CHAPTER 1
INTRODUCTION

1.1 Intelligent Transportation System and Vehicular Ad-Hoc Network

Intelligent Transport System (ITS) refers to the integration of technologies for connecting and exchanging data into the transportation infrastructure. This integration makes the transportation more efficient, secure and sustainable. Vehicular Ad-Hoc Network (VANET) is the crucial part of ITS and being an indispensable part of the smart city landscape. ITS for safer road transportation enables the communication between vehicles, infrastructure, and other road users. VANET, when integrated into Intelligent Transportation Systems (ITS), offer numerous advantages. These include real-time traffic monitoring, accident detection, and optimized route planning, among others.

VANET communication is categorized as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). V2V communication allows vehicles to directly exchange information with each other, while V2I communication facilitates communication between vehicles and infrastructure components, including traffic signals, road signs, and roadside units (RSUs). Moving vehicles continually collect and share real-time information about traffic, road conditions, and potential dangers (Taoufik Yeferny et al., 2020). The general architecture of VANET with the components and communications is shown in Figure 1.1.

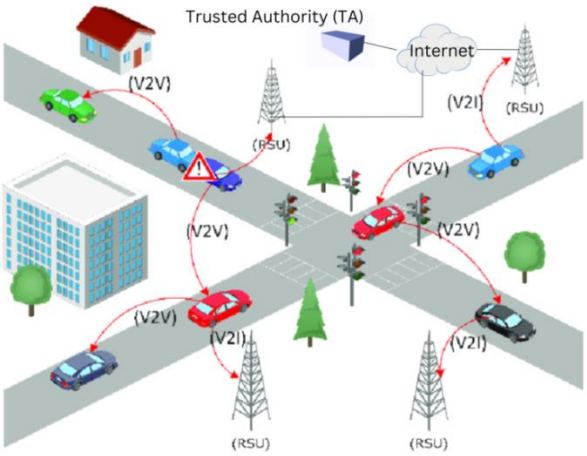

Figure 1.1 General Architecture of VANET

The intervehicle sharing, vehicle transfer to RSU happens through the On-Board Unit (OBU). A Trusted Authority (TA) in VANET plays the role of controlling and supervising the entire VANET. The communications in VANET are short-range, and the vehicles share information through intermediate vehicles. The road conditions and the incidents are instantly sent as alert signals to the other vehicles or nodes in the network to avoid such roads. RSUs installed on the road receive the shares from the vehicles through V2I communications. The ability of RSUs to communicate with the Traffic Authority (TA) and On-Board Units (OBUs) is facilitated by their fixed positions on the roads (Jabar Mahmood et al., 2021).

The European standard for vehicle-to-everything (V2X) communication is based on the CAR-2-X communication system developed by the CAR-2-CAR Communication Consortium. The domains in this architecture include the following:

- In-vehicle domain

In this setting, vehicles incorporate Application Units (AUs) and an OBU, which are interconnected using either a wired or wireless link.

- Ad-hoc domain

The ad-hoc communications happen among the vehicles in this domain with OBU-equipped vehicles, and stationary RSUs in specified locations along the road. The ad-hoc network coverage extends when RSUs connect to the infrastructure domain or to the internet.

- Infrastructure domain

In this domain, the access is based on hot spots and RSUs. There is no internet access while OBUs can exploit cellular radio networks (Taoufik Yeferny et al., 2020). The communications in VANET are based on direct or multi-hop using wireless short-range communication (Muhammet Ali Karabulut et al., 2023).

There are three layers: the physical, network, and application layers in the architecture of VANET-based ITS. The physical layer is responsible for providing a wireless communication channel between vehicles and infrastructure components.

Ensuring reliable and secure communication between network nodes is a core responsibility of the network layer. Finally, the application layer provides various services such as traffic monitoring, collision avoidance, and many others.

VANET have evolved since 2001 and were labeled as ITS in 2008. Gradually from 2012, the numbers of vehicles of different brands were included in projects and were tested. By 2025, around 300 million vehicles are expected to be globally networked making an entry in the mainstream market. In the next decade, VANET will offer real-time communications with 5G (Muhammet Ali Karabulut et al., 2023).

VANET Characteristics

The high mobility and the varying topology ordain the diff erent nature of VANET with complexity and dynamism. In addition, VANET has various characteristics due to its nature, and are listed below:

- Variable network density
- Transmission medium
- Frequent disconnections
- Limited bandwidth
- Heterogeneity
- Extensive computational processing

The structure and characteristics of VANET require ensuring confidential communications between V2V and V2I. Roads of today's world have VANET with high increase of vehicles inclusive of the above-mentioned characteristics. This makes it challenging to meet the stringent network requirements such as low latency, high mobility, security, and massive connectivity.

Challenges in VANET

The architecture and the characteristics of VANET lead to various challenges having the impact on the design, communication and the overall performance. The challenges impacting VANET are:

- Node velocity and density
- Movement patterns

- Network volatility
- Delay – sensitive message transmission
- Fading signals
- Lack of Communication
- Bandwidth Limitations
- Multi-hop connection
- Security
- Privacy
- Routing
- Data dissemination
- Heterogeneity
- Real time system

In the recent years, the challenges in VANET still addressable in the research are:

- Quality of Service (QoS)
- Dynamic topology
- Connectivity
- Privacy
- Security

Security in VANET is paramount to ensure the safety of both drivers and passengers. Emergency messages are crucial and have to be prioritized over the communications in VANET with high reliability and security. Adversaries may compromise the integrity of information, causing the TMC and RSUs to make erroneous decisions (Kaur et al., 2021).

1.2 Security in VANET

Vehicular networks have the nature and characteristics that enforces security measures for the safe travel of the users. The security demanded by VANET is based on the integrity of data, confidentiality and availability. Every vehicle user has a right to privacy. Vehicle and driver information must be shared securely only with

authorized users. The message transmission must be guaranteed until the destination vehicle receives the message. The communication in the network is based on the short connection duration in the wireless channels. Network size and mobility of vehicles vary leading to ad-hoc nature and unbounded network. Trust among the vehicles enables the information exchange in a frequent manner. VANET operate in an untrusted environment and most of the network's nodes are nameless, it is not easy to build trust between them.

The increasing integration of sensors and wireless communication technologies into vehicles unlocks significant potential for transformative applications. These advancements promise to enhance road safety, improve traffic management, and enhance driver comfort and entertainment during journeys (Sadaf, M. et al., 2023).

Security becomes the major concern for the VANET due to its distinctive nature, network, mobility, communication and information exchange. Secured message delivery without delay enhances traffic flow, relieves traffic congestion, and improves road safety.

Thus, to fully leverage the potential of Intelligent Transport Systems, robust security measures within VANET communication research and development are crucial (Mishra, R. et al., 2016). The unique characteristics of VANET present distinct security challenges, including issues related to trust group formation, position detection, and protection.

1.3 Security Challenges in VANET

The security of VANET requisites arises due to its characteristics. The communication, information exchange in a frequently changing topology, ad hoc nature with vehicles short connection durations determined as characteristics are impacting the security of VANET. Due to the characteristics, VANET becomes vulnerable to various attacks thus breaching the security. However, their reliance on open-air communication and dynamic topology exposes them to unique security challenges that can have dire consequences.

The major security challenges in VANET are shown in Figure 1.2.

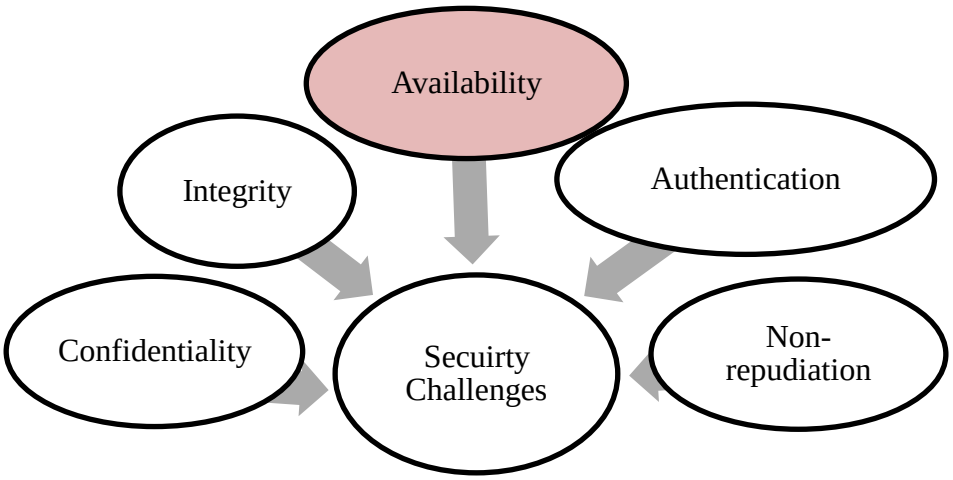

Figure 1.2 Security Challenges in VANET

VANET encounter a range of security challenges, encompassing availability, authentication, data integrity, confidentiality, non-repudiation, pseudonymity, privacy, mobility, data and location verification, access control, and key management. One of the main challenges in VANET-based ITS focus in ensuring the security and privacy of communication. In order to guarantee both driver and passenger safety, security is a critical concern in VANET. One important component of VANET security is availability. This guarantees that, in spite of vulnerabilities and launch of denial -of-service attacks, all resources remain permanently available. To defend against these attacks, VANET can leverage cryptography and trust-based algorithms and protocols.

Authentication is the process allowing the appropriate users to join the network. Additionally, it guarantees that the person sending the communication is not an unauthorized party. The usage of pseudonyms protects the user's privacy.

Integrity, often known as data integrity, guarantees that the sender's original data packets have not been altered. On the other hand, it needs to be shielded from the enemy in route. In VANET, data accuracy remains as the major security concern. It is possible to use public key infrastructure, digital signatures, and cryptographic revocation mechanisms to guarantee the integrity of communication between the sender and the recipient.

Data hiding from attackers is the definition of confidentiality. Researchers utilize cryptography techniques for authorized user's data access in terms of confidentiality. This maintains data as private and prevents unauthorized users from viewing private information. This feature establishes the original message's source from denying their authorship. Alternatively, this function links the content to the original sender of a certain message.

Pseudonymity is the act of concealing one's true identity. Pseudonyms are used by the legal players in place of their true identities. The lawful entities can converse anonymously in this way without disclosing who they are. This guarantees user's privacy protection.

A scalable network can easily adapt to varying levels of usage and traffic. Vehicular network's dynamic topology remains as a demanding difficulty to attain adaptability. Due to the rapid and frequent changes in node locations within VANET, mobility is a pervasive aspect of these networks. A key concern arising from this mobility aspect is the requirement for more dynamic and secure algorithms to guarantee high-quality service delivery. It is employed to get rid of harmful communications from the network. This guarantees data accuracy testing and confirms participating nodes' validity.

Access control is implemented to monitor and enforce the policies governing the rights and roles of all nodes participating in the network. The term "key management" describes the handling of keys in cryptography techniques during node-to-node communication. The network's security procedures are designed with key management and issuance in mind.

Due to their open nature, VANET are susceptible to security threats such as Denial of Service (DoS) attacks and the interception of data. Thus, various security mechanisms such as cryptography, authentication, and intrusion detection systems (IDS) have been proposed to ensure the security of VANET-based ITS (Rehman S.U. et al., 2013, Emmanuel Bamidele Ajulo et al., 2018, Kaur R et al., 2021, Jabar Mahmood et al., 2021)

1.4 Attacks in VANET

Vehicular Ad Hoc Networks face several security challenges due to their unique characteristics and requirements. Attackers can exploit the challenges faced by VANET to launch various types of attacks on the network. Vehicles and roadside equipment come together to establish wireless communication networks known as vehicular ad hoc networks. These networks are essential for increasing the effectiveness and safety of transportation. However, to operate safely and securely, VANET must overcome many security issues. The absence of a centralized control mechanism in VANET is one of the biggest security challenges. As a result of direct communication between vehicles, security regulations cannot be enforced by a centralized body. Hence these networks are less secure and based on the layers, attacks can be launched compromising the security requirements.

1.5 Classification of Attacks and Security Requirements

It is imperative to recognize the attacks targeting the VANET based on fulfilling the security requirements. The major concern in the network is providing safety to human lives with secured and timely information exchange. The communications among the vehicles and the infrastructure are open in nature thus invading the networks by the attackers are high. Figure 1.3 above exhibits the attack classification based on the security requirements.

Based on the security requirements, availability (Muhammad Sameer Sheikh et al., 2019) is the critical factor in VANET security. This ensures continuous and uninterrupted access to all resources within a network, even when faced with security threats like vulnerabilities and denial-of-service attacks. The network is always reliable and provides access to necessary information whenever it is operational. This crucial security aspect in VANET, primarily focused on safeguarding user lives, is a prime target for attackers. Several attacks are in this category, the most prominent are the Denial of Service attacks (DoS).

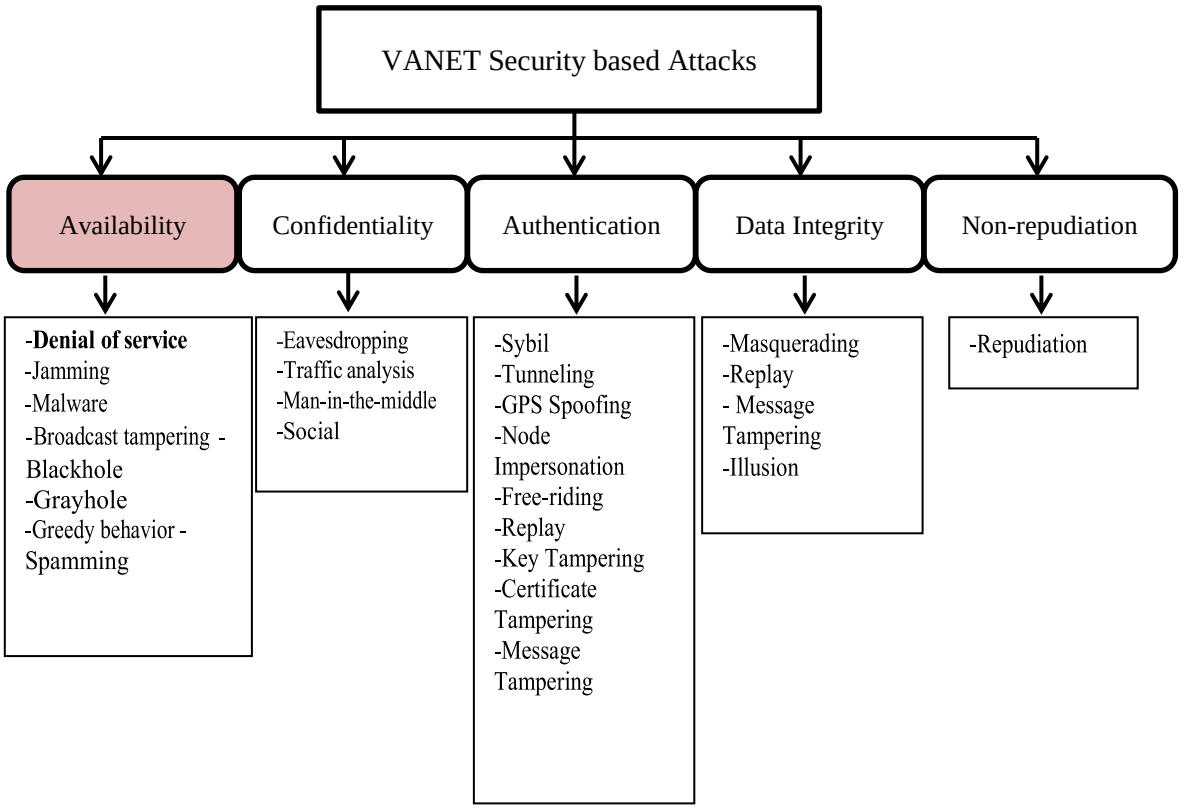

Figure 1.3 Attacks Classification on Security Requirements

1.6 Classification of Attacks on Layers

In Vehicular Ad-Hoc Network, the categorization of security threats is structured based on the Open Systems Interconnection (OSI) model layers. This model, consisting of seven layers, delineates distinct functionalities in network communication. Security threats in VANET are classified according to the specific layer they target. For instance, physical layer attacks involve jamming or eavesdropping, while network layer threats manifest as routing attacks or Sybil attacks. This layered approach provides a granular understanding of vulnerabilities, allowing for the implementation of targeted security measures to protect the integrity, confidentiality, and availability of data exchanged within the VANET infrastructure (Vamshi Krishna, K et al., 2023). The classification of attacks based on layers is as follows:

- Application Layer Attacks
- Transport Layer Attacks

- Network Layer Attacks
- Data Link Layer Attacks
- Physical Layer Attacks

The attacks targeting specific layers of the VANET architecture are shown in the Figure 1.4.

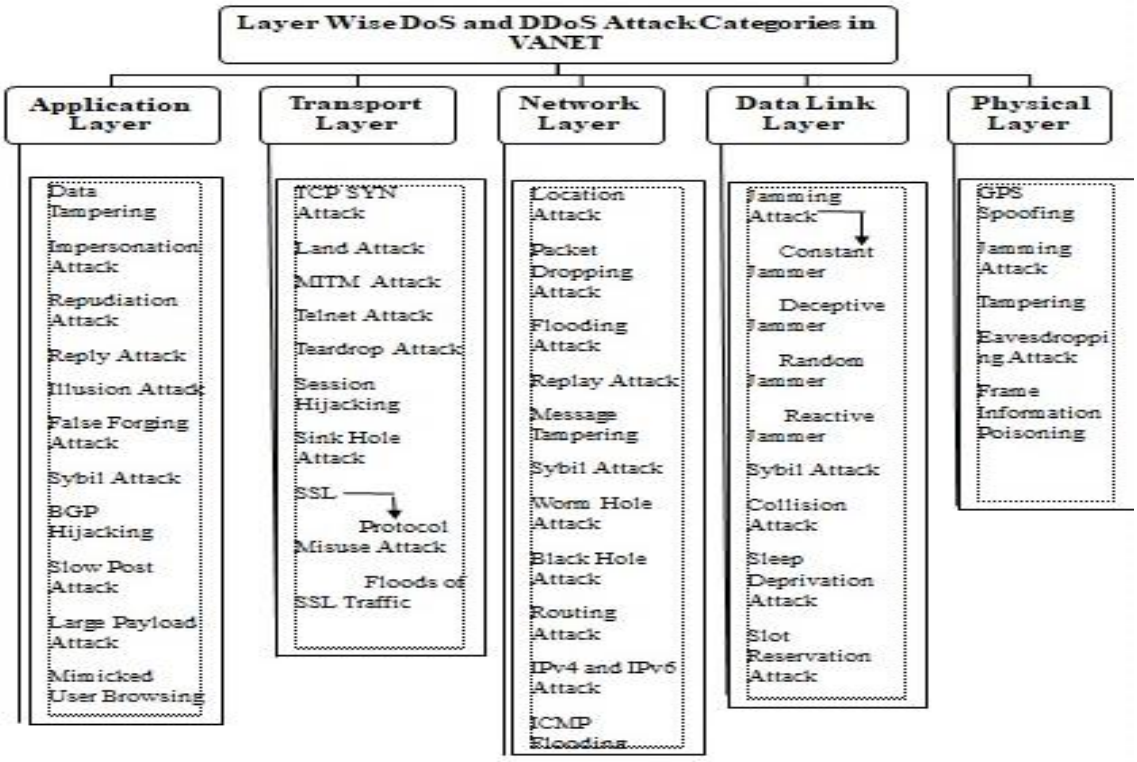

Figure 1.4 Layer-wise DoS and DDoS Attack Classification in VANET

VANET rely on secure communication for applications like safety messages, traffic information exchange, and cooperative driving. However, they are susceptible to various communication attacks that can disrupt functionality and compromise user privacy. From the mentioned layer wise attacks in VANET, network, transport and application layers have the susceptibility to communication attacks that can disrupt functionality of the VANET. This includes disrupting routing and information flow, reliable data transfer between applications on different vehicles, target specific applications. DoS and DDoS attacks are prevalent in network, transport and application layers.

Based on the attack classification provided, several studies investigated into the security challenges faced by VANET, specifically targeted by DDoS attacks. A DoS assault on a network or service may be conducted for several reasons. DoS attacks are a common motive for financial gain. Attackers may utilize denial-of-service and distributed denial-of-service attacks to criticize a business or government organization for engaging in what they consider to be unacceptable political, geopolitical, economic, or monetary behaviors. The escalating attacks on VANET demand effective security solutions to protect the safety of both passengers and other road users.

Reflection and exploitation DoS and DDoS attacks leverage vulnerabilities in network, transport layers of VANET to amplify an attacker's traffic and overwhelm the target vehicle that in turn exploit vulnerabilities in specific application protocols to trigger such attacks on application servers. The classification of DoS and DDoS attacks based on the layers in VANET is shown in the Figure 1.4.1

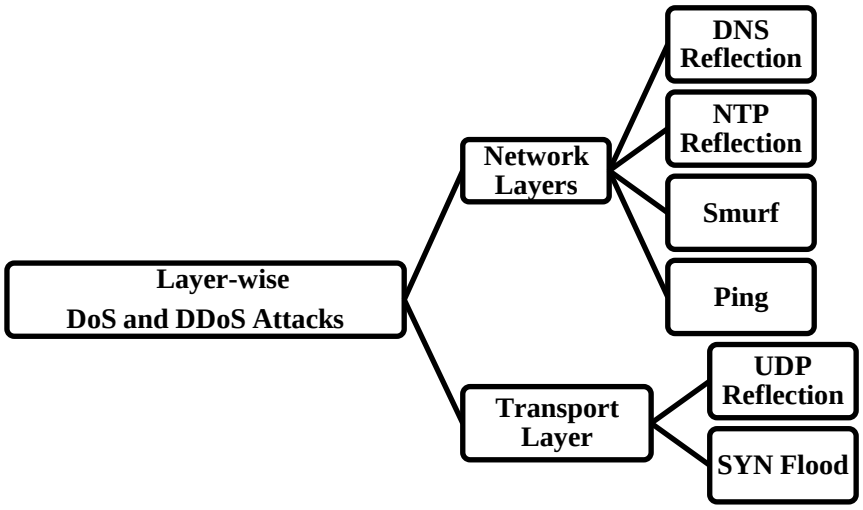

Figure 1.4.1 Layer-wise DoS and DDoS Attacks based on Communication

In addition, the other attack vectors relating to DoS and DDoS attacks disrupting communication in VANET are found in the application layer of the OSI model. The attacks included are:

- HTTP floods
- Domain Name System (DNS) query flood attacks

The network layer of the OSI model is targeted by DDoS attacks working on the network and transport layers. The attacks aim to flood the network and types of attack are majorly based on TCP and UDP. The attacks are:

- UPD flood
- SYN flood
- Network Time Protocol (NTP) amplification
- DNS amplification

The DDoS attacks appearing through network and transport layers are categorized as shown in Figure 1.5. The attacks escalate to application layer targeting specific applications running on VANET (I Sharafaldin et al., 2019, Setia, H et al., 2024).

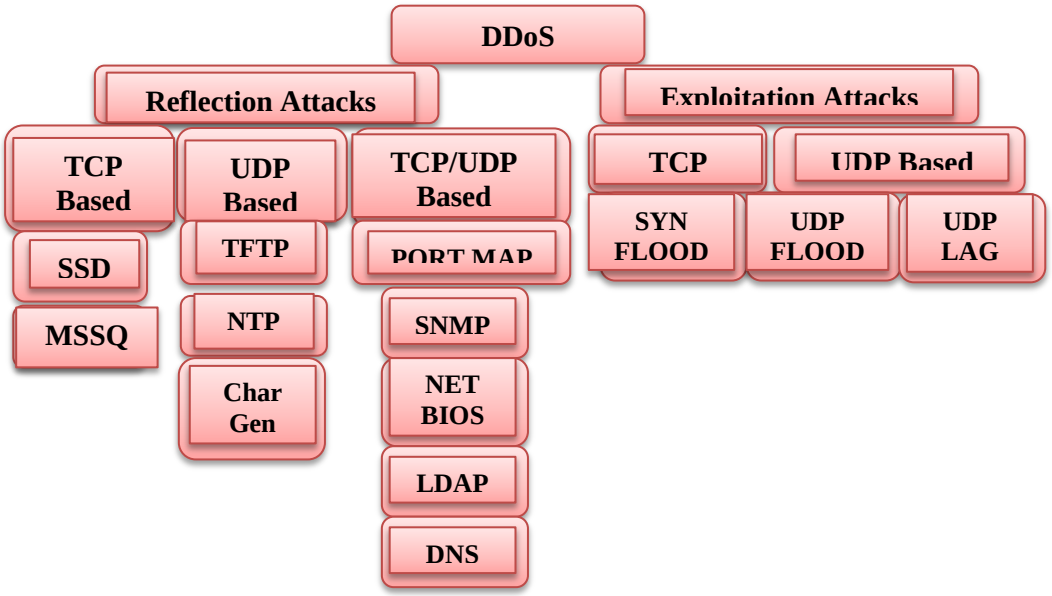

Figure 1.5 DDoS Attacks

A statistical survey of DDoS attacks equips researchers with the knowledge to diagnose and defend against these attacks in VANET. By analyzing the prevalence and trends of DoS and DDoS attacks, researchers can gain valuable insights. This knowledge allows them to prioritize countermeasures more effectively. They can then develop targeted detection and mitigation strategies tailored to each specific type of attack. The following section provided an attempt made in this study for the identification of defense strategy in securing VANET.

1.7 Statistical Survey on DDoS Attacks in VANET

DDoS assaults rose significantly as expected, according to a CISCO research, with a double-digit increase reaching 14.5 million in 2022. Service providers are at serious risk from these attacks, the largest of which was recorded at 1.7 Tb/s. DDoS assaults have resulted in significant downtime costs, amounting to USD 221,836.80. DDoS attacks on third-party data centers and cloud-based services have also escalated. Figure 1.6 illustrates a concerning trend in the frequency of Distributed Denial of Service (DDoS) attacks from 2017 to 2022. The vertical axis quantifies the number of DDoS attacks in millions, spanning from 0 to 16 million, while the horizontal axis denotes the respective years.

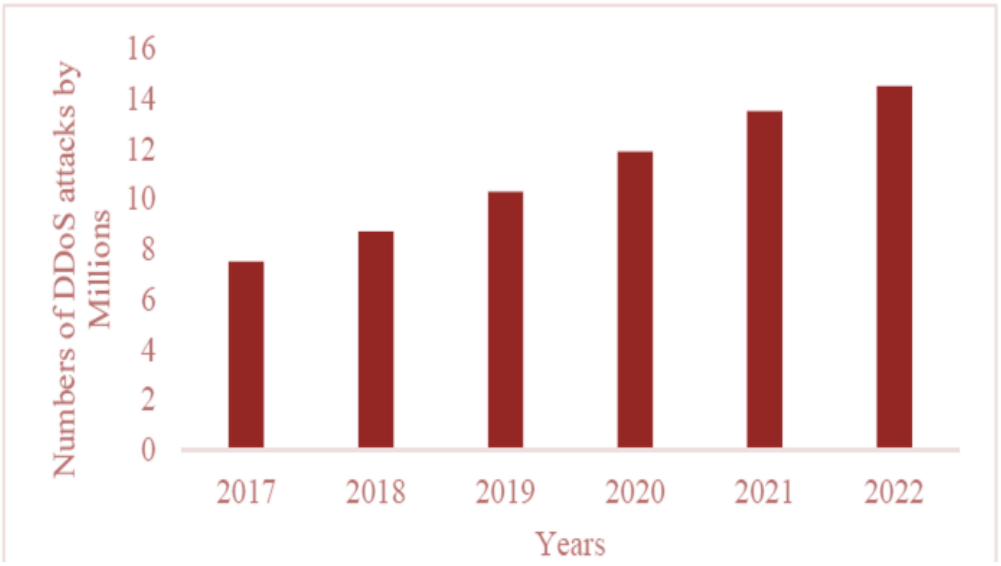

Figure 1.6 CISCO Research Trends of DDoS Attacks - 2017 – 2022

In 2017, the recorded attacks were under four million, marking the starting point of a consistent upward trajectory. Subsequent years witnessed a steady surge, with the figure escalating annually. By 2022, DDoS attacks surged to nearly sixteen million, underscoring a substantial and alarming increase. This escalating trend suggests a growing prevalence of such cyber threats, likely attributed to technological advancements, heightened reliance on digital platforms, and the dynamic nature of cyber threats, necessitating robust cyber security measures to counteract this worrisome trend.

1.8 DoS and DDoS attacks in VANET

The Network Layer (Layer 3) of the OSI model is closely associated with DoS and DDoS attacks. These attacks disrupt or hinder the availability of network resources or services. A DoS attack happens when a single source overwhelms a target system with an excessive amount of traffic, making it difficult or impossible to provide services to legitimate users. DDoS assaults are especially effective at the network layer, where resource depletion happens owing to the sheer amount of incoming requests because they include several dispersed sources coordinating their efforts to overwhelm the target, which is elaborated in further section (Ilavendhan, A et al., 2018).

1.8.1 DoS attacks

In a VANET, attacks known as denial of service (DoS) are a frequent occurrence and are designed to overwhelm or disrupt the network by saturating it with traffic or by interfering with the services it offers (Ilavendhan, A et al., 2018). An attacker often targets the communication channel to create traffic congestion or to block nodes from accessing the network. Preventing the authentic nodes from accessing network resources and services is the main goal. The assault would cause the VANET sources and nodes to fail. Lastly, genuine nodes can no longer access the VANET. DoS attacks shouldn't be allowed in VANET, where reliable life-critical data is exchanged. It has to arrive at its destination in a timely and safe manner. In summary, there are three ways that an attacker gets a denial of service attack: through a secure communication channel, network overloading, or packet dropping.

A DoS attack, as defined by calculation, is an effort to prevent a host's network-connected processes from accessing a system or VANET source by authorized users, such as by momentarily stopping or pausing. When many, sometimes hundreds of distinct IP addresses are used as the assault source, it is called a denial-of-service attack (DDoS). It's like when a group of individuals swarm the front entrance, preventing authorized people from entering the business and interfering with daily operations. DoS attacks are often carried out by malicious individuals and target popular online services like banks and credit card payment

gateways; however, other assaults may be motivated by activism, retaliation, or blackmail. In DoS, attackers disseminate misleading information to influence other drivers' actions (Gaurav, A et al.,2022).

Figure 1.7 shows the vehicle A2 delivers a bogus message containing traffic information luring vehicle V to alter its path for clearing the road.

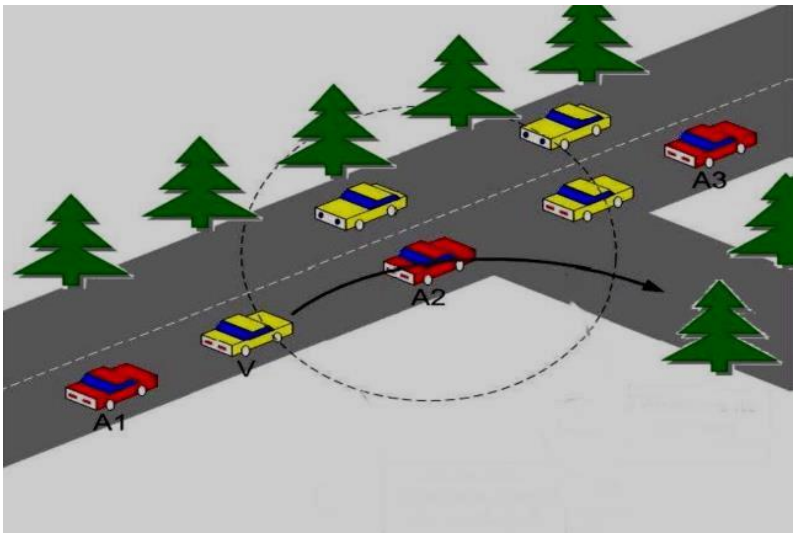

Figure 1.7 An Illustration of DoS attack in VANET

As a result, attackers monitor cars to get the private information of the drivers, and routing thwarts DoS attempts to sway the following scenarios:

- TCP, UDP, and ICMP are examples of overflow network types that interfere with legitimate traffic sites.
- Attempting to unplug the device and thus being unable to utilize their service.
- Making an effort to keep a certain person from using a service.
- Attempting to undermine a certain system or individual's service.
- Attempting to interfere with the routing system.

A DoS attack on a VANET can harm the safety-critical programs that depend on the network and cause communication failures.

1.8.2 DDoS attacks

One of the main risks to VANET is DDoS (distributed denial of service) attacks. In a DDoS assault, several attackers work together to overwhelm the network

with traffic, disrupting regular traffic in the process, as shown in Figure 1.8. DDoS assaults can seriously interfere with VANET, resulting in delays, data loss, and even system collapse. DDoS attacks can also be used as a cover for other attacks or as a means of disengaging network managers, making it more challenging to identify risks and take appropriate action.

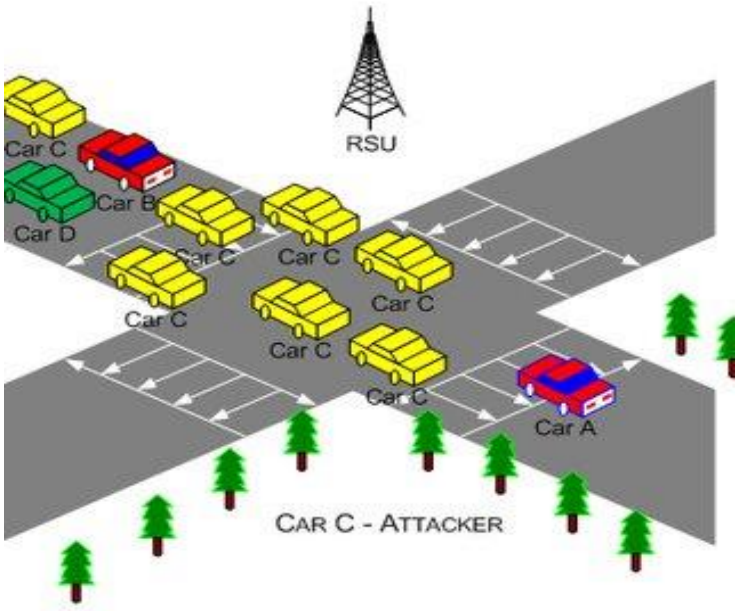

Figure 1.8 An Illustration of DDoS attack in VANET

The constantly evolving and growing nature of VANET, coupled with the critical need for real-time communication, makes defending against DDoS attacks a challenging task. DDoS attacks can be detected and mitigated using a variety of protection mechanisms, including intrusion detection systems, firewalls, and filtering approaches (Ilavendhan, A et al., 2018).

DDoS attacks on VANET can severely disrupt transportation systems and operations, jeopardizing network security and efficiency. As a result, it is crucial to create robust security measures and countermeasures in order to stop and lessen the effects of such attacks. These precautions include traffic filtering, dynamic network reconfiguration, and intrusion detection and prevention systems (Polat, H et al., 2020). From the research work (Kumar, A et al., 2019), there were twelve variants of DDoS attacks that pose significant security risks to VANET and can disrupt vehicle communication, leading to potential safety hazards on the road.

The existing defense landscape helps researchers prioritize their efforts and focus on developing more robust defenses. The variety of techniques highlighting their strengths and weaknesses hold significant value in identifying the gaps, feasibility and applicability of the existing solutions with the performance to select and implement the most effective defenses against DoS and DDoS attacks in VANET. The security solutions included cryptographic techniques, intrusion detection and prevention systems, trust and reputation management, artificial immune systems.

In the following section, the different security solutions that cater specific threats are introduced paving the way to better understand what works well in existing solutions. Further building up successful techniques to develop even more effective defenses is the focus of the research that has been proposed in the thesis.

1.9 Defense Landscape for VANET

Existing DoS/DDoS mitigation solutions for VANET provide valuable insights for researchers and network administrators. By understanding their strengths, limitations, and trade-offs, more effective defenses to safeguard VANET from these ever-evolving threats can be developed. The subsections that follow delve into the significance of existing solutions for securing VANET against DoS and DDoS attacks.

1.9.1 Cryptography-based Solutions

Cryptography-based solutions are crucial to addressing security challenges in VANET. Cryptography safeguards vehicle-to-infrastructure communication by ensuring the confidentiality, integrity, and authenticity of exchanged messages. It provides secure key exchange, message confidentiality, integrity, and authentication. Cryptography-based solutions in VANET include digital signatures, certificates, and encryption techniques. Digital signatures are used to provide message authenticity and are created using the sender's private key. Certificates are used to validate the authenticity of the sender's identity, and trusted authorities issue them. Encryption techniques are used to ensure message confidentiality and integrity. Symmetric key and asymmetric key encryption techniques are the two popular encryption techniques

used in VANET. Asymmetric key encryption is slower than symmetric key encryption but provides enhanced security. On the other hand, symmetric key encryption is faster, but it has limitations in key management. Cryptography is fundamental to ensuring the security of VANET communications (Ogundoyin, S.O et al., 2020).

1.9.2 Encryption and Decryption Techniques

Vehicular Ad-hoc Networks rely on secure communication between vehicles to exchange information for safety applications. Encryption and decryption methods are essential for safeguarding the security of these communications while they are being transmitted. The crucial aspects of VANET security relies on the security requirements based on the communication, computational power, communication overhead and the key management. The significance of encryption and decryption techniques in VANET leads to ensuring trust and security in data exchanged between vehicles. Secure communication through encryption and decryption in VANET favours improved road safety, enhanced traffic management and increased driver confidence. Encryption and decryption techniques are the backbone of secure communication in VANET.

Safeguarding sensitive data, promoting trust and enabling a safer and more efficient transportation system are the key benefits of encryption and decryption techniques. One commonly used technique is the block cipher algorithm in Advanced Encryption Standard (AES) for encryption and decryption of messages. Another popular technique is the RSA, a prominent public-key encryption algorithm that utilizes a pair of keys – a public key for encryption and a private key for decryption. Initially, symmetric encryption with a shared secret key was prevalent for its efficiency. However, secure key distribution and management for large networks proved challenging.

Public-key cryptography (RSA, ECC) emerged to address scalability issues. It allows for wider distribution of public keys for encryption, while private keys remain confidential for decryption. The security of communication in VANET is greatly

aided by encryption and decoding techniques. These methods safeguard the information against unwanted access and make sure that only the intended recipient may access it. When a message is encrypted, it is converted from plaintext to cipher text; when decrypted, it is converted from cipher text back to plaintext. Encryption techniques are employed in VANET to secure communication between vehicles and traffic management centers or road infrastructure (Polat, H et al., 2020). Without proper encryption and decryption, VANET become susceptible to the attacks, potentially leading to privacy violations, traffic manipulation causing unnecessary congestion or accidents and safety risks.

1.9.3 Intrusion Detection System based Solutions

Intrusion Detection Systems (IDS) are security mechanisms that monitor network activity for any unauthorized access attempts and then respond accordingly. IDS can be implemented in VANET to detect any malicious activities or attacks by analyzing incoming and outgoing packets. In order to detect anomalies in the system, the algorithm first creates a set of detectors that represent the self - cells. The method generates random bit strings and compares them to the detectors, which are commonly recorded as bit strings. A bit string is deemed a self-cell and rejected if it matches a detector. If no detector detects it, it is considered to be a non-self-cell and is flagged as an anomaly (Kumar, A et al., 2019).

1.9.4 Swarm intelligence-based techniques

Swarm intelligence-based techniques refer to a class of optimization algorithms that simulate the collective behavior of natural swarms such as ants, bees, birds, and fish. These techniques are inspired by the behavior of social insects that demonstrate decentralized, self-organized, and adaptive behavior to solve complex problems. In the context of VANET, swarm intelligence-based techniques have been used for various applications such as routing, clustering, and security. For instance, the ant colony optimization algorithm has been used for route optimization, while particle swarm optimization has been used for data clustering. These techniques have also been used for intrusion detection in VANET, where they help identify malicious

nodes attempting to launch attacks. Swarm intelligence techniques excel at solving complex problems efficiently and effectively through decentralized and self-organized approaches (Zaidi et al., 2018).

1.9.5 Artificial Intelligence-based Techniques

Artificial Intelligence (AI)-based techniques leverage machine learning algorithms to train a model that can accurately detect and classify attacks in real time. For instance, Support Vector Machines (SVM), Neural Networks (NN), and Decision Trees (DT) have been applied to VANET intrusion detection. In SVM-based intrusion detection, a model is trained using labeled data containing both normal and attack traffic. The model learns to classify incoming packets into either normal or malicious traffic. Similarly, NN-based techniques use a multi-layered perceptron to learn the features of the incoming packets and classify them accordingly (Remya Krishnan, P et al., 2022). DT-based intrusion detection systems operate on a tree-like structure where nodes represent features and leaf nodes represent the final classifications. Labeled data is used to construct a decision tree, and new packets are classified by following the tree's path from the root node to the relevant leaf node (Mokdad, L et al., 2015).

AI techniques have also been used to improve the efficiency and security of VANET routing. For example, Machine Learning (ML) algorithms have been applied to predict the optimal route for a vehicle based on factors such as traffic congestion, road conditions, and destination. Additionally, Reinforcement Learning (RL) algorithms have been used to learn the optimal routing strategy by interacting with the environment and receiving feedback in the form of rewards or penalties (Gad, A.R et al., 2021).

1.9.6 Artificial Immune System

A viable solution to the Host Based Intrusion Detection System (HIDS) is AIS. Immunology and known immune processes serve as the foundation for adaptive information systems (AIS), which are flexible systems that are used to solve problems and AIS based attack detection is shown in Figure 1.9. The behavior of AIS is studied using the Negative Selection Algorithm, Positive selection algorithm, Immune Network

Algorithms, and Dendritic Cell Algorithms. It aids in the network's ability to identify different DoS attacks. Artificial immune systems (AIS) frequently employ the negative selection algorithm (NSA) for anomaly detection in a variety of applications, such as intrusion detection systems (IDS) for VANET.

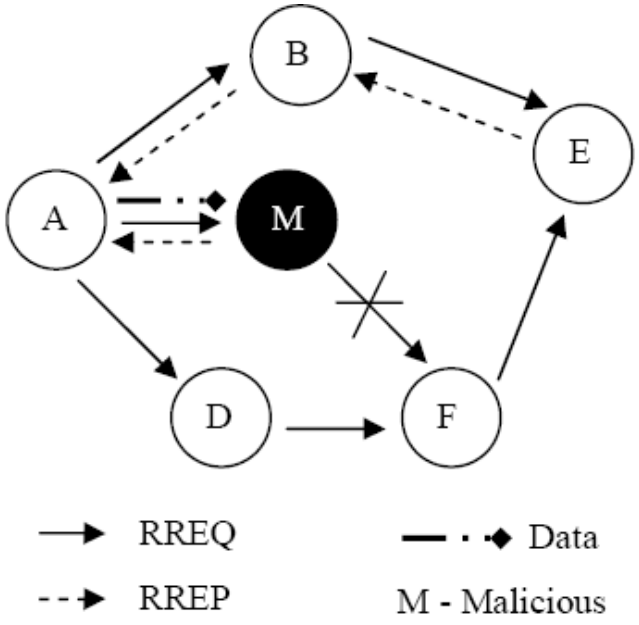

Figure 1.9 Artificial Immune System based Attack Detection

The biological process of the human immune system's negative selection of T-cells, in which self-cells are chosen, and non-self-cells are eliminated, served as the model for the NSA. The Artificial Immune System (AIS) framework includes the Positive Selection Algorithm (PSA), which is modeled after the biological immune system's techniques for identifying and eliminating foreign cells (Aldhaheri et.al., 2020). The immune system's capacity to eliminate self-reactive cells serves as inspiration for the NSA. The PSA, in contrast, is predicated on the immune system's ability to identify self-cells. The non-self-cells are therefore viewed as intruders. In essence, the NSA is made to be employed in situations involving anomaly detection, intrusion detection, change detection, similar pattern identification, and two-class categorization. Because of its simplicity and ease of use, NSA has been employed successfully over time in a variety of application domains. The foundation of conventional NSA is the random generation of a sizable number of self-cells and detectors, as well as a matching mechanism between the two. Only the unmatched detectors will be left after the elimination of the matched

detectors. Unknown intrusions are found using the non-matched detectors as a countermeasure. This technique has the potential to increase the amount of time that is wasted during the matching and self-cell production processes.

The PSA detects and reacts to particular antigens, which are alien chemicals or cells that might be harmful to the host, using a group of detectors known as antibodies. The fundamental job of the PSA is to choose the best combination of antibodies that can recognize and destroy antigens with the least chance of damaging the host's own cells. The training phase and the detection phase are the two stages of the PSA's operation. During the training phase, a pool of randomly selected antibodies is created, and each antibody is scored according to how well it can identify and bind to a particular antigen. To improve their capacity to detect and react to the antigen, the antibodies that have the highest affinity for the antigen are chosen and subjected to additional optimization. The chosen antibodies are employed to identify environmental antigens during the detection phase. When an antigen is encountered, the antibodies that correspond to its properties will bind to it, eliciting an immunological response. The immune reaction can take a variety of shapes, including the elimination of the antigen; it is marking for later removal, or the enlistment of additional immune cells to assist in the attack. Another important algorithm in AIS is dendritic cell algorithm (DCA) and clonal selection algorithm.

The function of dendritic cells in the human immune system served as the inspiration for the Dendritic Cell Algorithm (DCA), a form of Artificial Immune System (AIS). Several fields, including intrusion detection in VANET, have used it. The DCA operates in the context of VANET by gathering environmental data and detecting harmful activity by comparing the data with established rules. The DCA is appropriate for safeguarding VANET since it can identify fresh and undiscovered assaults. An Artificial Immune System (AIS) called the Dendritic Cell Algorithm (DCA) is modeled after the actions of dendritic cells in the human immune system. It has been used in many different sectors, such as intrusion detection in VANET. When applied to VANET, the DCA gathers data about the surrounding area and detects suspicious activity by comparing the data to predetermined rules.

To protect Vehicle Ad Hoc Networks (VANET), the Defense Countermeasures Agent (DCA) needs the capability to detect new and previously unknown cyberattacks. The Clonal Selection Algorithm (CSA), a type of Artificial Immune System (AIS) algorithm, can be employed. CSA mimics how the immune system responds to foreign substances (antigens) to identify and neutralize these threats. The CSA process starts with a group of randomly generated antibodies that have the potential to bind with antigens. The algorithm then evaluates the fitness of each antibody based on its ability to bind with an antigen. The antibodies with higher fitness are selected and cloned to generate a new population of antibodies. The new population undergoes a mutation process that introduces diversity in the population. The process of cloning and mutation continues until a stopping criterion is reached, such as the achievement of a certain level of diversity or fitness. The end result is a population of antibodies that are highly specific to the target antigen. Applications of the Clonal Selection Algorithm (CSA) are diverse, encompassing pattern recognition, optimization problems, and the detection of unusual events or anomalies.

1.10 Limitations of Existing Defense Landscape for VANET

Vehicle Ad-hoc Networks (VANET) hold immense promise for improving traffic safety and efficiency. However, securing these networks presents a significant challenge. Here are some limitations of the existing defense landscape for VANET:

The inherent openness (Alharthi, A et al., 2020), decentralized and dynamic nature (Al-Shareeda et al., 2020) continue to challenge existing defense based on prevention, detection, response and tolerance solutions to secure VANET against DoS and DDoS attacks. Various filtering mechanisms are in use for prevention. Different techniques for attack detection including statistical, soft computing, knowledge based and machine learning techniques were proposed. Tolerance or mitigation strategies have been considered for the handling of DDoS attacks and still research is towards keeping services operative as usual when VANET attacked. Intrusion Detection Systems (IDS) may face difficulties in distinguishing between normal and malicious traffic in real time, especially when dealing with the intermittent connectivity and rapidly changing network topology of VANET. Furthermore, ensuring the authenticity of messages in a decentralized and

dynamic environment is another hurdle, as existing cryptographic solutions may struggle to provide efficient and timely verification (Anyanwu, G.O et al., 2022).

In this thesis, a hybrid approach for mitigating DoS attack and types with self-healing effect and immunization is proposed. Triple Random Hyperbolic Encryption (TRHE) with Hex-tuple mapping is provided as the proposed strengthening method for the VANET for reliable transfer among trust nodes through routing. Trust based approach and self – healing effect of Artificial Immune System (AIS) are proposed for the detection, prevention and isolation of malicious DoS attacks and types. Encryption and mapping are also proposed to improve the performance of VANET and ensure continuous operation. These methods can enhance routing efficiency and provide a form of "immunization" against cyberattacks.

Assumptions

The following assumptions were made during the implementation of this research.

i. Vehicular Ad Hoc Network (VANET) was considered as the network organized into distinct areas called domains or clusters. Each of these domains is overseen by a designated Roadside Unit (RSU). This RSU is responsible for facilitating and managing group communication within its respective domain.

ii. In V2I communication model, all communication considered within a group of vehicles must be routed through the designated Roadside Unit (RSU) in their domain. To achieve this, each vehicle utilizes the Ad-hoc On-demand Distance Vector (AODV) routing protocol to send and receive messages via the RSU following IEEE 802.11 standard, commonly used for Wi-Fi, has been adapted for vehicular environments to provide wireless communication capabilities for vehicles.

iii. All Roadside Units (RSUs) were assumed to be able to communicate with each other directly (wired or wireless) or indirectly through the Regional Trusted Authority (RTA).

iv. The research assumed that all Roadside Units (RSUs), Regional Trusted Authorities (RTAs), and the central Trusted Authority (TA) were secure and not vulnerable to attacks. Furthermore, the security settings of each node within the network, including both vehicles and RSUs, were subject to regular updates.

1.11 Motivation and Justification

VANET are crucial for intelligent transportation systems, enabling safety-critical communication and improving traffic management. However, they are vulnerable to DoS/DDoS attacks that disrupt communication and potentially endanger lives. With the intention to provide safe roads, the present research proposal aims to exhibit the outcomes of the hybrid approach in securing VANET against DoS attacks and types with continued VANET services enabling safety and reliable communication. The message rate and transmission time among the vehicles in the RSU clusters are monitored through the algorithm. The difference between the predicted and actual transmission times for data communication is calculated. Deviations delay data transmissions and delays can compromise critical reaction times and increase the risk of accidents, impact the performance of applications. The trustiness with self-healing effect of AIS is enforced to mitigate deviations by isolating the maliciousness of the attack reducing reliance on centralized servers and improving response time.

However, the dynamic and unpredictable network environment brings in new attacks needs protection through ongoing self-healing effect of AIS. This brought in for the strengthening of the access control and mapping techniques in self-healing effect of AIS. Restricting attackers with strong access control measure prevents unauthorized access and limits the impact of compromised nodes. Mapping helps in facilitating the identification of the source and allows routing and isolation. The clusters with relation nodes for communication are difficult in mobility of the vehicles. With the help of the immunity approach, a balance between cluster groups with relation nodes is ensured to obtain a high packet delivery ratio without the need for positive or negative selection. The dynamic fluctuating network leads to transmission of attacks and communication is disrupted. With the help of multiple parallelized path links in regular circular updation

adopting time and frequency synchronized channel hoping eliminates the traffic of DoS attack and types.

1.12 Problem Statement

The Vehicular Ad-Hoc Networks experiences the unavailability of services, disrupted communications and inaccessibility of network resources due to DoS and DDoS attacks harming safety-critical situations resulting in delays, data loss, and even system collapse.

1.13 Research Questions

The statistics based on DoS attacks and types in VANET necessitate the securing methods to address the existing scenario. The research questions formulated in addressing this problem are

i. Is it feasible to effectively enhance the detection and classification of various DoS attacks in VANETs?

ii. Can VANET provide its continued operation in mitigating DoS attacks and its types?

iii. Can the data transmission be made without any loss in the VANET on mitigation?

1.14 Objective of the Thesis

The primary objective of this research is to secure Vehicular Ad-Hoc Networks in Intelligent Transportation System through a hybrid approach to detect and mitigate DoS attacks and types with Self-healing and Immunization.

The secondary objectives that aim to fulfill the major objective are:

i. To enhance the detection with classification of DoS attacks with improved accuracy of detection and classification, recall, precision, minimum delay.

ii. To detect, predict and isolate (Mitigate) DoS attack and types with the communication link maintained having increased accuracy of detection, recall, precision, minimum delay, improved packet delivery ratio.

iii. To enhance the security and reliability of VANET services with minimum packet loss, maximum throughput, minimum processing time and maximum packet delivery ratio.

Secondary objective (i) focuses on the detection and classification of DoS attacks. It aims to improve the accuracy, recall, precision, and speed of this process through enhancing methods. Secondary objective (ii) expands on this by adding prediction and isolation (mitigation) of DoS attacks to the scope and it also assesses towards the metric packet delivery ratio with the communication link maintained for continued operation.

The scope of the research will focus on DoS attacks and its types considering the characteristics, challenges and the security requirements of the VANET. The security of VANET through the hybrid approach with the design, implementation and evaluation is applied. Thus, leveraging the strengths of multiple approaches to create a more effective and comprehensive solution with enhanced detection, proactive defense, resilience, adaptability.

1.15 Significant Contributions of the Thesis

The six significant contributions proposed based on the three-phase methodology implemented in the research work are:

The contributions are highlighted below:

Contribution 1: Enhanced Feature Selection and Mitigation for Detection and Classification of DoS attacks using Glow-worm SLFN

In attaining the primary objective of the research work, the contribution 1, involved developing a model that uses feature selection to detect and classify Denial-of-Service (DoS) attacks. This model was initially designed to detect and mitigate these attacks. The model is built using Glow-worm optimized technique for optimized selection of features and a classifier to classify as normal and DoS attacks.

Contribution 2: Abnormal behavior Detection using Response Feedback Algorithm with Micro Cluster Outlier Detection and Linear Regression (MCOD-LR)

The enhanced model is built to deal with multiclass attacks of DoS wherein the contribution 1detected only two attacks. The proposed algorithm is implemented for the VANET simulated using Network Simulator 3 (NS3). The temporal information with variations is considered for abnormal detection due to DoS attacks. The simulation outcomes indicate that the proposed enhanced model exhibits a high degree of effectiveness in detecting anomalies or deviations in traffic flow patterns.

Contribution 3: Prediction of Malicious DoS Attacks using Kernel Density Estimation and Entropy-based Support Vector Machine (SVM) Classifier

The cluster behaviour determines the network performance with communication links established among the vehicles. Considering the neighbour vehicles is crucial for the transmission with the link established through trust vehicles to reach the destination. The malicious vehicles must be handled during the transmission. In contribution 3, the trust-based approach is incorporated to predict the maliciousness based on DoS attacks. The classifier predicts the variations in the trust value and entropy for randomness deviation. Kernel Density estimation with Entropy-based Support Vector Machine classifier predicts the maliciousness of the nodes based on DoS attacks.

Contribution 4: Isolation using Reliance Node Estimation - Pearson correlation coefficient and Bayesian aggregate model with Self-healing effect of Artificial Immune System (AIS)

In addition to the prediction of the maliciousness of the nodes based on trust factors, the communication link is to be maintained based on the nodes relationship, functionalities of the vehicles. This approach ensures the formation of high-quality clusters by carefully evaluating factors such as the vehicle density, energy consumption, packet delivery success rate, and the effectiveness of attack detection. The contribution 4 Reliance Node Estimation - Pearson correlation coefficient and Bayesian aggregate model with Self-healing effect of Artificial Immune System (AIS) focus on identifying the similarity among nodes and the functionality based on the credibility and isolating the malicious nodes based on DoS attacks. The self-healing effect of AIS is performed by checking the similarity and credibility of the new vehicles with the predicted values. On checking, the isolation is enforced resolving the cluster quality.

Contribution 5: Strengthening the Access Control and Mapping for Detecting DDoS attacks and its types using Triple Random Hyperbolic Encryption (TRHE) and Hex-Tuple Matched Mapping with Deep Auto Sparse Impasse Neural Network

The VANET changing topology with vehicles moving in varying ranges enforces challenging situation for routing of data packets through similar nodes. The contribution 4 implemented over varying vehicles has to be secured for the transmission from unauthorized access and attacks disrupting such transmission. In contribution 5, Triple Random Hyperbolic Encryption (TRHE) with Hex-Tuple Matched Mapping using Deep Auto Sparse Impasse Neural Network provides the secured traffic through rational vehicles. The mapping report identifies the secured way for communication and also utilized by Deep Auto Spare Impasse NN to detect the 12 variants of DDoS attacks.

Contribution 6: Immunization of clusters and Routing using Deep Trust Factorization (DT) NN, Moth Flame Optimization algorithm and Cache parallelized circulation link routing

The availability of VANET services is hindered by the rapidly changing topology. The fluctuating changes in the network challenge the continuous availability and stability of the VANET. The varying vehicles as nodes alter the connection status with delay in data transmission. In contribution 6, the mapping and sensing report with network metrics, feedback from vehicles are the determining factors for the network behaviour. Deep Trust Factorization (DT) NN monitors and isolates the irrational nodes based on the trust scores of the vehicles. On classification of rational and irrational nodes during the changing network topology, the transmission is enforced through immunization.

Moth Flame Optimization algorithm, a metaheuristic population-based algorithm, immunizes the VANET searching the only the reliable vehicles in the dynamic network isolating the malicious vehicles. VANET security is enhanced as the reliable vehicles are identified and the transmission can be made with high Packet Delivery Ratio (PDR).

For the transmission, the dynamic fluctuation of each vehicle remaining a challenge is handled by Cache parallelized circulation link routing. With the optimization

algorithm connecting the vehicles in the circular link, time and frequency synchronization base channel hopping is applied to reduce the interference among vehicles. The throughput of the VANET is enhanced thus the responsiveness of the network is provided.

The immunity is ensured to provide stability in the VANET with transmission of data through Moth Flame Optimization and Cache Parallelized Circulation Link Routing.

1.16 Organization of the Thesis

This thesis consists of four chapters and is focusing on the research objectives. The organization of the thesis is as follows.

Chapter 1 : This chapter presents the origin of the research work.

Chapter 2: This chapter presents the associated works on the VANET and its security landscape against DoS attacks and its types. The handling of DoS attacks and its types with detection, prevention and mitigation are studied and tabulated with significance of the existing security solutions. The need for the enhanced security approaches from the existing defense landscape provided is mentioned.

Chapter 3 : This chapter defines the conceptual framework of the research design. A three step methodology with six different contributions proposed is discussed. The framework is instantiated with the simulation of the VANET considering the datasets CIC-IDS 2018 and CIC-DDoS 2019. In the Phase 1, detection and classification of DoS attacks using Glow-worm Single Layer Feed Forward Neural Network (SLFN) is the contribution 1 proposed. Optimized selection of features and a classifier to classify as normal and DoS attacks are elaborated with its implementation process. Furthermore, an enhanced model is built to deal with multiclass attacks of DoS. For such detection, at the inception, the abnormal behaviour is detected with the deviations using Response Feedback Algorithm with Micro Cluster Outlier Detection and Linear Regression (MCOD-LR) is proposed as the contribution 2.

The malicious vehicles in the clusters are further detected based on trust based approach with the classifier as the contribution 3. In this, the Prediction of Malicious DoS Attacks using Kernel Density Estimation and Entropy-based Support Vector Machine

(SVM) Classifier is detailed with its procedure. The mitigation process through isolation of detected malicious vehicles based on DoS attacks is proposed using contribution 4. The Pearson correlation coefficient method is used to assess the degree of similarity between the predicted and actual values of parameters for different vehicles. The diverse features and the functionalities of the vehicles are also accounted using the Bayesian aggregate model based on the trust and credibility. The self-healing capability of Artificial Immune Systems (AIS) allows them to identify and isolate malicious nodes within a network.

Phase 2 focuses on the strengthening of the network traffic with encryption and mapping through the Triple Random Hyperbolic Encryption (TRHE) with Hex-Tuple Matched Mapping. In this contribution 5, Deep Auto Sparse Impasse NN is added to detect the twelve types of DDoS attacks. The proposed approach was evaluated by comparing its performance to that of existing methods, namely Trilateral Trust, H-IDS, Multi Filter, and SPPA. The final Phase 3 includes the immunization of clusters and routing using the contribution 6. The security and reliability is provided by the Deep Trust Factorization Neural Network (DT-NN) based on trust scores. The Moth Flame optimization (MFO) algorithm detects the best path in the network by updating each vehicle position. Efficient routing of packets around congestion and malicious nodes is enabled by considering multiple paths simultaneously to avoid congested or unreliable links. The Cache parallelized Circulation Link routing (CCL) through time and frequency synchronization base channel hopping achieves improved throughput, reduced latency, and enhanced security.

Chapter 4: This chapter provides the outcomes of six contributions with the experimental setup for implementation and to obtain the results based on the performance metrics with comparisons and discussions.

Chapter 5 and Chapter 6: The concluding remarks on the overall performance of the proposed approach for securing VANET are highlighted with significant outcomes in chapter 5. The exploration of the proposed research work for further enhancement with its scope of implementation are provided to widen the research perspectives on developing robust security solutions for VANET to be beneficial by the transportation system and the road users.

1.17 Conclusion

This chapter has established the critical importance of securing Vehicular Ad-hoc Networks (VANET) in the context of Intelligent Transportation Systems (ITS). Vehicular ad-hoc networks (VANET) face unique security challenges due to their dynamic nature, limited resources, and reliance on wireless communication. These factors make them highly susceptible to attacks, particularly Denial-of-Service (DoS) attacks. The potential consequences of these attacks on traffic safety and efficiency are severe, underscoring the urgent need for effective countermeasures.

This research presents a hybrid solution to address the security challenges in VANET. This solution integrates techniques for mitigating DoS attacks, enabling self-healing capabilities, and enhancing network immunization. By integrating these strategies, the aim is to create a resilient and secure VANET environment. The following chapters will delve deeper into the proposed methodology, its implementation, and evaluation.

1.18 Chapter Summary

A core focus of the chapter is the introduction of a hybrid approach to combating DoS attacks. This approach combines multiple security measures, including intrusion detection, prevention, trust and cryptographic techniques, to create a layered defense strategy. The chapter elaborates on the advantages of this hybrid approach in addressing the multifaceted nature of DoS attacks.

To enhance the network's resilience, the concept of self-healing is introduced. This involves implementing mechanisms to automatically detect and recover from DoS attacks, minimizing their impact on network performance. The chapter discusses various self-healing techniques, such as redundancy, fault detection, isolation, and recovery strategies.

Furthermore, the chapter emphasizes the significance of immunization in preventing future DoS attacks. It explores proactive measures like intrusion prevention, anomaly detection, blacklisting to strengthen the network's defense capabilities.

The chapter emphasizes the need for continued research and development efforts to advance the security of vehicular ad-hoc networks (VANET). The emphasis is made on the need for adaptive and intelligent security solutions to address the evolving threat landscape.

The next section focuses on the available literature for the problem defined.