An Overview of Security Challenges in Vehicular Ad-Hoc Networks

Nisha Malik, Deepak Puthal, and Priyadarsi Nanda
Faculty of Engineering and IT, University of Technology Sydney, Australia
Email: Nisha.Malik@student.uts.edu.au, Deepak.Puthal@uts.edu.au, Priyadarsi.Nanda@uts.edu.au

***Abstract*—Vehicular Ad hoc Networks (VANET) is emerging as a promising technology of the Intelligent Transportation systems (ITS) due to its potential benefits for travel planning, notifying road hazards, cautioning of emergency scenarios, alleviating congestion, provisioning parking facilities and environmental predicaments. But, the security threats hinder its wide deployment and acceptability by users. This paper gives an overview of the security threats at the various layers of the VANET communication stack and discuss some of the existing solutions, thus concluding why designing a security framework for VANET needs to consider these threats for overcoming security challenges in VANET.**

I. INTRODUCTION

The speedy aggrandizement in Wireless communication technologies concurrently with immediate measure requisites to improve road safety have expedited a considerable development in the (ITS). ITS came into existence with a strong perspective to provide end-to-end, better, worthier, safer, efficient and much more improved transport services, both on-road and off-road. Intelligent communication technologies such as trip guiding smart phone applications, the latest safety oriented in vehicle systems (such as Anti-Lock Braking systems, air bags, Navigation systems, etc.), are all part of the ITS. Therefore, ITS is not just about modifying or repairing the age-old infrastructures of roads, highways, stations, or bus stops, but persuading security and safety of transport to all the people and goods travel on roads [1].

Wireless technologies together with in-vehicular capabilities, resulted in the formation of Wireless Vehicular communication networks termed as 'Vehicular Ad hoc Networks' (VANET). Although VANET are considered as a use case of Mobile Ad hoc Networks (MANETS), as VANET inherit most of the MANET characteristics, such as infrastructure less functionality (due to lack of central coordinator), self-configuration and management of networks, and limited physical layer security. The high speed of vehicles, adds some more attributes to these common characteristics, such as more dynamic topology with varying density, predictable movement (predefined roads), and unlimited power supply. VANET can be briefly defined as *spontaneous, self-configurable networks formed between moving vehicles, where each vehicle serving both as a mobile node and router, is equipped with wireless capabilities to support short range communications and can communicate wirelessly both with other mobile nodes (vehicles, and pedestrians) as well as static Road Side units(RSU). The vehicles, can proficiently gather and process surrounding data and transmit the same via messages containing the vehicle's unique identifier, current position, timestamp, and other safety related data in a timely manner to nearby vehicles, thereby facilitating safe driving with, real time traffic assistance, accident prevention, and emergency warning among others.*

Considering the imperative parameters of short range connectivity, scalability, latency and throughput, in VANET, which stands them out from other wireless networks, there have been efforts of modifying the existing wireless technologies and raise new standards to fit to their needs. Thus, affiliated to VANET are a certain set of standards and protocols that have evolved to ensure invulnerable inside and out network design, attain impregnable message transmission, manage user identity and data, control access to resources, authorize and authenticate network users, thus safeguarding against tracing and hacking of user privacy. These standards have evolved differently in different regions namely, Wireless access in Vehicular Environment (WAVE) in U.S. [2] and C-ITS [3] in Europe, commonly referred to as (Dedicated Short range communications (DSRC) in both the regions.

The first milestone towards standardization in US took place in 2002 when on the appeal of ITS America the FCC allocated 75 MHz of spectrum in the 5.9. GHz band specifically for connected vehicle applications. FCC initially referred to a single (Physical) PHY and (Medium Access Control) MAC standard, developed by the ASTM (ASTM E2213, published in 2003), which was based on the IEEE 802.11A OFDM PHY. [4]. After IEEE incorporated all the earlier PHY and MAC features in single IEEE-2007 edition, the IEEE task group p was formed, which amended this IEEE-2007 edition especially for V2X (Vehicle-to-Anything) communications. This WLAN standard known as IEEE 802.11p [5] specifies the PHY layer and MAC layer for DSRC based Vehicular transmissions. Later, IEEE further developed the IEEE 1609 group [6] which established the family of protocols (IEEE 1609.x) on the top of this IEEE 802.11p PHY and MAC layers to provision open access for V2V(Vehicle-to-Vehicle) and V2I(Vehicle-to-Infrastructure) communications. This protocol stack came to be known as the WAVE. Thus, the terms DSRC and WAVE are used interchangeably to refer to this stack. IEEE 1609 group, not just defined the architecture, but also developed standards facilitating V2V and V2I communications as shown in Figure 1. Which depicts the WAVE stack defined in IEEE 1609.0-2013. [30]

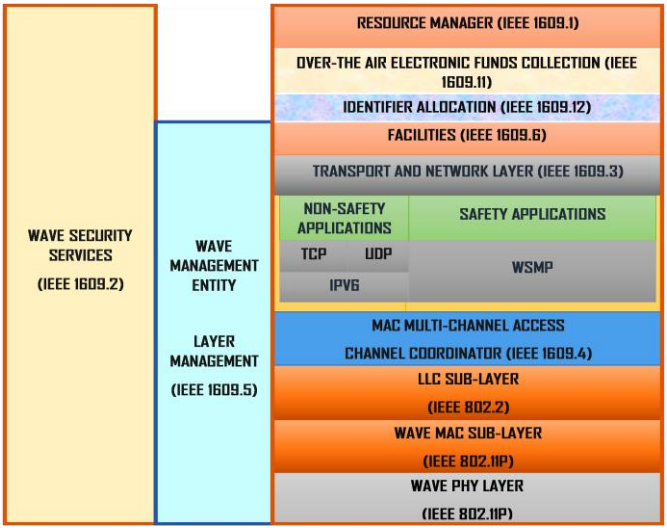

Figure 1. WAVE Protocol Stack [30]

To render security across the stack, this group defined the IEEE 1609.2 standard, which intends to provide a complete security framework incorporating all the security requirements to defend against the most common attacks. Schemes defined form components of Public Key infrastructure (PKI), where messages are securely communicated by encrypting them using Elliptic curve cryptography (ECC) and authenticated using Elliptic Curve Digital Signature Algorithm (ECDSA) [7]. ECDSA has been preferred since it delivers preeminent security with a smaller key size.

Security of road users' needs lot of attention, considering the use of openly accessible wireless channel by them, which poses threats to their security and privacy, since it gives attackers the opportunity to exploit the resources in an unauthorized way.

This paper presents the security challenges and threats to WAVE enabled VANET communications comprehensively. After listing the security requirements essential in a robust VANET framework, we have defined the various attacks at each layer of the WAVE protocol stack and the existing solutions bounding the VANET communications.

The remainder of the paper is organized as follows: Section II provides the vehicular network architecture. Section III lists the security threats of each layer, followed by an overview of existing security solutions in section IV and Conclusion of the paper is in Section V.

II. Architecture

This section discusses the core components of VANET and different types of communications achieved by them. Figure 2 depicts the complete VANET architecture, containing components involved and communications achieved.

A. Modules Performing Communications

WLAN (IEEE 802.11p compliant) modules which facilitate V2V, V2I and V2X communications form the vital parts of VANET as detailed below:

WLAN compliant OBU: The on-board unit is an in-vehicle DSRC enabled embedded device incorporating following components and devices necessary to communicate with other OBUs and RSU's. These include, *IEEE 802.11p radio transceivers*, *Communication Processor*, *Read/Write memory* to store data captured and processed from the vehicles' Electronic Control Unit (ECU) and communicated to and from the RSU with accurate time stamp, *OBD-II Interfaces* to the vehicle's Controller Area Network (CAN), to perform data acquisition from vehicle's ECU and *User Interface* to access multiple safety and infotainment applications.

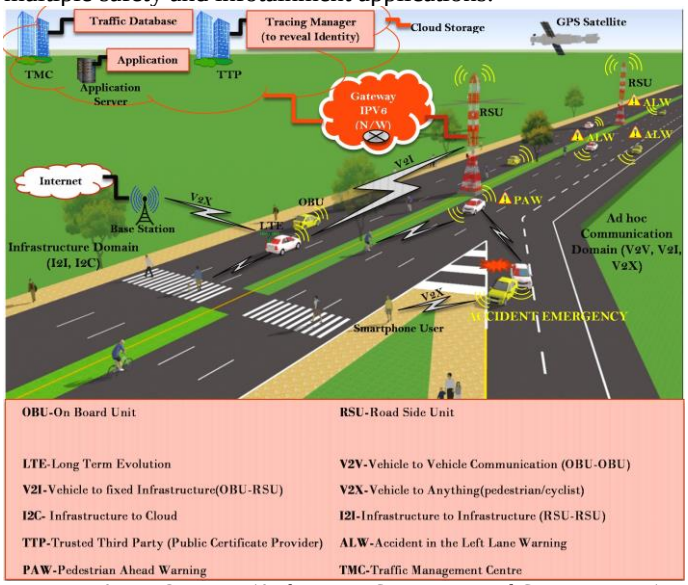

Figure 2. VANET Overview (Architecture, Components and Communication)

WLAN compliant RSU: They intrinsically contain *navigation systems*, *radio transceivers* supporting the openly available WAVE, and for more ITS applications there can be *Wii-Fi*, *LTE*, *GPRS*, *WIMAX* support [31, 32]. RSUs perform registration, association, with all the vehicles entering its region. Hence, it is equipped with slightly greater computation capabilities than the OBU and is responsible to execute three main functions: [8]

•*Serving as an Information source*: It is the provider/host of numerous safety applications and holds responsibility to disseminate warnings or alerts to vehicles in their area, such as low bridge warning, or work zone warning. Also, vehicles in an area can query RSUs regarding traffic on the road ahead.

•*Relaying information*: It relays messages to other RSUs and OBUs, thus spreading information widely.

•*Internet Connectivity*: Connects OBUs to internet via the IPv6 Gateways.

Tamper-Proof Device (TPD) [9]: It stores users' confidential data, such as private key and certificates. It is responsible to generate pseudo IDs and digital signatures using these Pseudo IDs, thereby preserving privacy and providing authentication of messages to the recipient. It is installed by the manufacturer and is only accessible to authorized parties. The users cannot tamper this device; else it will erase all the cryptographic information.

Application Unit (AU): The application unit, equipped in the vehicle, (either within the OBU or as a separate unit) [10], is a dedicated device with user interface, which by utilizing OBU's communication capabilities enables users to access services rendered by the RSUs. These can be safety

applications, information services, internet connectivity or forwarding of its own application data widely. Depending on the user's need there can be more than one application units serving different needs.

B. Modes of Communication

V2V communications: The vehicle to vehicle communications are achieved by direct radio connectivity between their respective OBUs. Embedded sensors and vehicles' RADAR perform the first step of V2V i.e. Data Acquisition and Processing, in which surrounding data is captured and analyzed by the processor and the Operating system to identify threats such as proximity of any nearby vehicle exceeding speed limits, sudden brakes by a preceding vehicle, hidden vehicle warning, lane change warning, etc. In the next step, Data Transmission happens. The values evaluated by the vehicle are then transmitted to vehicles in the 360-degree view of the vehicle in the form of data packets, every 100-300 ms according to DSRC specifications**.**

V2I Communications: V2I communications allow a vehicle to access the applications provided by the RSU. The vehicles query the RSU either for gaining road and traffic information, accessing the internet, or relaying messages to other OBUs in case of multi-hop communications.

I2V Communications: In this case, RSU's communicate with the OBUs either to revert to any query raised by the corresponding vehicle or to forewarn of any emergency event.

V2X Communications [11]: As defined by the 3GPP group vehicles performing communications with any entity other than the RSUs and other OBUs is called as V2X communication. For e.g., user accessing internet applications using a laptop or smartphone.

III. VANET Security Requirements and Possibele Attacks

Despite the numerous advantages for safety and driving assistance, it brings along a storm of threats spanning across the entire WAVE communication stack causing hazards affecting different modes of communication (V2V, V2I, V2X).

Following subsections discuss in detail the various security requirements, attacks performed by malicious users challenging these requirements and finally the measures to deal with these attacks, thus fulfilling the necessary requirements.

A. Security Requirements of VANET

Confidentiality and Access Control: Data Confidentiality ensures that the data contents are revealed only to the authorized individuals. In VANET confidentiality hails as a primitive requirement achieved by applying certain access control policies and cryptographic mechanisms on the stored and transmitted data. This requirement becomes even more imperative, particularly for the military application, where information disclosure is not just a security breach, but undoubtedly life threatening.

Integrity: Integrity of data is validated, if the transmission of data from source to destination occurs with no external (unknown and unauthorized) interference and tampering, and accuracy and reliability of data can be ensured at the destination. In VANET, if a malicious attacker alters the transmitted data pretending to offer safety, it can lead to traffic congestions, or unwanted route diversions for drivers.

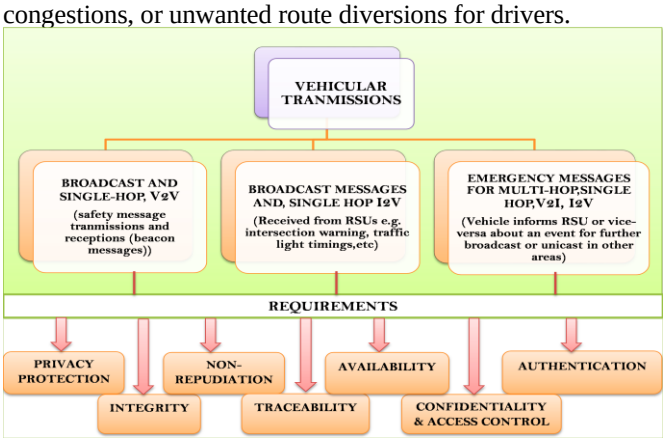

Figure 3. Security requirements of vehicular transmissions'

Availability: To access the network resources, it's necessary for them to be available when required in a timely manner. Considering stringent delay requirements of messages in VANET, if unnecessary message transmissions by attackers consumes most of the available bandwidth, it leads to DOS (Denial-of-service) for legitimate users. Thus, how we counter DOS attacks, plays crucial role in network availability for rightful users.

Authentication: Authentication is the process of identifying network users by means of Unique ID and password/biometrics to grant them authorization for accessing the resources. It's a necessary step in VANET to ensure both the message received and the sending node are authenticated. It's accomplished by means of the user certificate and signature verification.

Conditional Privacy preservation: Privacy refers to hiding critical and personal user information from unwanted and unauthorized entities, to ensure safety and security. In VANET, it is necessary to keep user's identity a secret or use frequently changing pseudonyms IDs to avoid location tracking or impersonation. Offering complete privacy is impossible in VANET as the user's identity needs to be revealed and traced in case of emergency scenarios such as any accident enquiry requiring the user's location and personal information.

Non-Repudiation: Non-repudiation ensures that when recipient identifies who the sender is, the sender takes complete responsibility and cannot deny sending the message. Digital Signatures included in the message can serve the purpose, to avoid any conflicts in such scenarios.

Trust: It is emerging as the most important requirement to deliver a successful security framework for VANET. Although we can verify, and authenticate received messages, but considering the number of entities involved and the difference in their backgrounds, we cannot trust them.

To achieve these security requirements as depicted in figure 3, firstly we need to have a clear view of the attacks preventing their accomplishment and later we review some of the existing solutions proposed and efforts made targeting these requirements.

B. Attacker Entities

Rapacious or impatient Drivers: Under normal driving conditions, a driver follows rules, and is ready to go through

congested scenarios and delivers reliable safety messages. But, if he turns out to be greedy, then irrespective of other road users' needs he would send false messages by impersonating to be 100 vehicles, thus declaring congestion on the route. In another case, to avoid any fines or to escape from message forgery accusations, he might tamper vehicles' hardware and Software, in the absence of TPD [11].

Malicious Attackers: These also cause deliberate damage, serving them a purpose, either for fun or accomplishment of any illegal activities.

C. Attacks on the Different Layers

As discussed earlier, the attacks span across the entire WAVE stack, which are listed in this section along with the damage they cause.

1) Attacks at the Application Layer: The application layer renders the services needed for the safety and non-safety applications, access them from the Provider (RSU and other fixed infrastructure) and defines the exact message format. It is the responsibility of this layer to identify the reachability of network providers, authenticate them, abide by necessary protocols and data syntax and ensure integrity of data by establishing trust. Following attacks on the application layer interrupt its normal functionalities and compromise the confidentiality, integrity, Privacy and may also result into Repudiation.

Message Falsification/tampering: It is the act of sending incorrect/false information in the network, either by the greedy drivers, or malicious intruders. To gain complete access and avoid congestion the driver might broadcast false messages, stating some accident emergency or congestion on route. In worst case scenario, an attacker might take over any RSU and send false warning, about work zone or access private information while other OBUs communicate with this RSU. Thus, message originator authentication and verification becomes inevitable to ensure integrity and confidentiality.

Repudiation: If the attacker fakes another vehicles' identity by replicating signatures, it can easily lead to the legitimate user denying of sending messages which were sent using his signature.

Malware Attack: In this by faking identities, user can send fake software updates to the OBU, or send unnecessary advertisements causing bandwidth consumption.

Location Tracking: It becomes easy for the adversary to perform 'signature linking' even from Pseudonyms if they aren't changed frequently and thus makes it easy for any insider to track user's activities, monitor route.

GPS Spoofing attack: [14]. In this attack, intruders use simulators generating GPS signals stronger than the GPS satellite signals, which can alter the vehicles' GPS device information, also interrupting with the working of other location based services and applications. [15]

2) Attacks Targeting Network and Transport Layer functionalities: The network layer makes it possible to deliver messages by performing routing and forwarding functions, logical addressing, and controlling congestion. Requisite Single-hop, multi-hop communications are performed by selecting appropriate route and QOS. It performs uni-cast, multi-cast and broadcast transmissions and the transport layer enforces protocols to achieve these transmissions, also assuring reliable delivery of data packets. Adversaries which attack these layers disrupt these functionalities by following attacks:

Impersonation Attack: Every vehicle associated with VANET is assigned with a unique ID. In this attack, an adversary forges the identity of a legitimate user and thus, enters the network falsely by claiming to be an authorized user.

Sybil Attack: It is a type of impersonation attack in which the adversary pretends to be multiple identities [16].Due to the absence of central coordinator in VANET, the nodes are responsible for performing the routing functions, hence, the authentication of messages and mapping of entity to identity takes place at the local level, relying solely on the assumption of cooperation and trust among the nodes, which can easily be violated by an intruder. The purpose of Sybil attack lies in the fact of 'believing mass messages delivering same information'. If a single node communicates falsely regarding some emergency or event, it would be difficult to trust, but similar data when received from multiple authorized identities tends to persuade the legitimate users and act in the favor of the adversary. It is the most treacherous and hazardous attack in the VANET scenario and it's important to detect the Sybil nodes [9] [17].

Black Hole Attack: A black hole is that part of the network which is created by an attacker, to gain access to the packets of a targeted node. The malicious node is the 'black hole' here, because even though it is shown a participant in the network, but it's not performing the routing functions, either unintentionally [16], by simply opting out of forwarding packets or intentionally where it cleverly advertises itself to be on the shortest route to the destination by cheating with the routing protocols and convinces other gullible nodes, thus causing a new corrupt route formed. The sender nodes being unaware, keep forwarding data packets to this node, which are forwarded to either undesired locations or kept by the node itself, thus initiating 'man-in-the-middle' attack. [18]

Grey Hole Attack: It is a type of Black Hole attack in which the black node routing the data, drops selected data packets at a particular time or destined for a certain node, but, at other times functions fine [19].

Worm Hole attack [20]: A single or multiple malevolent nodes come together to launch this wormhole attack, in which messages received at one point are 'tunneled' to some other point and replayed from there. The attacker is either in possession of some cryptographic information and as a legitimate participant, launches this attack, or as an outsider, attacks in the hidden mode, with a motive to analyze traffic or simply launch 'DOS' attack, thereby dropping packets.

Layer Targeted	Type of attack	Compromised security requirement	Communication affected
Application Layer	Message Falsification/tampering	Confidentiality, integrity	V2V, V2I
	Repudiation	Non-repudiation	V2V, V2I
	Malware attack	Availability	V2V, V2I
	Location tracking	Privacy	V2V
	GPS spoofing	Privacy	V2V
Network &Transport Layer	Impersonation	Integrity, Authentication	V2V
	Sybil attack	Authentication, Availability and Privacy	V2V
	Black Hole attack	All except privacy	V2V
	Grey Hole attack	All except privacy	V2V
	Worm hole attack	All except privacy	V2V
	Replay Attack	Authentication	V2V
PHY and MAC layers	Denial of Service attack	Availability	V2V, V2I
	Distributed DOS	Availability	V2V, V2I
	Spamming	Availability	V2V

Thus, every packet sent should include a timestamp so that the messages with the same content can be compared if re-transmitted.

3) Attacks on PHY and MAC layers: Following attacks on the application layer interrupt its normal functionalities.

Denial-of-service attack: It is a type of attack in which the network resources are intentionally kept occupied by adversary to prevent the legitimate users from accessing them. The malevolent node would usually flood the network [16] with unwanted messages such as advertisements, or replay messages (replay attack), or perform 'signal jamming'. In another case, a malicious node can send fake emergency messages to keep the RSU busy to respond to other genuine requests, causing accidents and collisions. [9]

Distributed DOS attack: It is a variant of the DOS attack where the DOS attack is carried out from different locations and different timings [22], creating additional problems for the network users.

The DOS attacks are specific to the PHY and MAC layers, but all the attacks discussed above, i.e. Sybil attack, message falsification or other attacks at the various layers are a breach to the PHY and MAC layers, because they make use of the network resources either from the inside or outside to perform these attacks.

Spamming: If intentional spam messages are injected in the network, it affects the channel access by other users. This is done to increase the transmission latency, thereby accomplish malicious acts [16]

The summary of the security threats and infrastructure with layer wise classifications are given in Table 1.

IV. Existing Security Solutions

Researchers have been extensively analyzing the attacks and security requirement of VANET, starting with the first of efforts by [9], [23], [24] [25]. Raya et al. [9] have highlighted the security threats of VANET for the first time, and addressed solutions to facilitate secure vehicular communications. In this, the authors propose a Public Key Infrastructure (PKI) System, to render all the above discussed security requirements. Methods for storing and distribution of public and private key, certification and revocation are addressed. Furthermore, privacy preservation is addressed by means of Electronic License Plate (ELP) and anonymous key pairs. For authenticating safe messages, Digital Signatures are proposed to verify the authenticity of messages. The Tamper-Proof device in the vehicle is the store-house of all the cryptographic information, and is thus responsible for storing the private key used to generate the digital signatures and signing messages. Keeping in view, the stringent delay requirement, authors have also stated the advantages of 'Group Communication' for quicker authentication of emergency messages.

In [26], authors have proposed a 'Global security architecture', which does not mention any standardizations, but describes a layer wise architecture, keeping all the security requirements at different levels of communication into consideration. The material level security comprises of the security of different modules which are adding to different steps of communication, & responsible for acquiring and transmitting data, for e.g. OBU, GPS, antennas, etc. These can be secured by the addition of a TPM [27] connecting them. The authentication level deals with the authentication of entities and data at different points of communication. This includes node authentication and association before entering network as well as data verification in communication. Also, authentication of user's location is performed to validate the position of the node. The trust level is meant to ensure the trustworthiness of different nodes and make sure that nodes responsible for transmitting the messages do not deny their participation i.e. non-repudiation. The message/data level ensures data security using Digital Signatures, and finally the cryptographic level ensures users' privacy by means of identity protection and tracking. It also tends to protect the system from Sybil attacks.

The above papers give a generalized overview of the VANET security challenges, and a survey on the existing solutions. But most of the recent works have targeted Authentication with privacy preservation.

Huang et al. [28] have specifically defined privacy preserving anonymous authentication schemes. Privacy preserving authentication (PPA) as discussed earlier, is an authentication scheme, whereby users authenticate each other without revealing confidential information. PPA schemes are classified based on authentication, i.e. symmetric or asymmetric encryption and on the basis of privacy preservation. It clearly differentiates PPA, if authentication is done via anonymous key pairs, and only Trusted third party is authorized to reveal identity in abnormal scenarios or is it based on pseudonyms, which can be generated by the TTP, RSU's or maybe the vehicle. The existing schemes implementing these or targeting these are discussed with their solutions with further challenges. Some of the emerging issues are the design of VANET with less dependency on the Infrastructure, trusting the origin and need of a heterogeneous solution to support interoperability among the Vehicular and other wireless networks (e.g. WiMAX, Cellular), etc.

Hasrouny et al. [29] have also discussed some of the significant and emerging issues such as trusting the node disseminating data, how to check for its reliability and what would be the immediate and necessary actions to take if the node isn't impeachable and is not able to prevent malware attacks in the OBUs, at that point of time, it is necessary to protect them against malicious code installations or updates.

Thus, with security and privacy of users, the most emerging issue is trust and certitude in the data origin. We need efficient, methodical and some business-like security frameworks with user privacy protection for VANET.

V. Conclusion

The last two decades have witnessed substantial augmentation in the 'connected vehicle applications', incorporating Highway Traffic safety and efficiency applications, along with tranquil and infotainment applications. Despite these developments, the transportation industry lacks in the world-wide implementation of the proposed standards and on-road deployment, majorly due to security of communications on road. We are in desperate need of some robust frameworks which can efficiently fulfil the security requirements of VANET to avoid any setbacks caused by the misuse of network resources by adversaries, thus risking people's life on road. The future ITS needs a lot of advancements in what exists today to give a better, reliable and a secure road experience to people on motorways.

This paper presented a comprehensive survey of security threats at each layer of the WAVE communication stack, attacker entities responsible and effects on the vehicular communications. The existing solutions resolving some or most of these have been detailed and finally, an insight into the current research challenges is given to motivate researchers to implement a secure and trustworthy framework for VANET in ITS.

VI. References

[1] Auer, Ashley, Shelley Feese, and Stephen Lockwood. History of intelligent transportation systems. No. FHWA-JPO-16-329. 2016

[2] Kenney, J. B. (2011): Dedicated Short-Range Communications (DSRC) standards in the United States. Proc. IEEE, 99(7), 1162–1182.

[3] Festag, A. (2014): Cooperative Intelligent Transport Systems (C-ITS) standards in Europe. IEEE Commun. Mag., 12(52), 166–172.

[4] ASTM E 2213, "Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems — 5GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2002.

[5] IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-2012 (Revision of IEEE Std. 802.11-2007), 2012, pp. 1–2793.

[6] Institute of Electrical and Electronics Engineers 1609 Working Group Public Site. Available Online: http://vii.path. berkeley.edu/1609/wave/.

[7] Johnson, Don B., and Alfred J. Menezes. "Elliptic curve DSA (ECDSA): an enhanced DSA." *Proceedings of the 7th conference on USENIX Security Symposium*. Vol. 7. 1998.

[8] Al-Sultan, Saif, et al. "A comprehensive survey on vehicular ad hoc network." Journal of network and computer applications 37 (2014): 380-392.

[9] M. Raya and JP. Hubaux. Securing Vehicular Ad Hoc Networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, 15(1):39–68, 2007.

[10] Baldessari, Roberto, et al. "Car-2-car communication consortium-manifesto." (2007).

[11] Study on LTE-Based V2X Services (Release 14), Tech. Specification Group Serv. Syst. Aspects (TSG SA), 3GPP TR 36.885, 2016

[12] ETSI, TCITS. Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions. Vol. 1. Tech. Rep. ETSI TR 102 638, 2009.

[13] Dhamgaye, Anup, and Nekita Chavhan. "Survey on security challenges in VANET 1." (2013)

[14] Zeadally, Sherali, et al. "Vehicular ad hoc networks (VANET): status, results, and challenges." Telecommunication Systems 50.4 (2012): 217-241

[15] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." Vehicular Communications 1.2 (2014): 53-66.]

[16] Douceur, John R. "The Sybil attack." *International Workshop on Peer-to-Peer Systems*. Springer, Berlin, Heidelberg, 2002.

[17] M. Raya, P. Papadimitratos, and JP. Hubaux. Securing Vehicular Communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 13(5):8–15, 2006.

[18] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." Vehicular Communications 1.2 (2014): 53-66.

[19] Nogueira, Michele, et al. "A security management architecture for supporting routing services on WANETs." IEEE Transactions on Network and Service Management 9.2 (2012): 156-168.

[20] Khabbazian, Majid, Hugues Mercier, and Vijay K. Bhargava. "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks." IEEE Transactions on Wireless Communications 8.2 (2009): 736-745.

[21] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[22] Al-Kahtani, Mohammed Saeed. "Survey on security attacks in Vehicular Ad hoc Networks (VANET)." Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on. IEEE, 2012.

[23] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In Proc. of European Wireless 2002 Conference, Florence, Italy, February 2002, 2002

[24] .-P. Hubaux, S. Capkun and J. Luo, The security and privacy of smart vehicles, IEEE Security and Privacy Magazine 2(3) (2004), 49–55.

[25] B. Parno and A. Perrig, Challenges in securing vehicular networks, in: Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[26] Engoulou, Richard Gilles, et al. "VANET security surveys." Computer Communications 44 (2014): 1-13

[27] Morris, Thomas. "Trusted platform module." Encyclopedia of cryptography and security. Springer US, 2011. 1332-1335.

[28] Lu, Huang, and Jie Li. "Privacy- preserving authentication schemes for vehicular ad hoc networks: a survey." *Wireless Communications and Mobile Computing* 16.6 (2016): 643-655.

[29] Hasrouny, Hamssa, et al. "VANet security challenges and solutions: A survey." *Vehicular Communications* (2017).

[30] IEEE 1609.0.2013 (2013) IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture. IEEE, USA.

[31] W. Drira, D. Puthal, and F. Filali. "ADCS: An Adaptive Data Collection Scheme in Vehicular Networks using 3G/LTE." in *3rd International Conference on Connected Vehicles and Expo*, pp. 753-758, 2014.

[32] D. Puthal, Z. Mir, F. Filali and H. Menouar, "Cross-Layer Architecture for Congestion Control in Vehicular Ad-Hoc Networks." in *2nd International Conference on Connected Vehicles and Expo*, pp. 887-892, 2013.