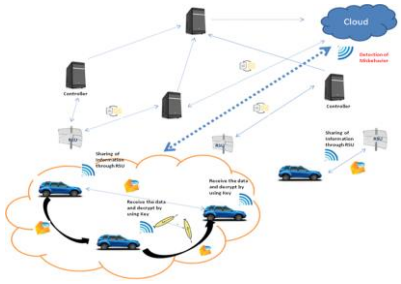

Fig 2: Vehicular network using Roadside unit

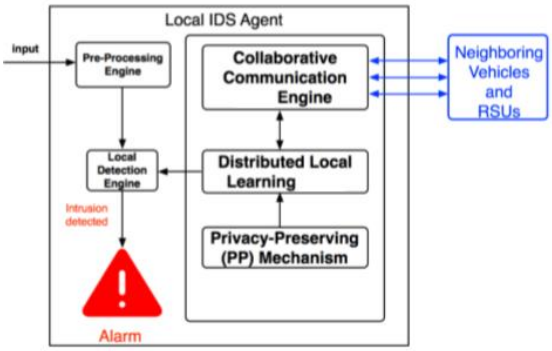

Fig 3: Architecture of Proposed IDS System using ML

The three main parts of the collaborative framework are a system-level local detection engine, a shared ML engine, and a pre-processing engine that protects users' anonymity. Information from the VANET framework is collected and pre-processed by the pre-processing engine, which then uses this information to regulate the vehicle system's activities in real-time and protect it from illegal access [23].

4. Proposed Approach

An innovative approach employing CBD and K-means is suggested here, HCMNDA, with the goals of improving the accuracy of activity identification results in autonomous vehicles and bolstering the convergence behavior. "Optimizing the number of hidden neurons and count of epoch" is how the HCMNDA approach improves recognition accuracy. A new machine learning algorithm called HCMNDA is developed, which combines the best features of CBD and K-means. Among CBD's many advantages, which led to its selection for this application, are its high searchability, robustness, and optimization accuracy, as well as its excellent optimization outcomes, feature selection, and maximization of classification efficiency [20]. Instead of reducing the number of attributes, it encounters complexity due to slow convergence and problems in obtaining globally optimal solutions. In order to get the fastest possible convergence, the K-means algorithm is employed [21]. This is because it has many advantages, such as consuming fewer resources and providing convergence more rapidly. A new approach has been introduced to achieve the highest possible throughput while maintaining very accurate results.

When applying an HCMNDA approach, the CBD algorithm's probability calculation and random number are considered. The position updating of the suggested approach is governed by the following condition: if "the solutions are updated" based on the global leader phase of the K-means algorithm, then "the solutions are updated" by considering the CBD algorithm; otherwise, it is not updated [22]. The global leader phase process assists in discovering the most appropriate positions using Eq. (1).

$$X_{isk}^{new} = X_{isk} + B[0,1](GL_{is} - X_{isk}) + B[-1,1](X_{uis} - X_{isk}) \quad (1)$$

In Eq. (1), "the random number is noted as B, the new position updating based on the global leader is termed as X_{isk}^{new}, the global leader position at k^{th} dimension is shown as GL_{is} and the u^{th} spider monkey at k^{th} dimension is termed as X_{uis}, the is^{th} at k^{th} dimension is derived as X_{isk}, where an arbitrarily chosen index" is specified as $is \in \{1,2,\cdots,Is\}$.

Movement: The source is computed through the priority of fitness values, in which the highest value of roosters will be accessed first. This is mathematically formulated in Eq. (2) and Eq. (3).

$$X_{i,k}^{is+1} = X_{i,k}^{is} * (1 + rn(0,\sigma^2)) \quad (2)$$

$$\sigma^2 = \begin{cases} 1, if\ Fn_i \le Fn_k, \\ \exp\left(\dfrac{(Fn_k - Fn_i)}{|Fn_i| + \varepsilon}\right), otherwise, \end{cases} k \in [1, Ns], k \ne i \quad (3)$$

Here, the smallest constant in the computer is termed as ε that is employed for avoiding the zero-division-error and the fitness value is denoted as regarding cs. A "rooster's index is termed as k that is chosen randomly

from the roosters group, and a Gaussian distribution is noted as $rn(0,\sigma^2)$ with mean 0 and standard deviation" σ^2

Node movement: The node search n neighbor based on their group-mate rooster, and avoids the other error. Additionally, the other node can steal the other node position. This behavior is formulated in Eq. (4).

$$X_{i,k}^{is+1} = X_{i,k}^{is} + RN1 * rd * \left(X_{z1,k}^{is+1} - X_{i,k}^{is}\right) + RN2 * rd * \left(X_{z2,k}^{is+1} - X_{i,k}^{is}\right) \quad (4)$$

$$RN1 = \exp\left(\frac{(Fn_i - Fn_{z1})}{(abs(Fn_i) + \varepsilon)}\right) \quad (5)$$

$$RN2 = \exp((Fn_{z2} - Fn_i)) \quad (6)$$

Here, a uniform random number is mentioned as rd that lies in the range of [0, 1] [23]. An "index of the rooster and an index of the node" are termed as $z1 \in [1,2,..,Ns]$ at the i^{th} hen's group-mate and $z2 \in [1,2,..,Ns]$, respectively, where $z1 \neq z2$. In the same way, $Fn_i > Fn_{z1}$, and $Fn_i > Fn_{z2}$, and so, $RN2 < 1 < RN1$.

Head node movement: The movement of "nodes around their cluster to search for neighbor node" is formulated in Eq. (7).

$$X_{i,k}^{is+1} = X_{i,k}^{is} + FU * \left(X_{Y,k}^{is} - X_{i,k}^{is}\right) \quad (7)$$

The pseudo-code of the proposed approach algorithm is given in Algorithm 1.

Algorithm 1: Proposed
Initialize the number of nodes as Ns and their parameters
Compute position of entire individuals
While $is <$ max. Generations
  if $\rho_{is} \geq B$
    Update the solutions based on algorithm
    Update the positions using
    $X_{isk}^{new} = X_{isk} + B[0,1](GL_{is} - X_{isk}) + B[-1,1](X_{uis} - X$
  Else
    Update the solutions based on CBD algorithm
    if $is == cluster\ node$
      Update Solution Using
      $X_{i,k}^{is+1} = X_{i,k}^{is} + FU * \left(X_{Y,k}^{is} - X_{i,k}^{is}\right)$
    end if
    if $is == normal\ node$
      Update solution using
      $X_{i,k}^{is+1} = X_{i,k}^{is} + RM * rd * \left(X_{z1,k}^{is+1} - X_{i,k}^{is}\right) + RN2 * rd * \left(X_{z2,k}^{is+1}$
    end if
    if $is == malicous\ node$
      Update solution using
      $X_{i,k}^{is+1} = X_{i,k}^{is} * (1 + rn(0,\sigma^2))$
    end if
  End if
    Estimate new solutions
    Update best solutions
  end for
end while

This section is organized as per objective and corresponding architecture.

4.1 Hybrid Cooperative Malicious Node Detection Approach (HCMNDA)

To develop an ML-based system to increase Intrusion detection system Performance & prevent harmful warnings for false positive / negative factors.

$$(TLI)^X = ATL^X / q^X{}_{max} \quad (8)$$

Where

$q^X{}_{max}$ is the length of interference of node X,

ATL^X is the average traffic load at the node X which is computed as follows

$$ATL^X = 1/Q \sum q\ i \quad (9)$$

Where,

we estimate the packet forwarding probability of node X related to the queue congestion parameter as following:

$$P^{load} = 1 - (TLI)^X \quad (10)$$

We used P^{load} as the packet forwarding probability with respect to the congestion load of node X. Higher the probability, the lesser the packets loss at node X.

$$(LCR)^X = (\sigma^X + \gamma^X) / (\max(\sigma^X) + \max(\gamma^X)) \quad (11)$$

Where σ^X is the link arrival rate and γ^X is the link breakage rate of node X.

By using Eq. (4), the probability of successful packet transmission with respect to the mobility is computed as follows:

$$P^{mobility} = 1 - (LCR)^X \quad (12)$$

We can further compute the final probability for successful packet forwarding as following

$$P^{final} = (P^{load} + P^{mobility}) / 2 \quad (13)$$

Algorithm:02

Inputs
M: a set of n number of malicious detected nodes in stage I
S: source node
δ=0.5: threshold value to check the successful packet delivery probability
Output:
M': verified malicious node list
1. FOR i:n
2. S Compute (M(i)) using Eq. (10)
3. S Compute (M(i)) using Eq. (12)
4. S Compute using Eq. (13)
5. IF (P^{final} (M'(i)) > δ)
6. M'(i) ='true'
7. ELSE
8. M'(i) ='false'
9. END IF
10. END FOR

5. Result & Discussion

This study seeks to achieve CBDS by using clustering, which provides high data transfers between nodes and reasonably priced real resources to the CU without compromising network security, since it is extremely difficult to maintain an effective routing and connectivity mechanism on the network and layer. Each node in the VANET is located at a distance of between 100 and 1,000 meters from the others. The CUs may always forsake their network or join forces with other groups due to their nomadic nature [20]. With its speed range of 0-30 m/s, the CU's gearbox range was set at 30 meters. Unfortunately, routers only had a 30-meter transmission range, and 802.11 was utilized as the layer's MAC standard. While transferring data and establishing connections, we used a probability distribution to add hostile nodes, also known as CUs, into the network in order to test its security [21].

5.1 Network Performance Assessment

A great deal of variation exists in both the experimental inputs and the results. As input features, we make use of both the total number of nodes and the arrival time. Number of shift changes, turn time, and attendance time are the success metrics. Overall performance, packet transmission rate, reduced return time, minimum waiting time, minimal power consumption, and minimal waiting time are all scheduling requirements that the proposed algorithm would meet while simultaneously having the lowest end-to-end delay in all possible arrival time scenarios [22]. This will be followed by an algorithmic evaluation of the suggested approach. While we do employ unique performance metrics for each experiment, we do share a few common performance characteristics, such as,

5.2 Simulation

We look at how Clustering can be used to improve energy-efficient resource assignment in an intelligent radio organization, and how this looks different from the prior techniques' steering conventions based on the Packet Distribution Ratio. Processing When there are many nodes in a network, the delay and throughput are used to evaluate how efficiently resources can be dispersed via the fastest path through the network. Detailed depiction of the process is provided in the image below [23].

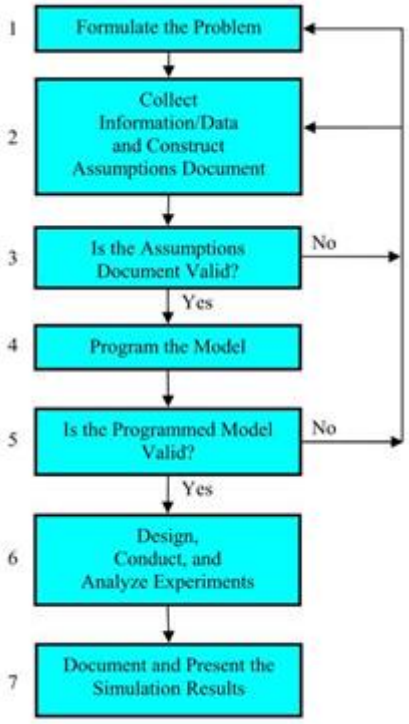

Fig 4: Steps in Simulation

5.3 Improve Hybrid Cooperative Malicious Node Detection Approach (HCMNDA)

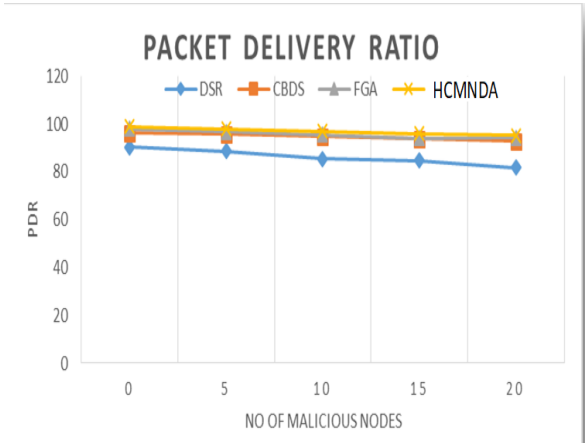

Fig 5: Packet delivery ratio vs number of malicious nodes

When shown in Figure 5, the proposed HCMNDA performs better than existing systems in terms of PDR as the number of hostile nodes increases. Sybil Attack causes a greater percentage of data loss in DSR, CBDS, and FGA than it does when using the HCMNDA routing protocol across the board [20].

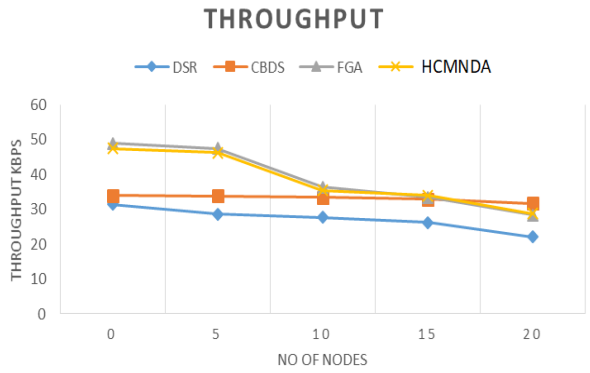

Fig 6: Throughput Vs Number of Malicious nodes

Compared to DSR, CBDS, and FGA, the proposed HCMNDA generated an average throughput of 38.37 percent higher. Under Sybil attack, the DSR is the lowest, and its throughput frequently fluctuated [21].

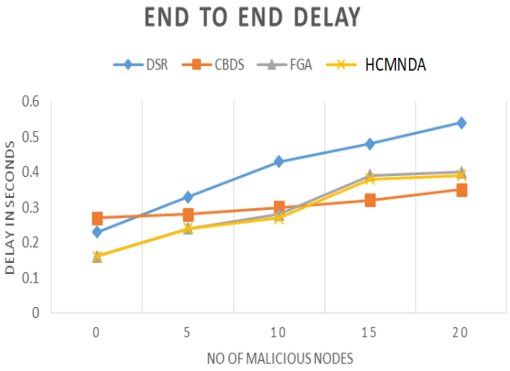

Fig 7: End To End Delay Vs Number of Malicious nodes

Figure 7 displays the results for standard DSR, CBDS, FGA, and the planned HCMNDA in terms of end-to-end delay [22].

This model has been shown to avoid Sybil attacks and floods with far less delay than competing models [23].

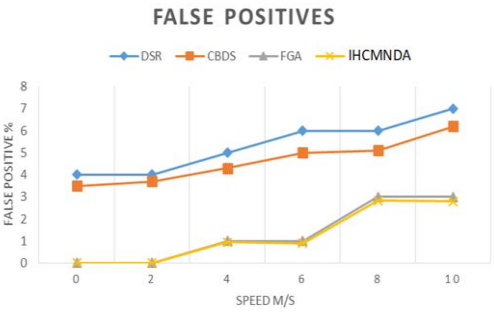

Fig 8: False Positive Vs Node Speed

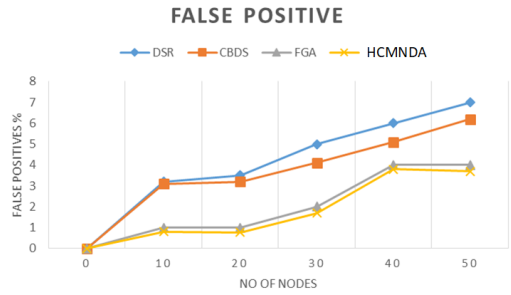

Fig 9: False Positive Vs Number of Nodes

Figures 8 and 9 demonstrate how our proposed methodology better analyses the whole possible reason of a packet drop event before reaching a conclusion about the node's reliability. According to the data, the percentage of false positives rises as network nodes get faster.

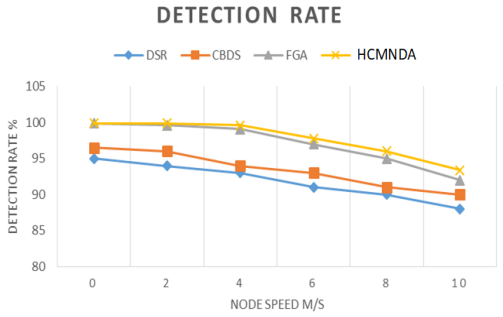

Fig 10: Detection Rate Vs Node Speed

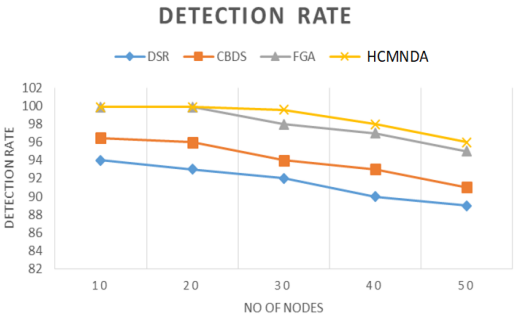

Fig 11: Detection Rate Vs Number of Nodes

As can be shown in Figures 10 and 11, the identification rate is higher with our suggested HCMNDA approach since each judgement takes into account more information about harmful behaviors and network nodes [20].

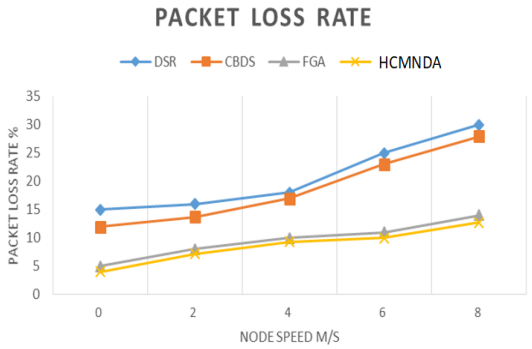

Fig 12: Packet loss rate Vs Node Speed

Our proposed system HCMNDA shows minimum packet loss as shown in Figure 12.

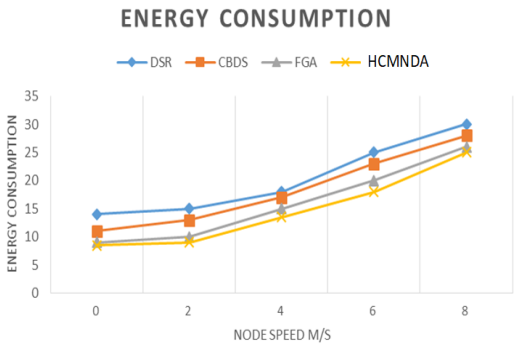

Fig 13: Energy Consumption Vs Node Speed

Energy consumption under the proposed HCMNDA and FGA schemes is depicted in Figure 13 as the node speed increases. To highlight the extra processing and communication expenses associated with the HCMNDA scheme [11], this experiment compares it to other schemes, such as the FGA [20]. Higher energy consumption is a common consequence of these alternative approaches. The majority of a node's power is consumed during the sending and receiving of packets. Rather than increasing the total number of messages transmitted, our proposed HCMNDA method makes use of previously established routing packets [22].

6. Conclusion

As can be seen from the above, the CBDS scheme can identify malicious nodes while still delivering over 90% of packets. This is despite the fact that 40% of the network's total nodes may be bad. As the number of malicious nodes grows, it is clear that DSR generates less routing overhead than the CBDS. This is because DSR does not have any built-in safeguards or security features. Because the CBDS transmits bait packets during its first bait phase and then changes to a reactive defence phase subsequently, it may create a little more routing overhead than the DSR. When multiple malicious nodes answer with an RREP at the same time, the CBDS is able to single them out. This means that the CBDS's end-to-end delay remains constant even if the number of malicious nodes in the network grows in tandem.

According to the findings, the false positive rate is significantly decreased using the suggested HCMNDA system compared to the non-FGA scheme. Before deciding whether or not to trust a node, the HCMNDA scheme considers all of the possible reasons for a packet drop. Generally speaking, the rate of false positives grows as the pace of the nodes does. Because of the increased chance of overhearing at the source node or out-of-date routing information, legitimate nodes are being labelled as malicious as the network's overall speed increases. Since HCMNDA thoroughly investigates each packet-drop event before drawing any conclusions about the behaviour of nodes, it produces significantly fewer false positives than the non-FGA technique. Every packet loss is treated as an attack by non-FGA schemes.

The proposed work enhances standard network node performance by taking into account a single accusation message from CH and allowing nodes with WL to carry out standard network operations.

Reference:

[1] Carlos H. O. O. Quevedo, Ana M. B. C. Quevedo, Ahmed Serhrouchni , “An Intelligent Mechanism for Sybil Attacks Detection in VANETs”, 978-1-7281-5089-5/20/$31.00 ©2020 IEEE.

[2] Stefan Mihai, Nedzhmi Dokuz, Meer Saqib Ali, Purav Shah, and Ramona Trestian,” Security Aspects of Communications in VANETs”, 978-1-7281-5611-8/20/$31.00 c 2020 IEEE.

[3] Fabio Gonc¸alves, Bruno Ribeiro, Oscar Gama,“A Systematic Review on Intelligent Intrusion Detection Systems for VANETs”, 978-1-7281-5764-1/19/$31.00 ©2019 IEEE.

[4] WANG TONG, AZHAR HUSSAIN , WANG XI BO , AND SABITA MAHARJAN ,“Artificial Intelligence for Vehicle-to-Everything: a Survey”, 2169-3536 (c) 2019 IEEE.

[5] C. Chembe, D. Kunda, I. Ahmedy, R. Md Noor, A. Q. Md Sabri, and M. A. Ngadi, “Infrastructure based spectrum sensing scheme in VANET using reinforcement learning,” Veh. Commun., vol. 18, p. 100161, 2019.

[6] Dimitrios Kosmanos, Apostolos Pappas , Francisco J. Aparicio-Navarro ,”Intrusion Detection System for Platooning Connected Autonomous Vehicles”, 978-1-7281-4757-4/19/$31.00 c 2019 IEEE.

[7] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, “Artificial Intelligence for Vehicle-to-Everything: A Survey,” IEEE Access, vol. 7, pp. 10823–10843, 2019.

[8] R. Boutaba et al., “A comprehensive survey on machine learning for networking: evolution, applications and research opportunities,” J. Internet Serv. Appl., vol. 9, no. 1, p. 16, 2018.

[9] S. Pouyanfar et al., “A Survey on Deep Learning: Algorithms, Techniques, and Applications,” ACM Comput. Surv., vol. 51, no. 5, pp. 92:1--92:36, Sep. 2018.

[10] Y. Gordienko et al., "Deep learning with lung segmentation and bone shadow exclusion techniques for chest x-ray analysis of lung cancer," in International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018, pp. 638-647: Springer.

[11] AB Kathole, KN Vhatkar, S Kumbhare, J Katti, VV Kimbahune, “IoT-Based Smart Agriculture for Onion Plant Disease Management: A Comprehensive Approach”, International Journal of Intelligent Systems and Applications in Engineering,2024.

[12] S Kumbhare, SA Ubale, G Dharmale, N Mhala, N Gandhewar, “IoT-Enabled Agricultural Waste Management for Sustainable Energy Generation”, International Journal of Intelligent Systems and Applications in Engineering,2024.

[13] SD Patil, AB Kathole, S Kumbhare, K Vhatkar, “A Blockchain-Based Approach to Ensuring the Security of Electronic Data”, International Journal of Intelligent Systems and Applications in Engineering,2024.

[14] Ara and A. Ara, "Case study: Integrating IoT, streaming analytics and machine learning to improve intelligent diabetes management system," in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 3179-3182.

[15] S. Shahrestani, "Assistive IoT: Deployment Scenarios and Challenges," in Internet of Things and Smart Environments: Springer, 2017, pp. 75-95.

[16] S. Pandit and G. Singh, “Spectrum Sensing in Cognitive Radio Networks: Potential Challenges and Future Perspective BT - Spectrum Sharing in Cognitive Radio Networks: Medium Access Control Protocol Based Approach,” S. Pandit and G. Singh, Eds. Cham: Springer International Publishing, 2017, pp. 35–75.

[17] N. Muchandi and R. Khanai, “Cognitive Radio Spectrum Sensing: A Survey,” Int. Conf. Electr. Electron. Optim. Tech. - 2016 Cogn., pp. 3233–3237, 2016.

[18] J. Qadir, “Artificial intelligence based cognitive routing for cognitive radio networks,” Artif. Intell. Rev., vol. 45, no. 1, pp. 25–96, 2016.

[19] S. M. Baby and M. James, “A Comparative Study on Various Spectrum Sharing Techniques,” Procedia Technol., vol. 25, no. Raerest, pp. 613–620, 2016.

[20] Atul Kathole , Dinesh Chaudhari “Secure Hybrid Approach for Sharing Data Securely in VANET”, Proceeding of International Conference on Computational Science and Applications pp 217–221, © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[21] Atul Kathole , Dinesh Chaudhari “Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach”, Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021) pp 447–457 © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[22] Atul Kathole , Dinesh Chaudhari “Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach”, Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021) pp 447–457 © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[23] Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons of Machine learning and Security Methods, "2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588, Volume 21 Issue 4.

[24] “Practical Guide to Principal Component Analysis (PCA) in R & Python”, accessed on 5/11/2016, https://www.analyticsvidhya.com/blog/2016/03/practical-guide-principal-component-analysis-python/

[25] Physical Human Activity Recognition Using Wearable Sensors Ferhat Attal , Samer Mohammed , Mariam Dedabrishvili , Facial Chamroukhi , Latifa Oukhellou and Yacine Amirat Received: 11 September 2015; Accepted: 8 December 2015; Published: 11 December 2015 Academic Editor: Vittorio M.N. Passaro.