Journal of Multimedia Information System VOL. 7, NO. 1, March 2020 (pp. 45-54): ISSN 2383-7632 (Online)
http://doi.org/10.33851/JMIS.2020.7.1.45

Security Attacks and Challenges of VANETs : A Literature Survey

Abdul Quyoom[1*], Aftab Ahmad Mir[2], Dr. Abid Sarwar[3]

Abstract

This paper presented a brief introduction along with various wireless standards which provide an interactive way of interaction among the vehicles and provides effective communication in VANET. Security issues such as confidentiality, authenticity, integrity, availability and non-repudiation, which aims to secure communication between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). A detailed discussion and analysis of various possible attacks based on security services are also presented that address security and privacy concern in VANETs. Finally a general analysis of possible challenges is mentioned. This paper can serve as a source and reference in building the new technique for VANETs.

Key Words: Security Attacks, Security Services, VANET.

I. INTRODUCTION

Vehicular networks are emerging as a new promising field of wireless technology. A VANET is a distinctive class of a MANET in which moving vehicles act as either a node or a router to exchange messages between vehicles, or an Access Point (AP). Typically, it can connect to vehicles within the range of 100 to 900 meters if using 802.11p. It is aimed to support both vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication over infrastructure-less network. It is essential to realize that the ITS aims to improve road safety and provides a comfortable travel experience to driver and passengers [1], [8]. There have been numerous research initiatives such as COOPERS, CVIS, SAFESPOT, PReVENT, Wireless Access in Vehicular Environments (WAVE) and Advanced Safety Vehicle Program (ASV) carried out across Europe, US and Japan to turn ITS into a reality. VANET provides the ability to a vehicle to communicate along with nearby vehicles and road-side unit (RSUs) as shown in Figure 1. When RSU receives a message from vehicle, it authenticates the message to ensure no malicious message. The Autonomous Server (AS) is responsible for security related issues between vehicle and RSU. Based on wireless fundamental concepts, Wireless Ad-Hoc Network (WANET) has many categories such as wireless mesh networks, wireless sensor networks and Mobile Ad-Hoc Networks (MANETs). VANETs is a subset of MANETs with a unique characteristic of dynamic nature or node mobility, frequent exchange information, real time processing, self-organizing, infrastructure less nature, low volatility and distance. It is considered the first commercial vehicles of MANETs. In VANETs, security and privacy are identified as major challenge. This research discusses the security issues such as confidentiality, authenticity, integrity, availability and non-repudiation aim to secure communication between V2V and V2I.The privacy issues are concerned with protecting and disclosing drivers personal information such as name, location etc. [21].

This paper has discussed and analyzed the possible of security attacks from 13 researchers that address security and privacy concern in VANETs [21]. The analysis concludes that a research gap in the area of security in VANETs. In Section 3, a study on the relationship between securities services versus the technique proposed to encounter the possible attacks is presented. VANETs are used to support safety critical applications and non-safety infotainment or entertainment based applications. Safety applications such as collision avoidance, pre-crash sensing or lane changing are aimed at minimizing road accidents by

Manuscript received December 02, 2019; Revised December 24, 2019; Accepted December 28, 2019. (ID No.JMIS-19M-12-046)
Corresponding Author (*): Abdul Qayoom, University of Jammu, India, quyoom12345@gmail.com
[1,3]University of Jammu, India,
[2]Shri Venkateshwara University U.P. India

using traffic monitoring and management applications. Non-safety applications, on the other hand, enable passengers to access various services like Internet/World Wide web, interactive communication, online games, payment services and information updates while vehicles are on the move. The key difference between safety and non-safety applications is that the safety applications are capable of sending and processing messages in real time [3]. The driver and passengers can access both kinds of services from the nearby infrastructure seamlessly using wireless access technologies [7].VANET and MANET have many similarities such as dynamic topology, multi-hop data transmission, distributed architecture and Omni-directional broadcast. In both networks, mobile nodes are able to route or relay datato the destination by itself [23]. However, there are some notable differences between VANET and MANET. Since the vehicles are moving along the road, the mobility of nodes in VANET is predictable unlike MANET [5]. Furthermore, there is no limitation of storage and processing capability and battery power of nodes in a VANET. Due to the fast movement of nodes the topology of network formed tends to become highly dynamic. In addition, network density in VANET varies significantly over time and location [8].

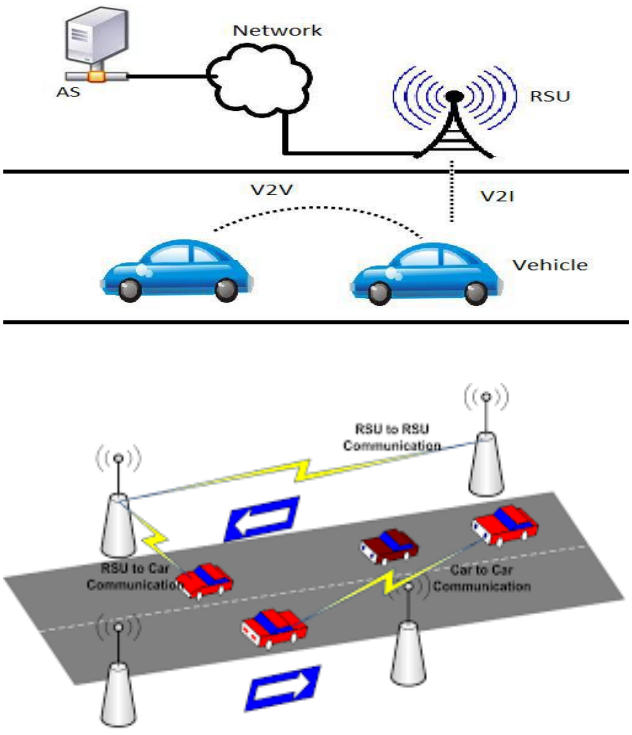

Fig 1: V2V and V2I communication.

II. STANDARDS FOR WIRELESS ACCESS IN VALNET

Vehicular environment supports different communication standards that relate to wireless accessing. The standards are generally helpful for the development of product to reduce the cost and it also helps the users to compare competing products. These standards are as follows:

2.1 IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE)

It is also known as IEEE 802.11p. It supports the ITS applications, for a short range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz frequency range. It provides real time traffic information improving performance of VANET. It also benefits the transport sustainability. It contains the standard of IEEE 1609 [7], [8], [9]. This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques to divide the signal into various narrow band channels. This also helps to provide a data transferring rate of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in10 MHz channels.

2.2 Dedicated Short Range Communication (DSRC)

It provides a communication range from 300m to 1Km. The V2V and V2R communication takes place within this range. DSRC [5], [6] uses 75MHz of spectrum at 5.9GHz, which is allocated by United States Federal Communications Commission (FCC). This provides half duplex, 6-27 Mbps data transferring rate. DSRC is a free but licensed spectrum. Free means FCC does not charge for usage of that spectrum and licensed means it is more restricted regarding of its usage. The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channel is reserved only for safety communication. Two channels are used for special purpose like critical safety of life and high power public safety and rests of the channels are service channels.

III. CHARACTERISTICS OF VANET

VANET is an application of MANET but it has its own distinct characteristics which can be summarized as:

- **High Mobility:** The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy [2], [21].

- **Rapidly changing network topology**: Due to high

node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.

- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.

- **Wireless Communication:** VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication.

- **Time Critical:** The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

- **Sufficient Energy**: The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited power.

- **Better Physical Protection**: The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack [23].

IV. SECURITY SERVICES IN VANET

Security is an important issue for ad hoc networks, especially for security sensitive applications. To secure an ad hoc network, we need to consider the following attributes as criteria to measure security which includes availability, confidentiality, integrity, authentication and non-repudiation.

4.1 Availability

The availability deals with network services for all nodes comprises of bandwidth and connectivity [13]. In order to encounter the availability issues, prevention and detection technique using group signature scheme has been introduced [5]. The scheme is focusing on availability of exchanging the messages between vehicles and RSUs. When the attack causes network unavailability, the proposed technique still survives due to interconnection using public and private keys between RSUs and vehicles.

4.2 Authentication

Authentication is the verification of the identity between vehicles and RSUs and the validation of integrity of the information exchange. Additionally, it ensures that all vehicles are the right vehicle to communicate within network. Public or private keys with CA are proposed to establish connection between vehicles, RSUs and AS [8], [12]. On the other hand, password is used to access to the RSUs and AS as authentication method [9].

4.3 Integrity

Data integrity is the assurance that the data received by nodes, RSUs and AS is the same as what has been generated during the exchanges of the message. In order to protect the integrity of the message, digital signature which is integrated with password access is used [10].

4.4 Confidentiality

Confidentiality ensures that classified information in the network can never disclose to unidentified entities [14]. It also prevents unauthorized access to confidential information such as name, plate number and location. The most popular technique, pseudonyms are used to preserved privacy in vehicular networks [2], [3], [21]. Each vehicle node will have multiple key pairs with encryption. Messages are encrypted or signed using different pseudo and these pseudo has not linked to the vehicle node but relevant authority has access to it. Vehicle need to obtain new pseudo from RSUs before the earlier pseudo expires.

4.5 Non-Repudiation

Ensures that sending and receiving parties cannot deny ever sending and receiving the message such as accident messages. In certain fields, non-repudiation is called audit ability whereby RSUs and vehicles can prove have been receive and sent respectively.

V. POSSIBLE ATTACKS IN VANETS

Even if there are advances in VANET but still it has many challenges to be overcome. This challenge is attacks on VANET. Raya et al. [13] classifies attacker as having

three dimensions: “insider versus outsider”, “malicious versus rational”, and “active versus passive”. The types of attacks against messages, can be described as follows: “Bogus Information”, “Cheating with Positioning Information”, “ID disclosure”, “Denial of Service”, and “Masquerade”. Irshad Ahmed Sumra et al. [14] proposed different classes of attacks like network, application, timing, monitoring, and social. Each class describes different type of attack, its threat level, and its priority. Along with this model some new attacks are also proposed by them. The aim of their model is to easily identify these attacks and their association to respective classes. The purpose of these attacks is to create problem for users to access the system or phishing some information. Attacks in VANET [4], [15] are classified depending on the Availability, Authentication / identification, Confidentiality, Privacy, Non-repudiation, and Data-trust. Some of them are discussed below [21].

5.1 Attacks on availability

Availability in VANET means any information at any time of communication. This security requirement is critical in time varying environment. Availability in VANET should be assured both in the communication channel and participating nodes. A classification of these attacks, according to their target, is as follows:

5.1.1 Spamming

Spamming are the messages which are of no use to the users like advertisements. The aim of such attack is to consume bandwidth and increase the transmission latency. Centralized administration control is difficult n such attacks [23].

5.1.2 Broadcast Tampering

In this type of attack the attackers introduces false safety messages into the network. This message sometime hides the traffic warnings [7]. This leads to the critical situation like accidents and road congestions’.

5.1.3 Denial of Service (DoS) and DDoS Attack

Denial of Service (DOS) [14] is one of the most serious level attacks in vehicular network. In DOS attack, the attacker jams the main communication medium and network is no more available to legitimate users. The main aim of DOS attacker is to prevent the authentic users to access the network services. DOS attack also causes the attacks like DDOS (Distributed Denial Of service) which is one of the sever attack in vehicular environment. The aim of this attack is to slow down the network. Jamming is also one of the kinds of DOS attack which jams the channel, thus not allowing other users to access the network services. The attacker attacks the communication medium or network’s nodes to cause the channel or some problem to networks or nodes. The vehicle is unable to access the networks and result in devastation and overtiredness of the nodes and network’s resources. None of the researchers are focusing on DoS and DDoS attack in VANETs as up to date.

5.1.4 Malware

Malware is a malicious software whose aim to disrupt the normal operation. This attack is carried out by insider. This attack is introduced in the network when the software update is received by car’s VANET units and roadside station.

5.1.5 Black Hole Attack

This is one of the security attack occur in VANET. In this attack the attacker node refuses to participate or even drop the data packet [16]. Hence the effect of this type of attack is most dangerous to the vehicular network.

5.1.6 Greedy Drivers

Greedy drivers are those who try to attack for their own benefit. These drivers cause overload problem for RSU. This leads to delay in service to the authorized users. On increasing number of such drivers the authorized users faced slow services.

5.2 Attacks on Authentication/identification

In these types of attack the affected area is identification/authentication. Whenever any vehicle in VANET needs secure communication its basic requirement is either identification or authentication of nodes under consideration. When the receiving vehicle is identified or authenticated then only a trustworthy transmitter vehicle is allowed to communicate amongst them. The different types of attack on authentication/identification are discussed as follows.

5.2.1 Replay /Playback Attack

It is a form of network **attack,** in which a valid data transmission is maliciously or fraudulently repeated or delayed. This attack happens when an attacker replays the transmission of earlier information to take advantage of the situation of the message at time of sending [6], [23].

5.2.2. Sybil Attacks

Sybil attack is the creation of multiple fake nodes broadcasting false information. In Sybil attack, a vehicle install with On Board Unit (OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity. The problem arises when

malicious vehicle is able to pretend as multiple vehicles and reinforce false data. There are several technique proposed to encounter Sybil attack in VANETs such as statistical and probability, signal strength and session keys [1]-[6]. However, each of these schemes has advantageous and disadvantageous due to dynamic characteristics, weather conditions and system design. One of the interesting method proposed by [1] and [4] are based on statistical and probability algorithm integrated with signal strength as an input data. The different between received signal strength and estimate signal strength is claimed by positioners calculated. It is analyzed by AS using statistical and probability algorithm. A framework to detect Sybil attacks in nodes has been proposed using Certificate Authority (CA) [2], [3]. Two main steps involve in the process are system initialization and attacks detection where public key and private key are used during system initialization to sign in the message.

5.2.3 Masquerading

This attack is a result of providing false identities while communication by an attacker. Masquerading [15] involves message fabrication, alteration and replay. For example, to slow down other vehicle speed an attacker tries to act as an emergency vehicle and hence defraud other vehicle.

5.2.4 Global Positioning System (GPS) Spoofing

The exact position on the earth can be easily known to every vehicle by using GPS. In this attack an attacker provide false information to other vehicle by producing false readings in the GPS devices. This is done by an attacker using GPS simulators that generate signals which are stronger than those generated by genuine satellite

5.2.5 Tunneling

This attack happens when an attacker connects two distant parts of the Adhoc network using an extra communication channel as a tunnel. As a result, two distant nodes assume they are neighbors and send data using the tunnel [12]. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack

5.2.6 Message Tampering

In this attack the valuable or even critical traffic safety messages can be manipulated. This is done by attacker by modifying, dropping or corrupting the messages [7].

5.2.7 ID Disclosure

In this type of attack the ID of targeted nodes will get disclosed for tracking the current location of that node. A global observer monitors the target nodes and sometime sends a malicious message such as virus to neighbor of targeted nodes. When the neighbors of the attacker are attacked by virus, then they take the ID of the target nodes as well as target's nodes current location [2], [7]. This tracked data is used for other purpose like car rental companies to track their own cars [15]. F. Li et al. is used pseudonyms as an exchange mechanism to encrypt and hide vehicle's unique identity such as driver's name, plate number and location [10]. The pseudonyms used the Public Key Infrastructure to sign the message and this make it difficult to track.

5.2.8. Sending False Information

Sending False Information can be described as sending the wrong and fake information purposely by one node to another to create chaos scenarios. This scenario may create misinterpretation of the actual scenario. False information is sent by attackers to vehicle for selfish reasons. For example, attacker might send false report on congestion, accident or road block in order to clear the road. A scheme has been proposed to detect the compromised nodes that may misbehave using different kinds of technique [2], [3], [5], [12]. One of the schemes is a group signature which relies on password access. It can be applied to sign message so that when another vehicle receives a message, it only check the authentication of the message. This scheme is not practical since group members always will change frequently especially in a city networks.

5.2.9 Node Impersonation

Node impersonation is an attempt by a node to send modified version of message and claims that the message comes from originator for the unknown purpose. An algorithm technique to detect and isolate node impersonation using greedy algorithm that is Detection of Malicious Vehicle(DMV) and Outlier Detection algorithm has been proposed to overcome this problem [7]-[9]. The schemes used RSU to detect and observe an abnormal behavior of nodes. The proposed scheme increases the trust value of the node if the vehicle is trusted. The identity (ID) of the vehicle will be reported to the relevant Certificate Authority (CA) as malicious if distrust value is higher than threshold value.

5.3 Attacks on confidentiality

Confidentiality is one of the important security requirement in vehicular communication, it assure that the message will only be read by authorized parties [16]. This kind of security requirement is generally present in group communications, in which only group members are allowed to read such information. The remaining VANET

settings transmit public information. Because VANET mobility is higher than MANET, routing with capability of ensuring security in VANET is more problematic than Adhoc [13]. Confidentiality of messages exchanged between the nodes of a vehicular network is particularly vulnerable with techniques such as unlawful collection of messages through eavesdropping and gathering of location information available through the transmission of broadcast messages. In case of eavesdropping, the attacker can collect information about existing users without their permission and use the information at a time when the user is unaware of the collection. Location privacy and anonymity are important issues for vehicle users [21], [23].

5.4 Attacks on privacy

This type of attack is related with unauthorized accessing important information about vehicles. There is direct relation between driver and vehicle. If the attackers illegally access some data this directly affect the driver's privacy [15]. Usually a vehicle owner is also its driver, so if an attacker is getting the owner's identity then indirectly vehicle could put its privacy at risk; this type of privacy attack is called as identity revealing. Location tracking is also one of the well-known privacy attacks. In this attack the location of vehicle or the path followed by that vehicle at particular period of time is considered as a personal data.

5.5 Attacks on non-repudiation

When two or more user shares the same key then non-repudiation [15] is occurred. Due to this, two users are not distinguished from each other and hence their actions can be repudiated. An identical key in different vehicle should be avoided using a reliable storage.

5.6 Attacks on data trust

Data trust can be compromised by simply inaccurate data calculation and sending affected message, this can be done by manipulating sensors in vehicle, or by changing the sent information [15]. This affects the whole system reliability. And hence some mechanisms must be developed to protect against such attacks in practice in vehicular network.

VI. CHALLENGES AND FUTURE PERSPECTIVES

Given the challenges and characteristics of VANETs, some future perspectives should be considered to design new efficient communication approaches, as follows:

Network Management: Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as rapidly as the topology changed.

Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

Real time Constraint: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm [22].

Key Distribution: All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue.

Therefore distribution of keys among vehicles is a major challenge in designing security protocols [22], [32].

Incentives: Manufactures are interested to build applications that consumer likes most. Very few consumers are agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers & government is a challenge to implement security in VANET.

Highly heterogeneous vehicular networks: many non-interoperable wireless networking technologies have emerged with the rapid development and availability of mobile computing systems and environments, As a consequence, connectivity across different wireless networking technologies is very complex in terms of node addressing, quality of service, routing, security and billing. Thus, it is expected that the next generation of intelligent transportation systems reflect a more holistic approach to network solutions. This would require support to the coexistence of multiple different co-located wireless networks to provide ubiquitous and universal access to broadband services [11].

Data management and storage: As outlined above, we can expect to have large scale vehicular networks with millions of vehicles, which will generate huge amounts of distributed data that must be stored in some fashion and distributed across the VANETs. Due to this feature, as pointed out in [17, 19], size of network and amount of produced data is very large, it pose new and unique challenges to data management in this setting.

Localization systems: Critical safety applications in VANETs require more reliable and high accurate localization systems. A natural solution of a localization system for VANETs is to embed a navigation device in each vehicle. But satellite-based positioning systems present some undesired problems such as not always being available. Furthermore, satellite-based positioning systems are vulnerable to several types of attacks such as spoofing and blocking. In addition, it has a localization error of 10 to 30 m, which does not satisfy the requirements of critical applications for VANETs and implies the need for other localization techniques.

Disruptive tolerant communications: Current problems, such as higher delay and lower reliability delivery, are more constant in sparse networks. To increase the delivery reliability, some solutions make use of the carry-and forward technique, which further increases the information delivery time. Those problems may be solved/minimized exploring new data communication approaches for Heterogeneous Vehicular Networks. As another alternative, the driver's behavior can be considered to improve the carry-and-forward method and reduce the information delivery time.

Tracking a target: Communication is a fundamental aspect in any network and, in VANETs, depends on the physical location of vehicles. Therefore, tracking a target is a fundamental functionality in VANETs for communication protocols and also for applications and services that can benefit from this type of information [20]. Tracking requires creating a mechanism to identify the path a node follows in the network and predict the next positions if necessary. As pointed out before, privacy issues have to be observed in the devised solutions [22].

VII. COMPARATIVE ANALYSIS OF ECURITY ALGORITHMS FOR VANETS

Table 1 shows the comparative Analysis of Security Algorithms for VANETS

7.1. Prevention Measures for Existing Attacks

Table 2 shows the preventive measures for existing attacks.

Table 2. Preventive measures for existing Attacks.

Property Violated	Attacks	Preventive Measures
Privacy	Location trailing	ID based system
Availability	Denial of Service (DOS)	IP Info. Handling
	Routing attacks	Cryptography Hashing etc.
Integrity and confidentiality	Eavesdropping	Creation of cipher
	Replay	Time-stamping
	Bogus info.	Hashing, Asymmetric cryptography
Authenticity	Sybil	Radio resource testing, Registration, Position verification, etc.
	Impersonation	Trust authority, PK1
	Timing attack	Encryption solution (TPM)
	Session hijacking	Encryption, Random SID generation

Table 2. Preventive measures for existing Attacks

Authors	Title	Techniques /technology Used	Attacks Covered/ Security dimensions	Limitations of used technology
AkhileshSingh,et al.[25] (2016)	VANET security: Issues, challenges and solutions	Symmetric cryptography, digital signature, hash function, elliptical curve parameter and ID registration technique.	Replay attack, DOS, Routing attack, fake information attacks.	
Arturo Ribagorda, et al.[26] (2010)	Overview of security issues in vehicular ad-hoc networks	Vehicular public key infrastructure, certificate validation, encryption, plausibility check mechanisms.	Eavesdropping, Identity revealing, Location tracking, attribute- based DOS attack	These techniques hadn't addressed the issues on privacy problems due to radio frequency finger - printing
Shiang-Feng Tzeng, et al. [27] (2015)	Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET.	System initialization, anonymous identity generation, message signing, and message verification.	Forgery attack	Effective solution for forgery attacks only. No solution for other attacks.
Ahmed Shoeb Al Hasan, et Al .[28] (2016).	Security threats in vehicular ad hoc networks.	Public Key, Symmetric and Hybrid, Certificate Revocation , ID-based Cryptography.	Privacy and security	Good privacy schemes with reduced overhead but no solution for attacks.
Lu Chen, et al. [29] (2013)	Analysis of VANET Security based on Routing protocol Information.	Elliptic curve algorithm, digital signature technology, Intrusion Detection.	Integrity, reliability and confidentiality.	
Asif Ali Wagan, et al. [30] (2015)	Emerging attacks on VANET security based on GPS Time Spoofing	Prevention of Time Stamp Jumps, short lived pseudonym certificates and retrospective attack detection via logging.	Denial of service attacks, sybil attack	No solution for other attacks.
Ghassan Samara, et al.[31] (2010)	Security Analysis of Vehicular Ad-Hoc Network (VANETs)	Vehicular Public Key Infrastructure, group signature, Certificate Authority, ECC,	DOS attack, Fabrication attack, alteration attack, replay attack, message	
Ram Shringar Raw, et al. [33] (2013)	Security challenges, Issues and their solutions on VANETs	ARAN, SEAD, SMT (Secure Message Transmission), NDM (Non-Disclosure Method), ARIADNE	Replay Attack, Impersonation, False Warning, information disclosure, DOS, routing attack	Efficient privacy solution but no solution for confidentiality.

VIII. CONCLUSION

This paper has briefly introduced various aspect of VANET like its environment and standards, detailed explanation of various possible attacks in VANET have been classified depending on the availability, authentication, confidentiality, privacy, non-repudiation and data trust. Possible challenges associated with security attacks and security services are also highlighted. Since attack creates a more severe condition, it is necessary to analyze the effect of attack on routing protocols which makes more secure vehicular environment.

REFERENCES

[1] Javed Muhammad Noman et al., "VANET's Security Concerns and Solutions: A Systematic Literature Review," in *Proceedings of the 3-rd International Conference on Future Networks and Distributed Systems* (ICFNDS) ACM, pp. 1-12, July 1–2, 2019.

[2] Abdul Quyoom, "Security Issues of Vehicular Ad Hoc Networks in OSI layers," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* ISSN: 2456-3307, vol. 2, no. 4, 2017.

[3] Abu Talib, Manar, et al., "Systematic literature review on Internet-of-Vehicles communication security," *International Journal of Distributed Sensor Networks*, ISSN: 1550147718815054, vol. 14, no. 12, 2018.

[4]Abdul Quyoom, MohdSaleem, MudasserNazar, Yusera Farooq Khan, "VANETs Applications, Challenges and Possible Attacks: A Survey, "*International Journal of Advanced Research in Computer and Communication Engineering*, ISO 3297:2007 Certified Vol. 6, Issue 7, July 2017.

[5] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks, " IEEE

Transactions on Intelligent Transportation Systems, vol. 20, no. 5, pp. 1621–1632, 2019.

[6] Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, and HussienZedan, "A comprehensive survey on vehicular ad hoc network," *Journal ofNetwork and Computer Applications*, vol.37, no. 1, pp. 380–392, 2014.

[7]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.

[8] Abdul Quyoom, Raja Ali and Devki Nandan Gouttam, "A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)," in *Proceedings of the IEEE International Conference on Computing, Communication and Automation (ICCCA2015)*, pp. 414-419, 2015.

[9] Jafer, Muhammad, et al., "Secure Communication in VANET Broadcasting," *ICST Transaction on Security Safety,* vol.5, no.17, 2019.

[10] Karimireddy, T. and Bakshi, A., "*A* Hybrid Security Framework for the Vehicular Communications in VANET," in *Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET*), pp. 1929-1934, 2016.

[11]. J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1621–1632, 2019.

[12]Mishra R., Singh A. and Kumar R., "VANET Security: Issues, Challenges and Solutions," in *Proceedings of International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT*), pp. 1050-1055, 2016.

[13]Md Whaiduz-zaman, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, 2014.

[14] Sumra, Irshad Ahmed, Iftikhar Ahmad, HalabiHasbullah, and J-L. bin Ab Manan, "Classes of Attacks in VANET," in *Proceedings of Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, pp. 1-5, 2011.

[15] A. Festag. "Cooperative intelligent transport systems standards in Europe," *Communications Magazine, IEEE*, vol. 52, no.12, pp. 166–172, Dec. 2014.

[16] Hussain Rasheed, Fatima Hussain, and Sherali Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," *Journal of Future Generation Computer Systems*, pp. 843-864, 2019.

[17] Kumar Mr Kamal, and Rahul Malhotra, "Analysis of Sybil Attack Isolation Technique in VANET," *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 8, no. 5, pp.187–192, May 2019.

[18] Singh Avinash et al., "Implementing Security Services in VANET Using Cryptography Based on Artificial Neural Network," *Journal of Computer and Mathematical Sciences*,vol. 10, no. 9, pp. 1573-1584, 2019.

[19] Karagiannis D. and Argyriou A., "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol.13,pp. 56-63, 2018.

[20] Safi, Q.G.K., Luo, S., Wei, C., Pan, L. and Yan, G., "Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs," *Computer Standards and Interfaces*, vol.56, pp. 107-115, 2018.

[21]. J. Liu, Y. Yu, Y. Zhao et al., "An efficient privacy preserving batch authentication scheme with deterable function for VANETs," in *Proceedings of the International Conference on Network and System Security*, pp. 288–303, 2018.

[22] Usha M., Ramakrishnan B, "An enhanced MPR-OLSR protocol for efficient node selection process in cognitive radio based VANET,"*Wireless pers. Commun*. vol.106, no.2, pp. 763–787, 2019.

[23] Usha M., Ramakrishnan B, "A robust architecture of the OLSR protocol for channel utilization and optimized transmission using minimal multi point relay selection in VANET," *Wireless Pers. Commun. Now*, pp. 1–25, 2019.

[24]. K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *Cognitive Systems Research*, vol. 55, pp. 153–163, 2019.

[25]. A. Singh, R. Mishra and R. Kumar, "VANET security: Issues, challenges and solutions," *International Conference on Electrical, Electronics, and Optimization Techniques*, *pp. 1050-1055*, 2016.

[26]. A. Ribagorda, J. M. de Fuentes and A. I. Gonzalez-Tablas "Overview of security issues in vehicular ad-hoc networks," *Handbook of Research on Mobility and Computing,* IGI Global, 2010.

[27] Horng S., Tzeng S., Li T., Wang X., and Huang P., Khan M., "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET,"*IEEE Transactions on Vehicular Technology*, vol. 66, no. 4 (2015): 3235-3248.

[28] A. S. Al Hasan, Md. Shohrab Hossain, and Mohammed Atiq-uz-zaman, "Security threats in vehicular ad hoc networks," in *Proceedings of the Conference on Advances in Computing, Communications and Informatic*, pp. 21-24, Sept.2016.

[29] Chen, L., Tang, H., and Wang, J., "Analysis of VANET security based on routing protocol information," in *Proceedings of the Fourth International Conference on Intelligent Control and Information Processing*, pp. 134-138, Jun. 2013.

[30] A. A. Wagan, Bittl, S., Gonzalez, A. A., Myrtus, M., Beckmann, H., Sailer, S. and Eissfeller, B., "Emerging attacks on VANET security based on GPS Time Spoofing,"in*Proceedings ofthe IEEE Conference on Communications and Network Security*, pp. 344-352, 2015.

[31] G. Samara, Al-Salihy, W. A., and Sures, R, "Security analysis of vehicular ad hoc networks (VANET),"in *Proceedings of the Second International Conference on Network Applications Protocols and Services*, pp. 55-60 , Sep. 2010.

[32] Sung-Ki Kim, Byung-Gyu Kim, Byoung-Joon Min, "Reducing Security Overhead to Enhance Service Delivery in Jini IoT," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID. 205793, pp. 1-7, 2015.

[33] R. S. Raw, Kumar, M. and Singh, N., "Security challenges, issues and their solutions for VANET," *International Journal of Network Security & Its Applications*, vol. 5, no. 95, Sep.2013.

Authors

Abdul Quyoom has received B.Tech from BGSBU Rajouri, J&K in 2013 and he is awarded M.Tech from Central University of Rajasthan specialized in Information security in 2015 . He has five Publications and attended various National, international conferences and workshops. He has worked as an Assistant Professor in YCET Jammu and the department of Computer Science in BGSBU Rajouri. Currently he is pursuing Ph.D. from Department of Computer Sc. & IT, University of Jammu and working on Artificial Intelligence and its application in medical domain. His research interest includes medical image processing, intelligent image segmentation, and deep learning.

Aftab Ahmad Mir has done Masters in information Technology, with specialization in Optimization techniques, Artificial intelligence and machine learning from Department Computer Sc. & IT, University of Jammu. Now he is pursuing Ph.D. in Information Technology with specialization in Deep Learning. He has three years of teaching experience in teaching and has also worked in software industry. His research interests include artificial intelligence, medical image processing, intelligent image segmentation, algorithm design, and deep learning.

Dr. Abid Sarwar has been working in the field of application of Artificial Intelligence in Medicine (especially in cervical cancer and diabetes) for the last 08 years. He did Masters in Computer Applications from Department of Computer Sc. & IT, University of Jammu in 2009. He obtained PhD degree from Department of Computer Sc. & IT, University of Jammu in 2017. Besides He has published more than 15 research articles in leading journals, conference proceedings, he has created a database of 8,091 digitally calibrated cervical cells, which is the only research database available to work on cervical cancer based on Bethesda system of classification. His research interest includes medical image processing, intelligent image segmentation, and deep learning.