Eyes on the Road: A Survey on Cyber Attacks and Defense Solutions for Vehicular Ad-Hoc Networks

Amber Hankins, Tapadhir Das, Shamik Sengupta, David Feil-Seifer
Department of Computer Science and Engineering, University of Nevada, Reno, USA
Email: amberhankins@nevada.unr.edu, tapadhird@nevada.unr.edu, ssengupta@unr.edu, dave@cse.unr.edu

2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) | 979-8-3503-3286-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/CCWC57344.2023.10099187

***Abstract*—In the last decade, Vehicular Ad-Hoc Networks (VANET) have garnered significant interest and concern. VANETs allow vehicles on the road to communicate with each other and with the Internet, ensuring the safety and comfort of passengers. VANETs provide traffic and weather reports, collision prevention, and many more applications. However, VANETs have become an alluring target for cyber attacks. In this paper, we provide a survey on cyber attacks and protection solutions for VANETs. We begin by addressing various types of cyber attacks that can affect VANETs and the security properties that they can compromise. We subsequently illustrate multiple protection solutions that have been proposed in response to these attacks and the various security concerns they can help alleviate. We observe that the proposed solutions have the capability of addressing all areas of security concern in a VANET. However, this knowledge can assist attackers in creating new cyber threats that can circumvent current protection solutions. Hence, we finish off the paper by introducing some open research areas that can help further address cyber threats and can assist in creating more robust security solutions to protect the next generation of VANETs.**

***Index Terms*—Vehicular Ad-Hoc Networks, Cyber Attacks, Defense Solutions, Machine Learning, Blockchain, Trust, Public Key Infrastructures**

I. Introduction

According to a 2022 statistic presented by the World Health Organization, road traffic injuries are the leading cause of death for persons aged 5 to 29 years [1]. Many of these incidents can be attributed to human error, including speeding, distracted driving, driving under the influence, and slow emergency response times. Greater communication between vehicles, pedestrians, and emergency services could save many lives. For this purpose, vehicular ad-hoc networks (VANET) can provide a comprehensive solution to many instances of human error on the road.

There are several important applications of VANETs. Using onboard units, vehicles can communicate with each other to share information about road conditions, weather reports, and emergency alerts. This data can allow vehicles to intelligently plan the safest and most efficient route while conveying important information to the user. Vehicles can also communicate location data to surrounding nodes on the network, eliminating many issues stemming from distracted driving, or driving under the influence. Since vehicles can constantly broadcast location data to nearby stoplights, smart crosswalks, and neighboring vehicles, VANETs contribute greatly to collision prevention as well as pedestrian safety. During emergencies, the vehicle's connection to the internet and central infrastructure allows it to immediately notify first responders, cutting down response times, and potentially saving lives.

979-8-3503-3286-5/23/ $31.00 ©2023 IEEE

Since these networks have so much potential, they must be designed with security in mind. Vehicles in these systems rely on trustworthy, secure information to make critical decisions, and any disruption to these systems could have dangerous consequences. For instance, cybercriminals may intercept information being transferred on the network, and redirect it so that it cannot reach its destination. They can also flood the system with false or outdated information, rendering the network incapable of keeping up with road conditions in real-time. Additionally, any attack that causes delays or outages in service could severely impact drivers and pedestrians on the road.

In this paper, we provide a survey of cyber attacks against VANETs and the central categories of security concerns that they can compromise: availability, confidentiality, authenticity, data integrity, and non-repudiation. Also, we highlight defense mechanisms for VANET security and identify the types of security concerns they can help alleviate. Additionally, we propose certain open research areas that can be explored to further provide VANETs with more robust security against cyber attacks. The main contributions of this paper include:

- Providing a survey of cyber attacks against VANETs and the respective category of concern that they compromise.
- Highlighting proposed defensive mechanisms in literature for VANET security and the type of security concern they help alleviate.
- Proposing open research areas that can be explored to provide more rigorous protection for VANETs against cyber attacks.

The rest of the paper is structured as follows: Section II provides a background on the VANET architecture. Contemporary cyber attacks on VANETs are presented in Section III, while the proposed protection solutions are illustrated in Section IV. Section V presents certain open research areas which have the potential of creating more robust security solutions for VANETs. Finally, conclusions are drawn in Section VI.

II. Background

Through the examination of existing work on VANETs, we establish a baseline of information regarding structure and security. The following subsections provide background on

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

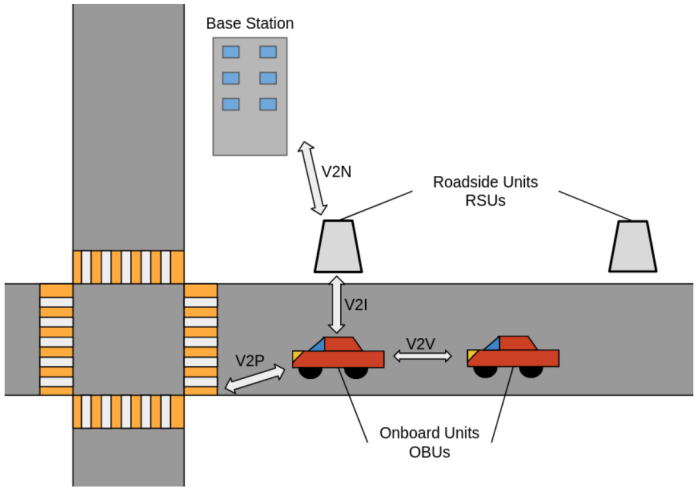

Fig. 1: WAVE Framework for V2X Communication

VANET communication standards and protocols, structures and architectures, and vulnerabilities.

A. Communication

To ensure the safety of passengers and pedestrians, VANETs must accommodate several types of communication. In [2], Nkenyereye et al. enumerate four categories of communication that are essential to the implementation of vehicular networks: Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Network (V2N). These modes of interaction are enabled by wireless communication standards and protocols. In the work presented in [3], the authors identify Wireless Access in Vehicular Environments (WAVE) and Dedicated Short Range Communication (DSRC) as the standards for vehicular network communication.

The IEEE 1609 family of standards aims to provide an architecture for V2V and V2I wireless communication with the introduction of WAVE. As explained in Uzcategui's WAVE tutorial [4], communication within the WAVE framework is made possible using onboard units (OBUs) and roadside units (RSUs). Each vehicle on the network is equipped with an OBU that can send and receive information from neighboring vehicles, RSUs, and any other authorized wireless access point. RSUs are fixed units positioned along roads that exchange information with vehicles, other RSUs, and the central infrastructure of the network. Utilizing both OBUs and RSUs, a WAVE framework enables all four categories of V2X communication previously enumerated, as seen in Figure 1.

The standard technology for facilitating this communication is DSRC. DSRC is accomplished using bands of radio frequencies, which have been allocated by governing organizations like the Federal Communications Commission. However, as discussed in [5], DSRC may encounter some limitations in the realm of vehicular networks. Due to the fast-paced, highly dynamic nature of a VANET, nodes may only be within range of each other for short periods. This requires DSRC to be supplemented with other technologies for effective operation.

B. Structure

Utilizing the WAVE family of standards, the common architecture of vehicular networks includes OBUs, RSUs, and a *trusted authority* or *base station*, which serves as a centralized connection to the Internet. Using a cloud-based architecture, [6] presents a system model consisting of the vehicular cloud, local cloud, and remote cloud. Vehicular clouds connect adjacent vehicle OBUs to establish V2V communication, pooling resources, and information. These clouds are constantly changing as traffic tends to be high-paced, and communications are proximity based. Local clouds are composed of nearby OBUs, RSUs, and other wireless access points, enabling V2I and V2P communication. The remote cloud is the top-level cloud hosted by the trusted authority or base station, offering internet servers for V2N communication. Since remote clouds are centralized authorities that provide key internet connectivity, they require the most resource allocation and suffer the greatest delay.

Yu et al. discuss relevant use cases of the cloud-based network model, including real-time navigation [7]. In this scenario, a vehicle requests cloud resources for real-time navigation. A virtual machine (VM) cluster is established in the remote cloud, and a VM is established in the nearby local cloud. The remote VM cluster provides traffic data, while the local VM forwards this information to the vehicle. As the vehicle moves, the local VM will move to adjacent local clouds, but will always refer to the same remote VM cluster. This example illustrates the basic functionality of the cloud-based network model.

C. Vulnerabilities

This section examines some known vulnerabilities of VANETs. Lu et al. [3] categorize several of these security concerns into five relevant groups:

- **Availability**: Any attack that threatens the operation of the network is an attack on availability, such as Denial of Service (DoS) and spam attacks. This should be the foremost category secured since it can render the entire system inoperable.
- **Confidentiality**: Attacks on confidentiality aim to intercept private data and information. The use of encryption within the network can drastically reduce the dangers of these attacks.
- **Authenticity**: Attacks on authenticity attempt to falsify credentials, send false information, or otherwise disrupt the regular operation.
- **Data Integrity**: Data integrity attacks are the unauthorized creation or modification of data.
- **Non-repudiation**: A repudiation attack allows attackers to deny that a certain transmission occurred, rendering system logs unreliable.

In our analysis of attack vectors and solutions, we will focus on vulnerabilities that affect these five categories.

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

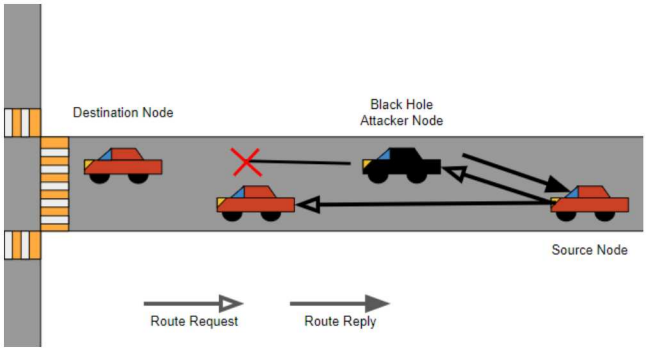

Fig. 2: Illustration of Black Hole Attack

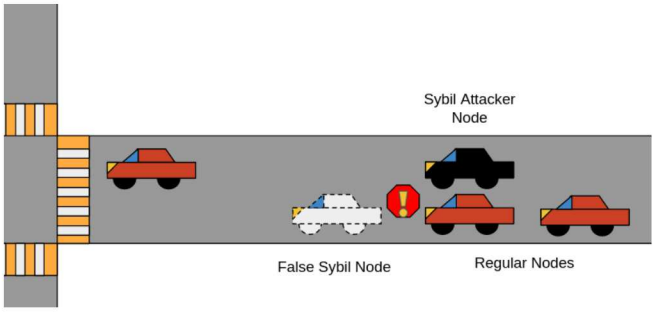

Fig. 3: Illustration of Sybil Attack

III. Attacks on Vehicular Networks

A. Availability

Attacks that threaten the functionality of networks resulting in delays, confusion, and outages will be referred to as attacks on availability. In this section, we discuss three such attacks.

1) ***Denial of Service (DoS):*** The purpose of a DoS attack is to prevent regular nodes from using the network properly. The mode of operation for a DoS is to overwhelm the network or exhaust its resources, to achieve this goal. Functioning nodes must use V2I and V2V communication to send and receive information from nodes around them. In a DoS attack, a malicious node continuously sends unnecessary messages to a nearby node, keeping up a constant stream. This keeps the node busy, effectively cutting them off from communication with the rest of the network. This can result in a vehicle on the road being overwhelmed with messages and unable to receive critical information from other nodes. It can also be used to overwhelm an RSU, keeping it from providing vital services to other vehicles [8]. In this way, DoS attacks can be achieved in both V2I and V2V avenues.

2) ***Black Hole:*** The Black Hole attack is another commonly discussed attack in vehicular networks. Functioning nodes on these networks regularly send out Route Request (RREQ) packets, communicating with neighboring nodes to map the optimal routes to their destinations. In a Black Hole attack, a malicious node will quickly respond to an RREQ packet with a Route Reply (RREP) Packet containing the minimum hop count. The source node will consider this to be the optimal route and begin transferring data packets to the malicious node. Now the malicious node can drop these packets, preventing them from reaching their destination [9]. A Black Hole attack halts the sharing of information in a specific geographic location on the network. Since communication packets are being dropped, redirected, or sent at a delayed pace, the network will experience serviceability issues in the specific location of the attack. An illustration of a Black Hole attack is provided in Figure 2.

3) ***Jamming:*** The Jamming attack is another attack on availability that strives to cut off communication in vehicular networks. Much of the communication in these networks relies on Dedicated Short-Range Communication (DSRC), utilizing radio signals. In a Jamming attack, a malicious actor uses a jammer to disrupt the communication signals between nodes on the network. As a result, packets that are sent over the channel are not received [10]. Since this halts communication between nodes, it inevitably causes serviceability issues. It can be very difficult to prevent attackers from entering the range of a vehicular network with a jammer because these networks are spread out over a large geographic area. Because of this, jamming attacks can be very difficult to protect networks against.

B. Authenticity

Attacks that involve falsifying or modifying credentials to access or alter the network will be referenced as attacks on authenticity. In this section, we discuss two such attacks.

1) ***Sybil:*** The Sybil attack is an authenticity attack in which an attacker creates several false nodes on the network. Functioning nodes on these networks will regularly broadcast identifying information, to inform other nodes of their identities and locations. In a Sybil attack, a malicious node will claim several identities, broadcasting multiple different identities and false locations [11]. As a result, surrounding legitimate nodes will believe that these false nodes exist, and will attempt to communicate with them. Since each of these false nodes can be manipulated by that single malicious node, they can easily be used to perform other attacks on a much larger scale. By creating and controlling several nodes on the network, an attacker can more efficiently disrupt regular operations. An illustration of a Sybil attack is shown in Figure 3.

2) ***Masquerading:*** The Masquerading attack is like the Sybil attack. Instead of creating false nodes, it involves altering a malicious node's identity to appear legitimate. If a malicious node cannot interact with the network, because of being unregistered or even blacklisted from the network's database, an attacker can attempt to circumvent this problem by masquerading as a legitimate node [12]. Any privileges or resources that legitimate nodes can access are now accessible by the attacker. As with the Sybil attack, the Masquerading attack is an avenue for attackers to execute other types of attacks. This simply gives them access to the network by posing as a legitimate node, thereby undermining the network's ability to authenticate users.

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

C. Confidentiality

The property of confidentiality within the network ensures that regular users cannot access sensitive data. Much of this data should only be visible to authorized parties. Therefore, attacks on confidentiality will be classified as attacks that involve accessing this restricted data with the intent to harm the network. In this section, we discuss one cyber attack that affects confidentiality.

*1) **Eavesdropping**:* The Eavesdropping attack aims to find sensitive data, allowing malicious users to potentially execute another type of attack with the information they gain. In an Eavesdropping attack, the attacker steals confidential data about the network. This may include users' identities, pseudonyms, location data, routes, and other information that should normally be inaccessible to regular users. In [13], a real-world scenario is simulated, where an attacker uses the Eavesdropping attack to find valid identification signatures from regular nodes on the network. If an attacker knows the identities of surrounding legitimate nodes, they may use them to launch a Masquerading attack. They may also passively gather this data before performing a direct attack, to learn more about the network. Attacks on confidentiality are not often harmful themselves, since much of the data transferred over a vehicular network is not necessarily sensitive. However, the information gained from these attacks can offer a starting point for other types of attacks that do more direct damage to the network.

D. Data Integrity

Attacks that use falsified, expired, or generally inaccurate data to confuse the network will be referenced as attacks on data integrity. In this section, we discuss two such attacks.

*1) **Replay**:* The Replay attack aims to confuse the network by re-transmitting old messages, confusing legitimate nodes with outdated information. In a Replay attack, the malicious node receives regular broadcasts from surrounding nodes with information including location data, traffic flow data, incident reports, and more. The attacker will capture one of these regular broadcasts, then inject it back into the network after some amount of time has passed. Surrounding legitimate nodes will believe that this is a regular broadcast message and will act upon this outdated information [14]. For instance, if a regular node accelerates, it will send out a broadcast to surrounding nodes to accelerate as well as to match the flow of traffic. If a malicious node captures this packet and re-sends it after a delay, surrounding nodes will believe it is safe to accelerate. However, since the message is outdated, traffic conditions may no longer be the same, and acceleration may result in an accident. By using old messages to confuse the network, attackers can cause regular nodes to act on unreliable information.

*2) **Man-in-the-Middle (MITM)**:* The MITM attack is another attack that threatens data integrity, as it can be used to modify, delay, or completely drop messages sent by legitimate nodes. In a MITM attack, a legitimate node passes information to a malicious node, believing that it will forward the message to surrounding nodes, or a specific destination. After intercepting the message, the malicious node can do multiple things. If the node chooses to delay or drop the message entirely, this behavior can be classified under the Replay or Black Hole attacks respectively. However, if the node chooses to alter specific fields of the message, this directly affects the integrity of the data. As [15] explains, an active MITM attack may involve altering the transmission time, sender location, or actual message data of an intercepted broadcast. A message warning nearby nodes of a sudden steep curve may be altered to instead tell nearby nodes to accelerate. This data alteration is a clear security concern of vehicular networks. An illustration of a MITM attack is shown in Figure 4.

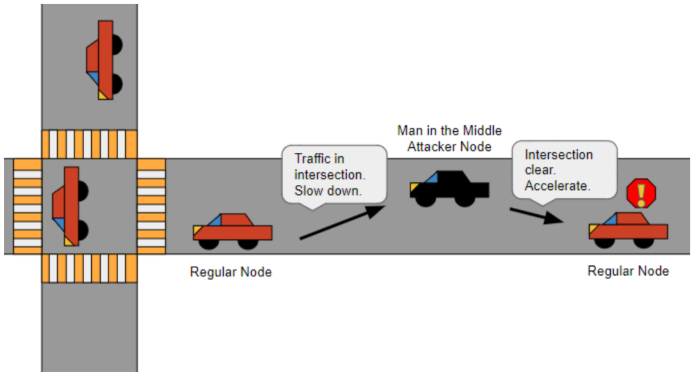

Fig. 4: Illustration of Man in the Middle Attack

E. Non-Repudiation

The property of Non-Repudiation within vehicular networks prevents users from denying their actions within the network. This could include regular traffic incidents where the driver denies being at fault or scenarios where malicious users deny their involvement in an attack. Therefore, any attack that attempts to obscure a node's identity or its past actions will be referenced as an attack on Non-Repudiation. Preserving this property requires the network to keep track of node identities, while still preserving their privacy. In this section, we discuss the Repudiation attack.

*1) **Repudiation**:* A Repudiation attack is often executed because of an attack on Authenticity. Since these attacks involve obscuring the identity of the malicious node, using a fabricated or stolen ID, they will naturally allow the malicious node to deny its actions through anonymity. The property of Non-Repudiation is an important component of vehicular network security. As a result, we will consider this property as we examine proposed solutions to various types of attacks.

IV. Protection Solutions

In this section, we discuss multiple protection solutions that have been proposed for protecting VANETs from various types of cyber attacks.

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

TABLE I: Protection Solutions and Relevant Areas of Security Concern

	Availability	Confidentiality	Data Integrity	Authenticity	Non-Repudiation
Trust-based Systems	Poongodi et al. [16]	Zhang et al. [17]		Sugumar et al. [18]	
Machine Learning	Alrehan et al. [19]		Sharma et al. [20]		
Blockchain	Ghajar et al. [21]		Ghajar et al. [21]	Wang et al. [22]	Wang et al. [23]
Public Key Infrastructure		Wasef et al. [24]		Mallissery et al. [25]	

A. Trust Based Systems

Trust-based Systems customarily aim to incorporate techniques that help evaluate node reputation and node trustworthiness in a VANET to prevent attacks.

1) ***Node Reputation****:* One proposed method for preventing availability attacks involves a Trust-based system. Nodes can verify the validity of their neighbors by sending packets through them and checking if those packets reached their destination. If a node discovers that its neighbor regularly drops or spams packets, it will update that node's reputation score, and report this to the nearest RSU. By updating the malicious node's reputation score, all vehicles will recognize this node as inoperable, and cease communication with it. To achieve this, each vehicle stores a table containing nearby nodes and their reputation scores. In addition, a Watchdog system is put in place to examine packets after reception [26]. Since each vehicle on the network is periodically altering the reputation scores of its neighbors, the system will experience higher end-to-end delays. The more dynamic and fast-paced the network is, the higher these delays will likely be since nodes will constantly be encountering new neighbors to test.

2) ***Node Trustworthiness****:* Another important consideration of Trust-based systems is an evaluation algorithm, which determines node trustworthiness. There are several ways in which an attacker can attempt to outsmart these algorithms. These allow the attacker to gain an unfair score of trustworthiness and continue having access to the network. These include ballot stuffing, where several nodes collude to raise each other's reputation scores, and badmouth, where these nodes instead focus on lowering the scores of legitimate nodes [27]. Due to these factors, evaluation algorithms must constantly evolve, considering new exploits. One way that Trust-based systems can become more secure is with the use of Certificate Authorities, which authenticate vehicles on the network by managing identities and cryptographic keys [18]. Another way Trust-based systems become more secure is with the calculation of direct and indirect trust. As proposed in one framework, an observer node calculates direct trust for a nearby vehicle, using only its observations. Then, the observer calculates indirect trust, using other nearby nodes' observations of the vehicle in question [28]. This way, one observer node does not have full control over determining if a node is trustworthy or not.

B. Machine Learning

Machine learning approaches that include both supervised and unsupervised learning have been investigated to protect VANETs from cyber threats.

1) ***Supervised Learning****:* There are several applications for machine learning in VANET security. One study analyzes the effectiveness of 5 different ML techniques against 5 different attack types. It finds that the Naive Bayes, decision tree, and random forest techniques are most effective against constant attacks, while the decision tree is best for constant offset attacks. For random, random offset, and eventual attacks, the random forest technique remains most effective for all three [29]. As a result, successful algorithms must employ a combination of techniques. One proposed approach attempts to combat location falsification, an attack on data integrity using multiple supervised learning algorithms. While many strategies detect malicious behavior using basic safety messages (BSMs) from surrounding nodes, this approach highlights the significance of using information from multiple successive BSMs to more accurately spot attacks [20]. This approach also removes the detection workload from individual OBUs, instead employing a detection framework at the RSU level. Since RSUs have more computational power and resources, they can run complex algorithms at a faster rate.

2) ***Unsupervised Learning****:* Another application of machine learning is preventing availability attacks, particularly proposed in the case of Jamming attacks. This proposed approach uses an unsupervised learning technique, the K-means algorithm, to detect jamming attacks. This approach successfully differentiates between general, benign interference, and intentional jamming attacks [30]. The use of unsupervised learning techniques is critical, as the algorithm must make inferences about data, rather than having prior knowledge as with supervised learning algorithms. The K-means clustering algorithm is particularly useful in this scenario, as it handles large data sets well despite its limitations in handling data of varying types [31].

C. Blockchain

Blockchain technology is another researched field that has shown promise for the protection of privacy, administering transparency, and enforcing trust management in the VANET environment.

1) ***Transparency and Trust Management****:* Blockchain is another highly versatile technology that can be applied to VANETs. Two properties of this technology, particularly, contribute to the non-repudiation facet of these networks. Blockchain allows for transparency on the network and provides a reliable database of past communications. All nodes on the network keep the same ledger of events, as recorded

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

by the blockchain database [23]. This effectively holds nodes accountable for their actions, eliminating any possibility of denial or repudiation. In addition, one proposed solution to malicious behavior is the use of blockchain for trust management. In this system RSUs collectively manage the blockchain, updating vehicle reliability values and communicating them in this way [21]. This trust management system can be used to combat data integrity and availability attacks, as it detects "bad behavior" to cut malicious nodes off from the rest of the network.

*2) **Authentication and Privacy**:* Due to the transparent nature of blockchain, privacy is a major concern. One proposed scheme specifies that only "dummy identities" or pseudonyms will be available to view on the public blockchain ledger. Both OBUs and RSUs will not have access to real IDs, only the Trusted Authority will look at these in the case of disputes [32]. As a result, this blockchain authentication scheme can effectively combat authentication attacks while preserving both trust and privacy.

D. Public Key Infrastructure

Public Key Infrastructures have been investigated in literature as a method to protect VANETs as they provide facilities such as certificates for authentication, encrypted communications, and reduction of operational overhead.

*1) **Certificate Authentication**:* By implementing a public key infrastructure, many authenticity attacks can be avoided, including the Sybil attack. As discussed in [33], a trusted party distributes certificates to all nodes within the network. Without a valid certificate, a node is unable to communicate with the network. False nodes created in a Sybil attack will not be recognized, because they do not have valid certificates. To ensure the security of this method, certificates must be changed periodically. If a node is deemed to be malicious, it will be placed on the trusted authority's Certificate Revocation List, which is broadcasted to nodes on the network. In this way, nodes are informed of certificates that are no longer valid and should not be communicated with.

*2) **Encrypted Communication**:* Using a public key infrastructure to prevent authentication attacks leaves some issues to be addressed. Wasef et. al address some of these, including location privacy [24]. To ensure location privacy, random encryption periods can be employed. Whenever a vehicle changes to a new certificate, an encrypted communication zone is created with surrounding nodes that have valid certificates. Once the vehicle confirms that revoked nodes cannot intercept messages, it switches certificates. This system appears to effectively confuse attackers by adding ambiguity to the process, preventing them from tracking vehicles across certificate changes.

*3) **Overhead Reduction**:* Another potential problem with public key infrastructures lies in overhead. Each time a node communicates with others, it must check the central authority's Certificate Revocation List (CRL) to ensure that these other nodes are still valid. This adds additional delay to the network. One proposed method utilizes Short Time Certificate Management and the Merkle Signature Scheme to negate this additional overhead. In this system, CRLs are distributed only to RSUs, rather than each vehicle node. Then, the RSUs issue each vehicle in range an SCM packet. This way, vehicles do not need to consult the CRL to find revoked nodes. Only valid nodes will have an SCM packet [25]. This method also increases the level of security, since short-term certificates are more dynamic, and therefore harder for malicious actors to exploit.

In this section, we illustrated various tools that have been investigated for protecting VANETs against various cyber attacks and the areas of security concern that they affect. An overview of this study is provided in Table I. Here, we observe that Trust-based Systems have been effective at addressing attacks that compromise VANET Availability, Confidentiality, and Authenticity. Correspondingly, Machine Learning solutions have helped address challenges associated with VANET Availability and Data Integrity. Blockchain technology has shown promising signs in addressing VANET Availability, Data Integrity, and Authenticity. Finally, Public Key Infrastructure mechanisms have assured risks that compromise VANET confidentiality and authenticity.

V. Open Research Challenges

As seen in the previous section, the proposed protection solutions for VANETs are comprehensive enough to cover all areas of security concern. However, as these mechanisms are starting to grow, cyber attackers are becoming more shrewd and can develop new methods to circumvent these protection solutions. Additionally, since these four technologies are constantly evolving in their applications to VANETs, certain areas can be investigated to provide more rigorous protection. In this section, we identify some open research areas that can be investigated to provide more robust security for VANETs against cyber attacks.

A. Improvement of Machine Learning Approaches

In the realm of machine learning, many of the algorithms that have been applied to VANET have shortcomings. The previously discussed Naive Bayes algorithm is highly efficient and scale-able, making it a prime candidate for the highly dynamic vehicular network. However, other algorithms such as DBSCAN and SVM handle outliers far better than Bayes, despite falling behind in flexibility [34]. Computational overhead also remains a potential problem for these systems. In a simulation, these algorithms are generally trained with smaller data sets than those that would be observed in a real-life scenario [35]. Analysis of larger, more complex sets of data may be difficult when these systems rely on RSUs, or even OBUs to do the computations. Both have limited resources and must operate at a very fast pace due to the dynamic nature of vehicular networks. Larger data sets are required for training, to ensure that machine learning algorithms geared toward these networks can scale appropriately.

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

B. Long-term Trust Information and Ensemble Protection Solutions

The central facet of Trust-based systems is that nodes can gauge the trustworthiness of nearby nodes with accuracy and efficiency. There are many considerations in this process, one of which is trust decay. It is often assumed that when a node first encounters another node, its trust value starts at a default level. However, nodes may be able to do more efficiently calculate trust if they are given access to "long-time" or historic trust values for nearby nodes. This way, past behaviors from before this encounter can play a role in the node's trust calculations. This presents problems of its own, primarily because RSUs and OBUs cannot store this "long-term" trust information indefinitely, for lack of space [36]. As a result, more research can help determine what is the optimal time that long-term trust information should be stored before it becomes too burdensome on the network.

It is also worth noting that Trust-based systems are inherently based on uncertainty. To continue developing optimal systems, several proposed solutions have combined this technology with blockchain and machine learning techniques, for more comprehensive systems.

C. Prioritizing Privacy Preservation

As mentioned earlier, a primary concern of blockchain applications in vehicular networks is privacy. As blockchain serves as a ledger for all transactions, privacy would be non-existent without the application of a pseudonym system or something similar. However, a simple pseudonym scheme can easily be cracked by a malicious actor. For this reason, blockchain systems must be designed with privacy preservation in mind. However, blockchain is already a very resource-heavy system due to the number of transactions occurring on the block [37]. As a result, the high computational cost of maintaining complex encryption or authentication schemes alongside the existing cost of maintaining the blockchain itself may be too much for the network to bear. These systems must be further developed to balance out the cost, in terms of both time and resources, so that privacy-preserving blockchain can scale in a real-world scenario.

VI. Conclusion

In this paper, we provide a survey on cyber attacks and protection solutions for VANETs. We begin by addressing the various types of cyber attacks that can affect VANETs and their respective security concern that they can compromise. Following, we illustrate multiple protection solutions that have been proposed in the literature in response to these attacks, and the various security concerns they can help alleviate. We finish off by introducing some open research areas that can help further address the cyber threats and can assist in creating more robust protective strategies and security solutions to protect the next generation of VANETs.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. IIS-2150394. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] "Road traffic injuries," Jun 2022. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[2] L. Nkenyereye, L. Nkenyereye, S. M. R. Islam, Y.-H. Choi, M. Bilal, and J.-W. Jang, "Software-defined network-based vehicular networks: A position paper on their modeling and implementation," *Sensors*, vol. 19, no. 17, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/17/3788

[3] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[4] R. A. Uzcategui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Communications Magazine*, vol. 47, no. 5, pp. 126–133, 2009.

[5] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of dsrc and cellular network technologies for v2x communications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457–9470, 2016.

[6] H. Meng, K. Zheng, P. Chatzimisios, H. Zhao, and L. Ma, "A utility-based resource allocation scheme in cloud-assisted vehicular network architecture," in *2015 IEEE International Conference on Communication Workshop (ICCW)*, 2015, pp. 1833–1838.

[7] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Network*, vol. 27, no. 5, pp. 48–55, 2013.

[8] H. Hasbullah, I. A. Soomro, and J. lail Ab Manan, "Denial of service (dos) attack and its possible solutions in vanet," *International Journal of Electronics and Communication Engineering*, vol. 4, no. 5, pp. 813 – 817, 2010. [Online]. Available: https://publications.waset.org/vol/41

[9] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J.-T. Seo, "An efficient dynamic solution for the detection and prevention of black hole attack in vanets," *Sensors*, vol. 22, no. 5, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/5/1897

[10] G. Kaur, "Technique to detect and isolate jamming attack in vanet," 2017.

[11] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting sybil attacks in vanets," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0743731513000191

[12] Hezam Al Junaid, Mohammed Ali, Syed, A.A., Mohd Warip, Mohd Nazri, Fazira Ku Azir, Ku Nurul, and Romli, Nurul Hidayah, "Classification of security attacks in vanet: A review of requirements and perspectives," *MATEC Web of Conferences*, vol. 150, p. 06038, 2018. [Online]. Available: https://doi.org/10.1051/matecconf/201815006038

[13] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[14] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets)," in *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)*, 2020, pp. 394–398.

[15] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/11/4040

[16] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, "Ddos detection mechanism using trust-based evaluation system in vanet," *IEEE Access*, vol. 7, pp. 183 532–183 544, 2019.

[17] C. Zhang, L. Zhu, C. Xu, K. Sharif, K. Ding, X. Liu, X. Du, and M. Guizani, "Tppr: A trust-based and privacy-preserving platoon recommendation scheme in vanet," *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 806–818, 2022.

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.

[18] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (vanet) - wireless networks," Jul 2016. [Online]. Available: https://link.springer.com/article/10.1007/s11276-016-1336-6citeas

[19] A. M. Alrehan and F. A. Alhaidari, "Machine learning techniques to detect ddos attacks on vanet system: A survey," in *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, 2019, pp. 1–6.

[20] A. Sharma and A. Jaekel, "Machine learning based misbehaviour detection in vanet using consecutive bsm approach," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1–14, 2022.

[21] F. Ghovanlooy Ghajar, J. Salimi Sratakhti, and A. Sikora, "Sbtms: Scalable blockchain trust management system for vanet," *Applied Sciences*, vol. 11, no. 24, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/24/11947

[22] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-tsca: Blockchain assisted trustworthiness scalable computation for v2i authentication in vanets," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1386–1396, 2021.

[23] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: Applications of blockchain in the internet of vehicles - eurasip journal on wireless communications and networking," Apr 2021. [Online]. Available: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-021-01958-8

[24] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 22–28, 2010.

[25] S. Mallissery, M. M. M. Pai, A. Smitha, R. M. Pai, and J. Mouzna, "Improvizmg the public key infrastructure to build trust architecture for vanet by using short-time certificate management and merkle signature scheme," in *2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, 2014, pp. 146–151.

[26] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni, "A reputation system for detection of black hole attack in vehicular networking," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015, pp. 1–5.

[27] H. Hu, R. Lu, Z. Zhang, and J. Shao, "Replace: A reliable trust-based platoon service recommendation scheme in vanet," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, 2017.

[28] K. N. Tripathi and S. C. Sharma, "A trust based model (tbm) to detect rogue nodes in vehicular ad-hoc networks (vanets) - international journal of system assurance engineering and management," Sep 2019. [Online]. Available: https://link.springer.com/article/10.1007/s13198-019-00871-0citeas

[29] A. Sonker and R. K. Gupta, "A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 3, p. 2535, 2021.

[30] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of rf communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol. 13, pp. 56–63, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221420961730222X

[31] M. Ahmed, R. Seraj, and S. M. S. Islam, "The k-means algorithm: A comprehensive survey and performance evaluation," *Electronics*, vol. 9, no. 8, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/8/1295

[32] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "Bbaas: Blockchain-based anonymous authentication scheme for providing secure communication in vanets," Feb 2021. [Online]. Available: https://www.hindawi.com/journals/scn/2021/6679882/

[33] N. Kumar, R. Iqbal, S. Misra, and J. J. Rodrigues, "An intelligent approach for building a secure decentralized public key infrastructure in vanet," *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 1042–1058, 2015, special Issue on Optimisation, Security, Privacy and Trust in E-business Systems. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0022000014001809

[34] S. Ftaimi and T. Mazri, "A comparative study of machine learning algorithms for vanet networks," in *Proceedings of the 3rd International Conference on Networking, Information Systems amp; Security*, ser. NISS2020. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3386723.3387829

[35] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," *Procedia Computer Science*, vol. 184, pp. 877–886, 2021, the 12th International Conference on Ambient Systems, Networks and Technologies (ANT) / The 4th International Conference on Emerging Data and Industry 4.0 (EDI40) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921007894

[36] R. Hussain, J. Lee, and S. Zeadally, "Trust in vanet: A survey of current solutions and future research opportunities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553–2571, 2021.

[37] J. Grover, "Security of vehicular ad hoc networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, p. 100458, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209622000055

Authorized licensed use limited to: UNIVERSITY OF NEVADA RENO. Downloaded on February 21,2024 at 17:17:06 UTC from IEEE Xplore. Restrictions apply.