Detection Mechanism on Vehicular Adhoc Networks (VANETs) A Comprehensive Survey

Shobana Gopalakrishnan[1] **and Dr.Arockia Xavier Annie R.**[2]
[1] Assistant Professor, DIT, Loyola ICAM College of Engineering and Technology,
[2] Assistant Professor, DCSE, Anna University

Abstract—VANET is an upcoming technology with an encouraging prospect as well as great challenges, specifically in its security. This paper intends to survey such probable attacks and the correlating detection mechanisms that are introduced in the literature. Accordingly, administering security and protecting the owner's privacy has become a primary argument in VANETs. To furnish stronger security and preserve privacy, one should recognize the various probable attacks on the network and the essence of their behavior. This paper presents a comprehensive survey on diversified attacks and the recommended unfolding by the various researchers which concentrate on security services and the corresponding countermeasures to make VANET communications more secure.

Key words: *VANET, Attacker model, attacks, Sybil attacks, attackers, security requirements.*

1. INTRODUCTION

A vehicular ad-hoc network is a distinct type of Mobile Adhoc Network (MANET) that furnish dissemination between neighboring vehicles and roadside equipment. The connectedness in Vehicular Ad-Hoc Network (VANETs) can be classified into vehicle-to-vehicle (V2V) communications and Vehicle-to-Infrastructure (V2I) communications in accord to succeeding situations of VANETs [15]. Dedicated short-range communication (DSRC) radio and a few IEEE standards such as IEEE 802.11p standards can be adopted for V2V and V2I communications in VANETs. The DSRC standard, wireless access in the vehicle environment (WAVE), which employs the IEEE 802.11p standard for remote conformity [14]. So, every vehicle has traffic-related messages after some time (100-300 milliseconds) and disseminate to various vehicles or RSU. The architecture of vehicular ad hoc networks comprises several hardware and software components. In a VANET network, vehicles are implemented with a unit called OBU (On-Board Unit), mounted in the vehicle [16]. On roads, units of framework communication are called RSU (Road-Side Unit). TA is a third party that is handled by the RSU and OBU, also authoritative for regulating and administering the whole network [16]. All vehicles are propelling freely on the road network and interacting with each other or with RSUs and definitive authorities. VANETs are one of the affirming approaches to carry out Intelligent Transportation Systems (ITS). The significant attributes of VANETs, such as dynamic network topology, high mobility, and expected node movements, need new algorithms and protocols to be evolved precisely to this recent environment. Typical VANET applications consist of route changing, collision avoidance, warning about dangerous road conditions, post-crash warnings, etc[17][18][19]. VANET users make use of several applications that are categorized into infotainment, active road safety, traffic efficiency, and management. The objective of VANETs is to grant communication between vehicles [18]. The occurrence of being free from any sort of threat or uncertainty in the course of communication is described as security. It means safety or any countermeasures captured for being intact or secured. In vehicular ad-hoc networks, it is necessary to preserve the network against malignant activity to guard the security architecture. This is because the wireless connection is normally quite crucial to secure. The security and its assured level of implementation are essential for people's safety. However, exclusive features of VANETs make security, privacy, and trust management challenging controversies in VANETs' design. Considerable exemplary surveys have been carried out in recent years, which all enclose the background of VANETs such as the requirements, challenges, various types of threats, and correlating solutions [20][21].

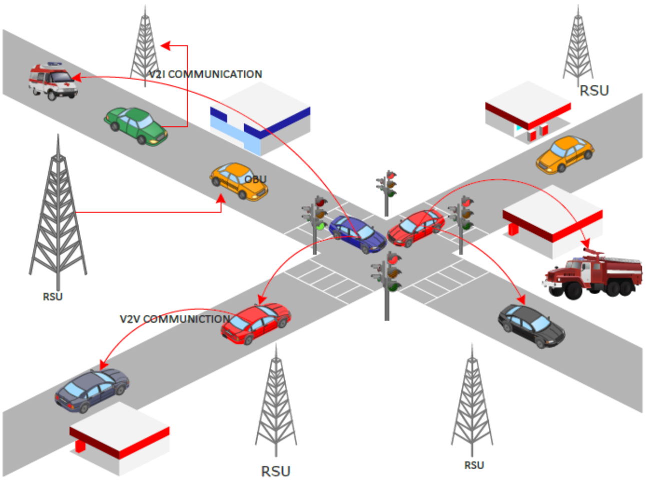

Fig 1. VANET System

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.38

As all communication is organized over a distributed broadcast channel and through the periodical transfer of beacon packets, an attacker can claim multiple identities without being detected. In an unsecured network like VANET, the identities of nodes can conveniently be contravened by malicious nodes, which presents a fortuity for a Sybil attack [22]. In a Sybil attack, an attacker falsifies its identity to masquerade as another node. In such a locale, an attacker can devise multiple identities either by forging, stealing, or by employing any other means [23]. Attackers can establish a hallucination of a non-existent event by disseminating fraudulent messages using some or all of these identities at the aforementioned time [23]. This attack is a source motivation of all other forms of attacks in VANET.

2. Related work

The major impetus that led us to accomplish this work is to contribute in the same paper a novel essence about VANET state of art and a study about VANETs detection mechanisms and their feasible associated cryptographic solutions. Existing methodical literature reviews devote straightforward and pervasive glance of unrestricted research overseen to delve into the problems and elucidations. Pengwenlong et.al evaluate the similarity of vehicle driving patterns, using SVM classifiers to distinguish the malicious nodes from the benign ones [13]. Lu et.al only targets the privacy and authentication specifications for the scrutiny of the security schemes urged so far [25]. Rida Khatoun et.al represent vehicle driving patterns by using eigenvalues of their driving pattern matrix and the classification procedure based on kNN classifiers [13]. Elvin Eziama et al. proposes the Bayesian Neural Network (BNN) model framework for high-performance prediction, classification accuracy, and low detection latency, in trust computation in VANETs [11], when compared with NN, in the presence of uncertainty in the information. In the survey article from Avleen Kaur Malhi et.al, discusses and reviews eminent safety solutions to address the security aspects for VANETs [15]. The RSSI-based localization algorithm is designed both for detecting Sybil attacks and providing the location of any vehicle is discussed in [10] Mevlut Turker Garip et al. However, none of the preceding works fixate completely on all the detection mechanisms of the Sybil attack in vehicular networks giving an exhaustive depiction of the security of the vehicular networks. Moreover, none of the previous works fixate on the classification of security mechanisms based on their cryptography mechanism. This paper has done a relative inquiry of disparate cryptography schemes and their efficacy for VANET.

3. VANET Attacker model

The distribution of a security system for VANET is confronting. In fact, the exceptionally dynamic nature with recurrent disconnection, spontaneous arrivals, and departures of vehicles, the management of wireless channels to swap emergency and safety messages, bring to light VANETs to diversify threats and attacks. Accorded the diversification of VANETs possible threats and attacks, and in the significance of precision and adaptation, it is indispensable to organize them [23]. In this section, we will organize the attacks, the attackers, and inspect which VANET communication tone they influence.

3.1 Attacks in VANETs

The researchers in papers like [36] explored several attacks in VANETs. The analysis of these attacks is essential and effective because the essence of VANET delivers vulnerabilities and restraints that require explanation [33][36].

The classification of attacks is given below:

1. Identity and geographical position revealing (Location Tracking): an attacker tries to get information about the driver and track him. This discloses a certain node at risk.
2. Denial of Service (DoS) attacks: In Denial-of-Service attacks, an attacker attempts to make the resources and the services inaccessible to the users in the network. It is done by obstructing the physical channel. It actually targets the availability of network services, which can have deliberate aftermath notably for VANETs applications.
3. Sybil Attack: an attacker devises multiple vehicles on the road with look-alike identity. It contributes deception to other vehicles by relaying some wrong messages for the benefits of this attacker.
4. Malware: In this attack, an attacker sends spam messages in the network to exhaust the network bandwidth and reinforce the transmission latency. It is crucial to oversee this kind of attack, due to the shortfall of fundamental infrastructure and centralized administration. The attacker disperses spam messages to a group of users. These messages are of no concern for the users and are treated as an ordinary advertisement message.
5. Spam attack: An insider node disseminates spam messages to intensify transmission, latency, and bandwidth consumption.
6. Man in the Middle Attack: a malicious node listens to the communication established between two other vehicles. It impersonates to be each one of them to reply to the other. It injects false information between them.

7. Brute force attack: It is a trial-and-error method where an attacker uses to retrieve information like a user password or personal identification number or to crash encrypted data, or to test network security.
8. Blackhole attack: It is a type of denial-of-service attack where a malicious node advertises the shortest path to get the data, routes and diverts them. The malicious node is able to deflect the data packet or preserve it. When the falsified route is strongly established, it depends on the malicious node whether to drain or onward the packet to anywhere the attacker wants.
9. Wormhole attack: Overhearing data, an attacker secures packets at a point targeted through a shaft to another point. The attacker recapitulates it from there.
10. Greyhole attack: a malicious node entices the network by granting to forward the packets. But at intervals, the attacker leaks them for a moment and then converts to his routine practice.
11. GPS spoofing and tunneling attack: hidden vehicles engender distorted positions that cause accidents.
12. Timing attack: Malicious vehicles compute some time slots to the received message, to devise delay before advancing it. Thus, nearby vehicles secure it after they actually desire, or after the point when they should receive it.
13. Replay attack: malicious or illegal users try to portray a genuine user or RSU by using formerly spawned frames in new connections.
14. Illusion attack: the adversary victimizes purposefully the sensors on his car to contribute wrong sensor readings. Therefore, erroneous traffic warning messages are broadcasted to neighbors.
15. Jamming attack: the attacker hinders with the radio frequencies adopted by VANET nodes.
16. Session Hijacking: authentication is accomplished at the creation. After that, the attackers take control of the session between nodes.
17. Repudiation: the rejection of a node in a communication.
18. Free-Riding attack: In cooperative authentication schemes, selfish vehicles may take advantage of others' authentication contributions without making their own. Such selfish behavior is called a free-riding attack that will bring about a serious threat to cooperative message authentication

The above detailed discussion of attacks has been given in numerous literatures on VANETs [23][30][32][33][34][35][36][37][38].

3.2 Attackers in VANETs

VANET attackers are one of the basic significances of the researchers in most of the research. They got many authoritative names detailed below based on their actions and targets:

I. Selfish driver: he can divert the traffic.
II. Malicious attacker: he has precise targets. He induces devastations and damages through applications in VANET.
III. Pranksters: attacker does things for his own pastime; such as DoS or message diversification (hazard warning) to cause road traffic.
IV. Greedy drivers: These attackers try to attack for their own profit. For example: sending accident

Table 1 Correlation of security attacks, attackers and security requirements in VANETs

Name of the Attack	Attacker Type	Security Requirements
Identity and geographical position revealing (Location Tracking)	Selfish driver, Greedy drivers	Data Integrity, Authentication
Denial of Service (DoS) attacks	Malicious attacker, Pranksters	Availability, Confidentiality
Sybil Attack	Selfish driver, Greedy drivers, Malicious attacker, Pranksters, Snoops/eavesdropper	Authentication, Confidentiality
Malware	Malicious attacker, Pranksters	Availability
Spam attack	Malicious attacker, Snoops/eavesdropper	Availability
Man in the Middle Attack	Selfish driver, Greedy drivers	Data Integrity, Confidentiality
Brute force attack	Greedy drivers, Selfish driver	Authentication
Blackhole attack	Selfish driver	Availability
Wormhole attack	Malicious attacker, Selfish driver	Authentication, Confidentiality
Greyhole attack	Malicious attacker, Selfish driver	Authentication,

		Confidentiality
GPS spoofing and tunneling attack	Pranksters, Snoops/eavesdropper	Authentication
Timing attack	Malicious attacker, Selfish driver	Data integrity
Replay attack	Greedy drivers, Pranksters	Data Integrity, Confidentiality
Illusion attack	Malicious attacker, Pranksters	Authentication
Jamming attack	Pranksters, Greedy drivers	Authentication
Session Hijacking	Pranksters	Authentication
Repudiation	Selfish driver	Non-Repudiation
Free-Riding attack	Selfish driver	Authentication

messages may cause congestion on-road or sending fake messages for clearing up the road.

V. Snoops/eavesdropper: attacker tries to compile information about other resources.

3. Sybil attack in VANETs

As we are dealing with the Sybil attack and its detection mechanisms, let us look at how the Sybil attack works. As per the Sybil attack, a vehicle makes a numerous vehicle character. These spurious characters urge that there are additional vehicles on the roads. The consequence of this attack is that any attack could be a serious threat after snooping on the locales or another existence of the nodes in the Sybil attack network, initially discussed by [40] Douceur et.al, because it disturbs the function of the VANETs. Gradually in this attack, an attacker advances the multiple proclamations to the other nodes in the networks. The striker simulates plentiful nodes. The other nodes are called the nodes of the network, and the nodes whose identities are confidential are called Sybil nodes. Comparatively, any of the attacks could execute on a network escorting Sybil attacks, one of the anticipations can be the deception of the traffic chaos or the accident so that the other vehicles accustom or diverge the route or fly the road in support of the attacker. The desirable risk could be the falsehood generated by the intruder as traffic congestion to invoke the user to adjust the route.

One of the possible hallucinations by Sybil Attacker is inserting erroneous information assimilating illegal nodes. Recognizing the accident on a highway, the primitive vehicle confronting the circumstances could send a warning prompt, of speed, for all the vehicles accompanying the first one. This broadcast can be disclosed to the whole group of the vehicle. This warning prompt could be deleted exploiting the Sybil vehicle that endangers the lives of traveling people.

Recognizing the specifications, the type of communications, identities, and their presence in the networks, the Sybil attacks are partitioned into three groups.

I, Transmission Group

When an authentic node disseminates a message, it might be convincing that the data is shuffled to the Sybil node, which is malignant. Furthermore, messages from the Sybil nodes are sent from malicious devices. Back and Forth communication from the Sybil nodes might be explicit or implicit. In the case of the explicit, all the malevolent nodes interact with honest nodes. Then again, in the implicit case, authentic nodes reach the Sybil nodes accompanying a malicious node.

ii. Identity Group

Sybil's adversary that generates the new identity is described as Sybil identity, which could be a nearby node's identity or stolen identity that is a 32-bit integer.

iii. Contribution Group

Concurrent attacks could be executed assimilating numerous Sybil identities falsified by the malicious node, or it can be performed sequentially. An identity can be executed on the network intermittently, but, once at a time. The number of Sybil nodes exploited by an attacker typically is equivalent to the number of physical identities or less than that. The appropriate functionality of the network could be distributed by the Sybil Attack, in which some susceptibilities can be contributed.

Concerns on Sybil Attacks:

Sybil attacks can easily affect the performance of vehicular ad-hoc networks in various aspects. Some of them are listed below.

Data Gathering

The sequence can be amended through the control of multiple identities, the malignant node could enforce the data gathering. If we determine the average number of the packets in networks, packets are shortened by the Sybil nodes which adds the total nodes in the network. As a result, network performance is remarkably lowered.

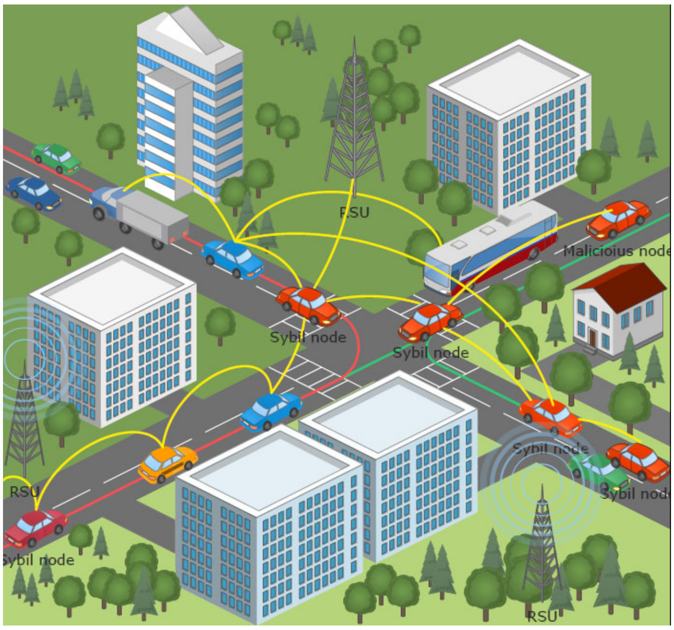

Fig 2. Sybil Attack in VANET

- Proper resource allotment

Righteousness in resource allotment may also be influenced by the Sybil nodes. When the resource allotment proceeds in the existence of the Sybil identities, the malignant nodes may secure a more enormous share among the resources. This fallout in DoS lowers the authority of the nodes as the distribution of the resources driving to the DoS attacks.

- Routing

Sybil attacks are operable against the routing protocols in the VANETs. In the multi-way routing, independent paths are exploited. The existence of the Sybil characters from a malignant node in these forms can disturb the routing path. Geo-routing is further exposed because a malignant node can exhibit up in more than one location at any accustomed instance.

- Polling

The Sybil attacks can dispatch the result of the polling plan erroneously. If the attacker makes ample Sybil nodes to take significance in resolving the inaccurate nodes, a trustworthy node and behavior can be aborted from the system.

- Discover Misbehaving nodes

An attacker can employ a system to notice a malignant node by expelling a node through the Sybil nodes. If the discovering process handles disparate viewpoints to put a malignant node, the intruder can, in any case, avoid acceptance by engaging multiple nodes on varied moments. If some of the Sybil nodes are spotted and recessed from the system for vicious behavior, the intruder takes advantage of distinct identities.

Security Requirements in VANETs

In VANETs, security is significant as VANET packets keep life-critical information and it is indispensable that these packets must attain to the drivers without any alteration or infusion of data; furthermore, the duty of drivers should also be remembered that they reveal the traffic status promptly and within time. So, VANETs must satisfy the following security requirements:

- Authentication

Authentication brings us the assurance that data is brought about by a trustworthy client. It is critical that the data which proliferates in the network must be precise and generated by a trustworthy client because, in VANETs, nodes revert according to the data authorized from the other end.

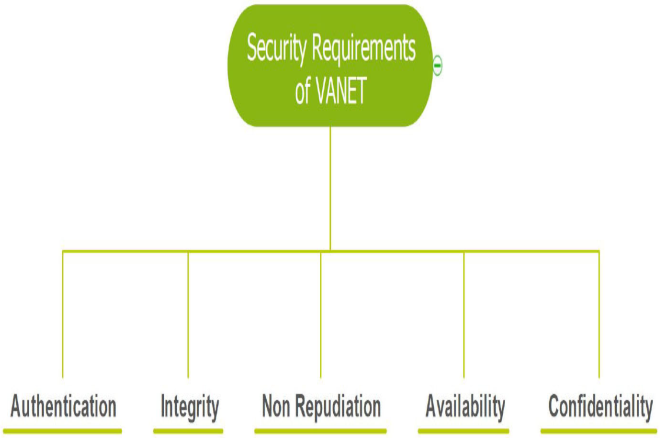

Fig 3. Security Requirements in VANETs

- Integrity

It assures that the data at the transmitter and receiver side are the same. Modification of messages is accomplished by recognized users only. The receiver takes advantage of a similar course of action as used at the transmitter side to generate another digest from the message for correlating it with the authentic message. This strategy establishes the integrity of the data. So, we should preserve all messages in opposition to modification attacks.

- Non-Repudiation

Non-Repudiation is the affirmation that someone cannot refuse the authenticity of something. This evades scams from declining their violation because in this, even if the attack occurs, non-Repudiation will facilitate the capacity to pinpoint adversaries.

- Availability

Vehicular networks require real-time inference for numerous motivations so they must be available all the time. These applications need a more rapid response from sensor networks or Ad-hoc networks, elimination of the consequence can appear or the message can become insignificant if there is any setback in seconds for disparate applications.

- Confidentiality

Every driver's privacy needs to be restricted. This security specification is to assure that data will precisely be read by authenticated users. The necessity of confidentiality is demanded in network communications, where scarcely network nodes are authorized to read such data.

4. Detection Mechanism in VANETs

In this section, we summarily review the detection mechanism used to defend against Sybil attacks in VANET. In VANET, an enormous amount of data should be handled rapidly from each node. To examine any malicious activity in that massive data and process them with the merest time, certain detection techniques have been enforced to deal with the issues in the VANET environment.

Existing detection mechanisms of Vehicular Adhoc Networks (VANETs) can be organized into the following classification.

Shan Chang et.al [1] proposes a novel Sybil attack detection mechanism called Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. Footprint integrates three elegant techniques like infrastructure construction, location-hidden trajectory generation, and Sybil attack detection. The vehicle is allowed to request multiple authorized messages from an RSU using different temporary key pairs.

Bo Yua et.al [2] introduces a cooperative method to authenticate the location of potential Sybil nodes. They handle a Random Sample Consensus (RANSAC) based algorithm to compose this cooperative method more vigorously against outlier data constructed by Sybil nodes. They recommend a statistical method Presence Evidence System (PES) and devise a system that is able to authenticate where a vehicle comes from. It evaluates a node's location by interpreting its signal strength distribution and then finds out whether its location state is persistent with the predicted location.

Kenza Mekliche et.al [3] proposes an approach that uses infrastructures and localization of nodes to detect Sybil attacks. L-P2DSA is an infrastructure-based scheme where vehicles are assigned a pool of pseudonyms. These pseudonyms are hashed to a prevalent value to restrict the vehicles from using them to bombard a Sybil attack. The prospective scheme goes through three steps, the 1st is the initialization step, the 2nd is the detection step in RSU, the 3rd and last step is the verification step.

Rakesh Shrestha et.al [4] presents a lightweight solution for Sybil attacks based on received signal strength. It is used by autonomous vehicles without using a centralized trusted third party and added hardware like GPS. They present a simple scheme that utilizes the received signal strength to differentiate the legitimate nodes from Sybil nodes without calculating the position of the Sybil nodes. The Sybil attack is detected by identifying if two different signal streams come from the same node or not. They calculate the distance between the received signal strength vectors of two onboard units (OBUs) to find a similarity between them. It identifies the distinct OBUs with similar signal strength as OBUs participating in a Sybil attack. They detect the Sybil attack by comparing the distance between two different signal vectors with the threshold.

Khaled Rabieh et.al [5] prefer a cross-layer scheme to facilitate the RSUs to determine Sybil vehicles. The challenge packet is dispatched to the vehicle's guarded location using a directional antenna to perceive the presence of a vehicle with a beamforming technique. The cross-layer design is achieved by constructing the challenge packet at the MAC layer and leading the PHY layer to forward it to a distinct location. The hash function and public-key cryptography are adopted to protect the challenge and response packets. Sybil attack detection is classified into three stages termed alarming, verification, and decision. The challenge packet generates a random number that is one time generated and the vehicle's pseudonym, all encrypted by the vehicle's public key.

D. Srinivas Reddy et.al [6] put forward a Cryptographic digital signature certificate method to establish trust between participating entities. Every mobility vehicle in VANET is assigned with a set of Public/Private Key pairs by which the vehicle is authenticated itself to receivers by digitally signing the messages. The asymmetric cryptographic technique is used to combine digital signatures. The verification procedure is established on a local certificate session key. Using the hash function and XOR operation this technique also verifies the verification time of vehicle ID.

Pengwenlong Gu et.al [13] proposes three SVM kernel functions-based classifiers to discriminate the malignant nodes from benevolent ones by assessing the divergence in their Driving Pattern Matrices (DPMs). The proposed security services are based on three major mechanisms: Encryption algorithms, Public Key Infrastructure (PKI), and Pseudonymous. They evaluate vehicle driving patterns in neighborhood road traffic situations and consider the possibility to detect Sybil attacks based on the variation of their driving patterns. The main intention is to estimate the resemblance of vehicle driving patterns, then use SVM classifiers to recognize the malicious nodes from the benign ones.

Chunhua Zhang et.al [7] launch a misbehavior detection mechanism based on a support vector machine (SVM) and Dempster Shafer theory (DST) of evidence to thwart false message attack and message suppression attack. The proposed mechanism includes the data trust model and vehicle trust model. They propose a data trust model using an SVM-based classifier, which can effectively determine the authenticity of the alert message based on message content and vehicle attributes. The local vehicle trust module is presented by using another SVM-based classifier, which explores the behavior of the vehicle in terms of message propagation to determine whether the vehicle is trustworthy and submits the trust report to the TA.

Celestine Iwendi et.al [8] offers a novel biologically inspired spider-monkey time synchronization technique for large-scale VANETs to hike packet delivery time synchronization at reduced energy consumption. The urged procedure is based on the metaheuristic stimulated framework perspective by natural spider-monkey behavior. They introduce the pseudocode algorithm randomly assigned for energy-efficient time synchronization in a two-way packet delivery sequence to assess the clock offset and the propagation delay in transmitting the packet beacon message to destination vehicles correctly.

Mohamed Baza et.al [9] brings forward a notion where each roadside unit (RSU) publishes a signed time stamped tag as proof for the vehicle's anonymous location. The Proofs relayed from multiple successive RSUs are adopted to discover vehicle trajectory which is used as vehicle anonymous identity. Immediately after acquiring the proof of location from an RSU, the vehicle should determine a computational puzzle by running a proof of work (PoW) algorithm. The use of PoW can prohibit the vehicles from setting up multiple trajectories in case of low-dense RSUs.
Mevlut Turker Garip et.al [10] proposes an algorithm called INTERLOC which is an RSSI-based localization algorithm that is devised both for exposing Sybil attacks and contributing to the position of any vehicle. It dynamically picks up the new interference levels and accustoms itself. It does not bank on the existence of RSUs or any other stationary roadside infrastructure for localization. INTERLOC takes the heterogeneity of interference levels into interpretation for localization. INTERLOC uses the evaluated localization areas to detect progressive Sybil attacks. INTERLOC gets eliminated false positives by predicting the smallest area that exactly incorporates the vehicle being localized even with all the GPS fluctuations.
Elvin Eziama et.al [11] proposes the Bayesian Neural Network (BNN) model framework for high-performance prediction, classification accuracy, and low detection latency in trust computation in VANETs when compared with NN, in the presence of uncertainty in the information. BNN maintains this high performance over NN in node's analysis, by providing a strong distribution and inclusion of uncertainty on the weights in the network. The Bayesian phase of the model will enhance the model selection by inferring the optimal number of components (feature extraction/feature selection). The model selection attribute will extract the different features of different attackers. The main goal of BNN is to uncover the full posterior distribution over the entire network weights.

Yuan Yao et.al [12] proposes a Sybil attack detection method based on the Received Signal Strength Indicator (RSSI), Voiceprint, to conduct a lightweight and full-distributed detection for VANETs. Voiceprint endorses the RSSI time series as vehicular speech and studies the resemblance among all received series. It does not depend on any predefined radio propagation model and oversees independent detection without the backing of the centralized node. It detects a Sybil attack by measuring the similarity between two RSSI time series. Dynamic Time Warping (DTW) is used to find the distance which adopts a dynamic programming technique to determine the best matching between two-time series by warping the series in the temporal domain.

Conclusion

Vehicular Adhoc Networks (VANETs) are attaining a reputation in transportation systems as they expedite traffic management, extend road safety, and equip approach to the Internet on highways; likewise, disseminate safety information to passengers as well as drivers. This paper brings out many things that set VANETs apart from other fields of study. Whether it be their unique characteristics, the unique services they can provide, or the challenges that are faced by this sort of system, there are many aspects of this tract that cause it to be worth inspecting in its own right. By investigating these, this paper put forward the advantages of research in VANET systems and motivates prospective study in the field.

Numerous security applications can adequately reinforce the security essentials, for example, traffic reports and incidents warning. VANETs application has the prospect to meet such security requirements. Nevertheless, emergency messages must be transferred from hub to hub in the VANETs environment in a dependable and encouraging way. To perform this, secure correspondence and system receptiveness must be earned in the VANETs environment. In this paper, we have examined the different types of attacks that might be administered to VANETs. We spotted that network accessibility has been reasonably disturbed on account of multiple attacks, where the attacks have persuaded the most intense reaction by making the system down.

In another aspect, and because of an attack, trust in the system may not be established if the presence of the dominant data is modified by the attackers before transmitted to the beneficiary. Therefore, it is demanding to keep up system availability and to build trust in the VANETs environment, all together, for the safety applications to be supportive and fortunate to the road users. Thus, devising secured communication protocols for VANETs to safeguard user-profiles and private data from malignant vehicles should be given the greatest precedence in this area of research. In this paper, the intention was to furnish a comprehensive perspective to earlier works on intrusion/misbehavior detection in VANETs. Essentially, this survey has presented an analysis of the attacks, combined with their desirable consequences along with functioning principles.

References

[1] Shan C, Yong Qi, Hongzi Zhu,Jizhong Zhao,and Xuemin (Sherman) Shen,”Footprint: Detecting Sybil Attacks in Urban Vehicular Networks”,, IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, June 2012.

[2] Bo Yua, Cheng-Zhong Xu, Bin Xiao, "Detecting Sybil attacks in VANETs", February 2013, J. *Parallel Distrib. Comput.* 73 (2013) 746–756

[3] Kenza Mekliche, Dept. of Computer Science, USTHB Algiers, Algeria Samira Moussaoui, Dept. of Computer Science, USTHB Algiers, Algeria, 2013, "L-P2DSA: Location-based privacy-preserving detection of Sybil attacks", *11th International Symposium on Programming and Systems (ISPS).*

[4] Rakesh Shrestha, Dept. of Information and Communication Engineering Yeungnam University, Korea, Sirojiddin Djuraev Dept. of Information and Communication Engineering Yeungnam University, Korea, Seung Yeob Nam, Dept. of Information and Communication Engineering Yeungnam University, Korea, 2014, "Sybil Attack Detection in Vehicular Network-based on Received Signal Strength", *International Conference on Connected Vehicles and Expo (ICCVE)*.

[5] Khaled Rabieh, Mohamed M. E. A. Mahmoud, Terry N. Guo, and Mohamed Younis, 2015, "Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs", *IEEE International Conference on Communications (ICC).*

[6] D. Srinivas Reddy, V. Bapuji, A. Govardhan, S S V N Sarma, “Sybil Attack Detection Technique Using Session Key Certificate in Vehicular Ad Hoc Networks”, *2017 International Conference on Algorithms, Methodology, Models, and Applications in Emerging Technologies (ICAMMAET)*, December 2017.

[7] C.Zhang, Kangqiang Chen, Xin Zeng, and Xiaoping Xue, “Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs”, Special Section On Security and Privacy for Vehicular Networks, IEEE Access, Volume 6, 2018.

[8] Celestine Iwendi, (Senior Member, IEEE), Mueen Uddin, James A. Ansere, P. Nkurunziza, J. H. Anajemba, and Ali Kashif Bashir, (Senior Member, IEEE), “On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique”, September 21, 2018, *IEEE Access.*

[9] Mohamed Baza, Mahmoud Nabil, Niclas Bewermeier, Kemal Fidany, Mohamed Mahmoud, Mohamed Abdallahz, "Detecting Sybil Attacks using Proofs of Work and Location in VANETs", *IEEE Transactions on Dependable and Secure Computing (Early Access)*, May 2020.

[10] Mevlut Turker Garip, Paul Hyungmin Kim, Peter Reiher, Mario Gerla, “INTERLOC: An Interference Aware RSSI Based Localization and Sybil Attack Detection Mechanism for Vehicular Ad Hoc Networks”, *IEEE Annual Consumer Communications & Networking Conference*, August 2017.

[11] Elvin Eziama, Kemal Tepe, Ali Balador, Kenneth Sorle Nwizege, and Luz M. S. Jaimes, "Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning", *2018 IEEE Globecom Workshops (GC Wkshps)*, February 2019.

[12] Yao Y, Xiao B, Wu G, X Liu, Z Yu, K Zhang, and X Zhou, February 2019, IEEE Transactions on Mobile Computing, "Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI”, Vol. 18, No. 2, February 2019.

[13] G Pengwenlong, Khatoun R, Youcef B, Serhrouchni A,2017, "Support Vector Machine (SVM) Based Sybil Attack Detection in Vehicular Networks", (WCNC).

[14] Y L Morgan, 2010, 1–18, International Journal of Vehicular Technology. "Managing DSRC, WAVE Standards Operations in a V2V Scenario"

[15] Avleen Kaur Malhi , Shalini Batra , Husanbir Singh Pannu,"Security of vehicular ad-hoc networks: A comprehensive survey", 2019 *Elsevier.*

[16] Sameer Sheikh and Jun Liang ,”A Comprehensive Survey on VANET Security Services in Traffic Management System Muhammad”, *Wireless Communications and Mobile Computing*, 2019, 1–23.

[17] Vishal Kumar, Shailendra Mishra, Narottam Chand, "Applications of VANETs: Present & Future", 5, 12-15, 2013, *Communications and Network.*

[18 Lee M, Atkison T," VANET Applications: Past, Present, and Future", Vehicular Communications,2020.

[19] Momina Hafeez, Rehan Ahmad, Umair Hafeez, *"International Journal of Advanced and Applied Sciences"*, 5(11) 2018, Pages: 1-15.

[20] Ram Shringar R, Manish K, Nanhay S, "Security Challenges, Issues and their Solutions for VANETs", Vol.5, No.5, September 2013, International Journal of Network Security & Its Applications (IJNSA).

[21] Yousef Al-Raba'nah, Ghassan Samara, "Security Issues in Vehicular Ad Hoc Networks (VANET): a survey", *International Journal of Sciences & Applied Research,* IJSAR, 2015; 50-55.

[22]Salam Hamdan, Amjad Hudaib and Arafat Awajan, "Detecting Sybil attacks in vehicular ad hoc networks", *International Journal of Parallel, Emergent and Distributed Systems*,2019.

[23]Chaitanya Kumar Karn and Chandra Prakash Gupta," A Survey on VANETs Security Attacks and Sybil Attack Detection", *International Journal of Sensors, Wireless Communications, and Control*, 2016, 6, 45-62.

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

[25] Lu, H. , Li., J. , 2014.Wireless Communication Mobile Computing, Privacy preserving authentication schemes for vehicular ad hoc networks: a survey.

[26] Rasheed Hussain, Heekuck Oh, On secure and privacy-aware Sybil attack detection in vehicular communications.Wireless Personal Communication, 2014,77 (4), 2649–2673

[27] J Grover, MS Gaur, V Laxmi, Open Computer Science, Multivariate verification for Sybil attack detection in VANET, 2015.

[28] Hasrouny, H. , Samhat, A.E. , Bassil, C. , Laouiti, A. , 2017a. VANet security challenges and solutions: a survey. Veh. Commun. 7, 7–20 .

[29] Mejri, M.N. , Ben-Othman, J. , Hamdi, M. , 2014a. Vehicular Communication, Survey on VANET security challenges and possible cryptographic solutions".

[30] G E Richard, Martine B, Samuel P, Alejandro Q, VANET security surveys, Computer Communications 44 (2014) 1–13

[31] A.A. Pouyan, M Alimohammadi, Sybil Attack Detection in Vehicular Networks, Computer Science and Information Technology 2(4): 197-202, 2014

[32] Razzaque, M.A. , Salehi, A. , Seyed, M.C. ,"Security and privacy in vehicular ad-hoc networks-Survey and the road ahead", 2013, Wireless Networks and Security, Springer, Berlin Heidelberg, pp. 107–132 .

[33] Hamdan S, Al-Qassas RS, Tedmori S. Comparative study on Sybil attack detection schemes. Int J Comput Technol.2015;14:5869–5876.

[34] Jain M, Saxena R. 2nd International Conference on Computational Intelligence and Informatics. Springer; 2018.VANET: security attacks, solution, and simulation.

[35] Zaid A. Abdulkader, Azizol Abdullah, Mohd Taufik Abdullah & Zuriati Ahmad Zukarnain, Vehicular Ad Hoc Networks and Security Issues: Survey, Modern Applied Science; Vol. 11, No. 5; 2017.

[36] Dhamgaye, Chavhan Nekita, Survey on security challenges in VANET, Wireless Communication, and Computing, International Journal of Computer Science and Network, Vol 2, Issue 1, 2013

[37] M. Azees, L J Deborah, and Vijayakumar P, IET Intelligent Transport Systems,"Comprehensive survey on security services in vehicular Adhoc networks," vol. 10, no. 6, pp. 379–388, 2016.

[38] Irshad Ahmed Sumra, Halabi Bin Hasbullah, and Jamalul-lail Bin AbMananan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey," in Vehicular Ad-hoc Networks Smart Cities, pp. 51–61, Singapore Springer, 2015.

[39] Jaballah, W. B., Conti, M., Lal, C., 2019. A survey on software defined vanets: benets, challenges, and future directions. arXiv preprint arXiv:1904.04577.

[40] Douceur J R, "The Sybil attack," Proceedings of the International Workshop on Peer to Peer Systems, 251–260, 2002.

[41] Zhou T, Choudhury R. R, Ning P, K Chakrabarty, "P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks," Selected Areas in Communications, IEEE Journal, Vol. 29, No. 3, 582-594, 2011.

[42] Zeadally Sherali, Hunt Ray, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, Vehicular ad hoc networks (VANETs): Status, results, and challenges. Telecommunication Systems, 50(4), 217–241, (2012)

[43] F. Zhang, D. Clarke, A. Knoll, Vehicle detection based on lidar and camera fusion, in: 17th Int. IEEE Conf. Intell. Transp. Syst., IEEE, 2014, pp. 1620–1625.

[44] R. Mishra, A. Singh, R. Kumar, VANET security: Issues, challenges and solutions, in: 2016 Int. Conf. Electr. Electron. Optim. Tech., IEEE, Chennai, India, 2016, p. N/A

[45] A. Vaibhav, D. Shukla, S. Das, S. Sahana, P. Johri, Security challenges, authentication, application and trust models for vehicular ad hoc network- A survey, I, J. Wireless MicrowaveTechnology (2017) 36–48.

[46] S.S. Manvi, S. Tangade, Vehicular Communication, A survey on authentication schemes in VANETs for secured communication, 9 (2017) 19–30.

[47] V. Hoa La, A. Cavalli, Security attacks and solutions in vehicular ad hoc networks: A survey, Int. J. AdHoc Netw. Syst. 4 (2014) 1–20.

[48] D. Kushwaha, P. Kumar Shukla, R. Baraskar, A survey on Sybil attack in a vehicular ad-hoc network, Int. J. Comput. Appl. 98 (2014) 31–36.

[49] M Rahbari, M Ali, J Jamali, International Journal of Network Security & Its Applications (IJNSA) (November 2011),Efficient Detection of Sybil Attack Based on Cryptography in VANET.

[50] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil,IEEE Communications Surveys and Tutorials, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards, and solutions, 13 (4) (2011) 584-616.

Dr. Arockia Xavier Annie R, is currently an Assistant Professor (since Aug 2006) in the Department of Computer Science and Engineering at Anna University, Chennai. She earned her doctorate in Information and Communication Engineering from CEG, Anna University, Chennai, in Feb, 2014. Her research concentrated on providing efficient video streaming by enhancing the local cache with interactivity. She has also worked on Security and bio-medical applications. She pursued her doctoral research under the guidance of Dr.P.Yogesh, Associate Professor at the Department of Information Science and Technology. She is well motivated and is appreciated by her peers. Her willingness to work even in confined environment is her major achievement. She has several publications both National and International Journals to her sleeve. She has eight international journals and over seven conference proceedings, and has delivered over ten lectures in seminars, symposium and workshops. Her research interests include video processing combined with machine learning, computing methods in bio-medical synthesis and processing of medical forums through neural networks. She has coordinated and arranged a platform called Technical Innovative Project (TIP) from 2015 to 2018. TIP is to boost up students' projects and lay open a venue for evaluation to several companies who are interested in procuring and enhancing the projects from the students. Students who have benefited from her mentoring are now placed in Google, Facebook and other dream companies.

G Shobana received the B.E. degree from Periyar University and M.Tech degree from SRM University in Information Technology. She is currently working toward the Ph.D. degree in Computer Science Engineering with the Anna University, India. Her research interests are in the areas of Network Security, vehicular communications and Machine Learning.