A REVIEW ON SECURITY TECHNIQUES IN VANETS

Mohit Balu¹, Gulshan Kumar^{2*} and Se-Jung Lim³

¹*Research Scholar, School of Computer Science and Engineering, Lovely Professional University, India*

²*Assistant Professor, School of Computer Science and Engineering, Lovely Professional University, India*

³*Department of Computer Engineering, Chonnam National University, Republic of Korea*
gulshan.16865@lpu.co.in

Abstract— Vehicular ad hoc network (VANET) is one of the most promising candidates for Intelligent Transport System (ITS). It is also an emerging application of Mobile ad hoc network (MANET). Along with its popularity it also comes with number of challenges such as security, routing and data dissemination. Lots of solutions are already proposed for these challenges but because of daily emergence of new threats and attacks, security requires more concern among all of these. Therefore, in this paper different security techniques proposed by the researchers have been discussed, along with the security services they have considered (Confidentiality, Integrity or Availability). Moreover, different security attacks have been discussed which the proposed solution mitigates. Furthermore, comparison of all these techniques have been done by taking some security parameters.

Keywords— VANETs, security, DSRC, threats, attacks

1. INTRODUCTION

With the modern pace of life, transportation system is getting advanced and becoming intelligent than ever before. Vehicular ad hoc Network (VANET) is one of the most promising candidate of Intelligent Transport System (ITS). VANETs is an emerging application of Mobile ad hoc networks in which vehicles are acting as mobile nodes [1]. It is gaining popularity because of some unique features it holds.

VANETs provides communication between moving vehicles to distribute the information about traffic, road conditions, weather conditions, accident information and other related information to deliver assistance for vehicle or for the driver of the vehicle. It can help vehicle to reduce the risk of accidents and other disruptions. There are different fields in VANETs upon which lot of research is pending such as routing protocols, security, architecture, challenges, standardization [2].

1.1. ARCHITECTURE OF VANETS

VANETs architecture is basically comprised of three types of domains [3-5] as shown in Fig 1. These domains are divided based on source and destination of information that is being communicated. These 3 domains are:

Received: January 4, 2019
Reviewed: March 28, 2019
Accepted: April 8, 2019

1. Mobile Domain
2. Infrastructure Domain
3. Generic Domain [6]

Fig. 1 Architecture of a Vehicular Ad hoc Network

1.1.1. MOBILE DOMAIN: Mobile domain basically deals with two types of components: Vehicle Component and Mobile Component. Vehicle components are moving vehicles such as cars, buses and other vehicles. Mobile Components are other movable components but are not the vehicles such as personal smartphones with GPS navigation moving on the road side. Fig 2 clearly shows the mobile domain and its components.

Fig. 2 Different domains in a Vehicular Ad hoc Network

1.1.2. INFRASTRUCTURE DOMAIN: Infrastructure domain is having those components which are not mobile but plays an important role in VANETs. These components are Infrastructure itself on the roads. It is also comprised of two types of components: Road Side Units (RSUs) and Central Infrastructure. RSUs are the sensors

deployed on the side of the roads to collect the information from moving vehicles taking part in the network. The main task of RSUs is to forward the collected data to other vehicles for their safety and assistance. RSUs can also send collected data to Central Infrastructure so that this data can be used for traffic signals, analytic purposes or traffic forecasting under certain conditions. Fig 2 clearly describes both the components of Infrastructure domain.

1.1.3. GENERIC DOMAIN: Generic domain deals with cloud and internet services. For dissemination and updating of information. Generic domain is comprised of two components: Private network and Internet. Private Network can be used to disseminate local information like traffic flow, accident information. Internet can be used to store the data on cloud for data analytics. Fig 2 clearly depicts the concept of generic domain in VANETs.

1.2. COMMUNICATION IN VANETS

VANET uses DSRC (Dedicated short-range communication) to communicate within the network because cars usually move at high speed and the information exchange between two entities should be completed in a short span of time. Within this limited period, a dedicated network must be created, and data must be transferred. Along with its security, personnel privacy must be maintained as well, which may include large calculations such as key pair generation. So, in a VANET several small networks are being created and information is being exchanged within a small period along with taking care of data security and driver's privacy. There are 3 types of communication in VANETs as shown in Fig 3.

1. Vehicle-to-Vehicle Communication
2. Vehicle-to-Infrastructure Communication
3. In-Vehicle Communication

1.2.1. VEHICLE-TO-VEHICLE COMMUNICATION: Vehicle-to-Vehicle communication also known as V2V communication, holds the most important part of a VANET. Fig 2 has described V2V communication. When two moving vehicles connects with each other using wireless communication for the short span of time to exchange information until they are in contact is called V2V communication.

It usually is comprised of exchange of warning messages such as traffic jams to predict the delay time, road conditions to make the driver careful about speed, accident information to provide first aid assistance.

1.2.2. VEHICLE-TO-INFRASTRUCTURE COMMUNICATION: Vehicle-to-Infrastructure communication also known as V2I communication, is the communication between mobile vehicle and Road Side Units (RSUs) until the time they are in contact with each other. RSUs and vehicles exchanges information about parking lots and weather updates. Vehicle sends the recorded data to RSUs and RSUs sends collected data to another vehicles.

Fig 3. Different types of communication in a Vehicular Ad hoc Network

1.2.3. IN-VEHICLE COMMUNICATION: Another type of communication is In-vehicle communication. It is different from other two types of communication. It happens inside the vehicle only, by using wireless communication. Mainly there are two components in vehicle which are important for taking part in VANET, which are OBU (On-Board Unit) and AU (Application Unit).

Vehicle which takes part in VANETs have some sensors embedded in those vehicles. Those sensors record the real data which is communicated. These sensors are GPS, digital compass, vibration sensors, parking sensors, temperature and other weather sensors. These set of sensors are called On-Board Unit.

Application Unit segregates and uses the data provided by OBU and process it to disseminate to other parts of VANET. Communication between OBU and AU is called In-vehicle communication (Fig 3). In-vehicle communication also identify driver's fatigue, drowsiness and vehicle's performance.

1.3. ROUTING IN VANETS

Data collected by vehicles may have specific destination or route based on which some routing protocols have been proposed and already been implemented in VANETs. The task of routing is to find the optimal path to send the data to destination so that least time is consumed.

Reader might be aware about routing used in conventional networks, but in VANETs routing is somewhat different because of two reasons. First is the architecture of VANETs, because networks in the VANETs are dynamic, it changes rapidly, and its lifetime is only for a short period of time. Second reason is are resources which are limited in case of VANETs as compared to conventional networks. Three types of routing are discussed as following:

1. Geocast / Broadcast
2. Multicast
3. Unicast

1.3.1. GEOCAST/BROADCAST: It includes the data which is to be broadcasted to every vehicle taking part in the VANET. It may include weather information or information about environmental factors like temperature, pressure, wind speed and direction.

1.3.2. MULTICAST: It includes data which is to be sent to a group of vehicles. It may be the data from services which the vehicle owner has subscribed.

1.3.3. UNICAST: The data which is to be sent to the individual vehicles such as warning signal of drowsiness of driver, drunk driver or bad performance of a vehicle will be routed by the unicast routing.

1.4. SECURITY IN VANETS

Security is the main aspect for which this detailed review of VANETs has been done by the author.

There are 3 types of security services which fulfill the security triad. Most of the researchers focus on any one service to improve VANETs' security partially. But some of the researchers have also worked on complete triad to improve VANETs' security collectively [7]. These security services are Confidentiality, Integrity and Availability. These 3 services complete the security triad. Apart from these three, there are some more services which are also held responsible for security of VANETs. These services are Authentication, Authorization (Access Control) and Non-Repudiation. Some of the researchers have also worked on these services.

There are number of challenges in VANETs security which have been discussed in Literature Review. Different types of attacks and solutions proposed by the researchers have also been discussed.

The rest of the paper is organized as follows. Section 2 reviews the existing literature about VANETs' security. Section 3 represents the comparison table among reviewed literature. Section 4 represents the future scope of existing security methods and finally Section 5 concludes the paper.

2. LITERATURE REVIEW

Different authors have discussed about different aspects of VANETs security in their researches, including Modification of data, Exhaustion of VANET services and Privacy of drivers and their proposed solution and their advantages has been discussed.

2.1. DIFFERENT THREATS TO VANETS SECURITY

There are different types of threats which hinder security services of a System. Threats such as DoS attacks, Malware and Spamming are threat to Availability of the data.

DoS (Denial of Service) attack makes a network non-usable to its connected nodes by any means like sending jamming signals in the form of radio waves to de-authenticate connected nodes or by flooding the nodes with fake messages. These types of attacks are mostly performed by insiders, but outsiders also perform it to create disruptions. Flooding refers to generating large no of fake packets to disrupt the services of system, so that the real users can't use the services. Jamming means creating interference on the same channel on which service is running to cancel the radio waves generated for transmission of data.

Malware, like worms and viruses, that are injected into the VANET may cause some serious disruptions to the working of VANETs. Because the On-Board Units (OBUs) and Road Side Units (RSUs) usually get some sort of updates like software update, firmware upgrade and or some bug fixes, then these Units are vulnerable to malware which may come along with the update, encapsulated by outside attackers.

Spamming is also a threat to availability, since spam messages can cause overhead for system and create latency delays because of limited resources of VANETs.

Masquerading, Re-play attack, GPS Spoofing, Black hole attack, Broadcast and Transaction Tampering are some threats to Authenticity, because it may spoof the fake

node as authenticated node and they will become the part of the network and play malicious things which may breach the security of whole system.

Outsider and Insider eavesdropping, Location tracing are threats to confidentiality of the system, because attacker may intercept the messages which are supposed to reach at some other vehicle. Most critical thing is location tracking which clearly breach the privacy of the driver and his habits [8]. Laurendeau and Barbeau has identified these threats according to European Telecommunication Standards Institutes.

2.2. CONFIDENTIALITY IN VANETS

Confidentiality refers to readability of message only to the node for which it is supposed to. No other node should be able to read the message intended for some other node. This may be achieved by secret key cryptography or public key cryptography, but again generation of keys creates an overhead for the system. There may be outside attacker inside the network range or a malicious vehicle inside the network which may try to intercept the messages not intended for them. Intercepting someone others' messages is as simple as receiving your own message. Attacker, however should not be able to read it by any mean, which achieves confidentiality in the system. If they are able to read it by any means, the concept of confidentiality gets vanished. So, there should be reliable mechanism in VANETs which can help us to preserve the confidentiality of the messages.

Relevance based approach in VANETs for prioritizing important \& urgent messages and removing redundant \& surplus message is based only on ideal conditions. But in real life ideal conditions are not always possible, so this approach may be vulnerable to malicious attacks.

There may be some malicious nodes or selfish nodes in the network which may trick the system to discard important messages and forward unwanted messages. It may also breach the confidentiality of the system by remaining into the network and capturing communication. *e.g.*, Personal Identification of driver may be used for malicious purposes.

So, relevance-based approach is not suitable for preserving the confidentiality of the system [9]. Rahim and Muhaya observed that global benefit has been decreased using relevance-based approach.

Most of the applications of VANETs are location dependent. So, the accurate location information is required by the system. However, if there are attacker within the network, they may manipulate the location or forward the false location. It might spread the wrong information over the network. This false information can also be spread by malicious vehicle sending bogus messages. In order to avoid this an intrusion- tolerant location system should be introduced [10].

Yan, Yang, Shaner and Rawat implemented a technique to detect and filter the false location information. Their algorithm refines low resolution location information and estimates high resolution information using multi granularity deviation factor. In fact, it also provides accuracy by refining location information.

2.3. AUTHENTICATION IN VANETS

Authentication in VANETs refers to mechanism of allowing only authenticated nodes in the system. Authenticated nodes are those nodes whose identity is confirmed and are not fake nodes. Authentication mechanism in VANETs prevents the system from number of attacks, because malicious nodes gets filtered out and are not allowed to take part in the network. Attackers may try to inject malicious nodes in the network using fake identities called impersonation. Researchers have proposed different mechanisms for identify trusted node and removal of malicious nodes from the network.

Trust Establishment is a challenging task due to lack of infrastructure and high-speed mobile nodes causes frequent changes in the network topology. High speed vehicles in large numbers and dynamic topology of the vehicular ad hoc network makes authentication task difficult.

Dasgupta, Chaki and Choudury in their work have proposed TruVal, a trust value mechanism for authentication of vehicle for secured communication in VANETs [11]. They have used a layered framework for assigning a trust value to vehicle which helps in detecting a node taking part in malicious activity. A vehicle must have a desired trust value and be registered under an authorized registration authority for accessing the network.

A vehicle must be registered using registration mechanism and trust value gets assigned to each registered vehicle. After registration there should be a trust value updating mechanism for existing vehicles.

Use of signatures is a good method to check authenticity of the nodes. Every node which sends a message will sign that message with its digital signature, leaving its identity with the message they have sent. It removes the requirement of use of certificates for authentication. But again, digital signature can create an overhead on the system. Instead of using certificates and signatures aggregate signature mechanism can be used which will greatly save other resources and bandwidth as well [12].

Zhong, Han, Cui, Zhang, Xu have proposed this aggregate signature-based mechanism for preserving the authenticity of the system. When a vehicle enters into RSUs range some calculations are pre-computed rather than calculating during the communication. Length of aggregate signatures are constant which reduces the communication and storage overhead.

Chikhaoui, Chehida, Abassi, Guemara El Fatmi [13] has proposed ticket-based authentication mechanism in their work. A temporary ticket will be assigned to the vehicle to communicate. Only that vehicle can communicate who is having ticket and it will be used with message during transmission. It will ensure non-repudiation in the system in case of any malicious activity and culprit can be traced and removed from the network.

2.4. ACCESS CONTROL IN VANETS

Access control or Authorization means allowing only particular set of nodes to access some data which is not accessible to all other authenticated nodes even.

This can be achieved by enabling attribute-based encryption that Rao and Dutta [14] have proposed in their work. Conventional access control methods are expensive in terms that cipher-text length grows linearly with the number of attributes in the access policy and for decryption. In their research they have used a constant number of pairings which are needed for decryption. Access control in VANETs was introduced by Huang and Verma [15] based on cipher-text policy attribute-based encryption. Rao and Dutta have designed a computationally efficient access control scheme with low communication overhead for VANETs.

2.5. AVAILABILITY IN VANETS

Availability in VANETs means all the resources and services are available for the users as they have requested. It is a conventional method of working of a network that its resources should be readily available to the all the intended users. But attackers in the network may try to consume all the resources by some methods to make the resources unavailable for all other authenticated users. This is called Denial of service attack (DoS attack). Attackers load the resources with unwanted queries and system stops responding creating unavailability of the resources. Sometimes attackers may use authenticated nodes for denial of service attacks by malfunctioning them. In this method, several

authenticated nodes simultaneously request the system resource, and the system gets in irresponsible state. This is called Distributed denial of service attack (DDoS attack).

When malicious node spoofs a large number of fake identities i.e. IP address, it hinders the proper functioning of the data transfer between two fast moving vehicles [16]. If an attacker forges multiple identity of nodes i.e. uses spoofed IP addresses, it exhausts the network by disseminating fake packets and make it deny allowing requests made by authenticated users [17].

Verma, Hasbullah and Kumar have analyzed fake identities of malicious nodes with the help of consistent existing IP address information scheme. If some nodes observe that they have similar IP address it is identified as DoS attack. They have proposed the approach which will be able to locate malicious nodes without any secret key information exchange and special hardware support. There may be various attack pattern for DoS attack such as Sybil attack, Fabrication attack, Alteration attack and replay attack.

Targeted vehicles can be exploited with vulnerability and turned into malicious node called zombies or slaves. Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, Nazar A. Saqib have proposed detection and prevention of DDoS attack by keeping check in on the number of packets injected into the network.

2.6. C-I-A IN VANETS

Confidentiality, Integrity and Availability are the prime aspects of security. It should be fulfilled at utmost priority to complete the security requirements of the any system. Similarly, in VANETs CIA triad must be accomplished in order to have secure communication.

Most of researchers refine any one of the CIA services in order to enhance VANETs' security. But some of the researches also have worked on complete CIA triad collectively to improve security in VANETs. Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, Tai-Hoon Kim [7] in their research have worked on CIA triad to mitigate potential attacks and have used hierarchical model to utilize minimum number of message exchange. They have proposed ECC (Elliptic Curve Cryptography) for Confidentiality and End-to-End Authentication for Integrity and Availability. For the security of downloaded services, they also have proposed sand-boxing mechanism.

3. COMPARISON OF DIFFERENT SECURITY TECHNIQUES

A comparison has been done between 10 different papers proposing different security techniques that can be used in VANETs. Security services that the author has considered in their proposal has also been mentioned along with its advantages. A Comparison table has been created for comparing different security techniques in Table I.

Table I. Comparison Between Different Security Techniques In VANETs

Sr. No.	Paper	Targeted Security Service(s)	Proposed Technique(s)	Advantage(s)
1	Multidimensional Security Provision for Secure Communication in Vehicular Ad hoc Networks using Hierarchical	Confidentiality, Integrity, Availability	The authors have proposed a solution for VANET security using CIA triad to mitigate potential attacks and they have proposed hierarchical model to utilize minimum number of	1. The proposed solution is less costly and can provide better security than existing algorithm. 2. In comparison with existing algorithm,

	Structure and End-to-End Authentication [7]		messages exchange. They have proposed ECC for Confidentiality, End to End Authentication for Integrity and Availability. They have proposed use of sand-boxing for security of downloaded service.	transmission delay is lesser. 3. In proposed solution, processing time for resolving the query from multiple vehicles has been reduced significantly in reference.
2	Intrusion Tolerant Location Information System in VANET [10]	Integrity	The author has proposed an adaptive algorithm for computation of high resolution location information by refining low resolution location information using multigranularity deviation factor to detect and filter false location information injected by the intruders from given noisy inputs by the vehicles.	1.Filters false location information. 2.Compute high resolution location for further use. 3.Improve accuracy of filtering and location estimation. 4.Don't need any probability distribution of input samples.
3	Computationally Efficient Secure Access Control for Vehicular Ad hoc Networks [14]	Authorization/ Access Control	The author has proposed the use of constant number of pairings during encryption and decryption for access control, while having a significant improvement in the communication overhead using an existing distributed ABE scheme.	1.Computationally efficient as it uses only a constant number of pairing computations during encryption and decryption. 2. The length of cipher-text is linear in the number instead of number of attributes in the access policy, which means that their design has Low communication overhead as compared to the other's works in this field. 3. Proposed scheme is collision resistant and is proven to be secure

				in generic group model.
4	TruVAL: Trusted Vehicle Authentication Logic for VANET [11]	Authentication	The author has proposed trusted vehicle authentication scheme for secured communication in VANET using layered framework. A trust estimation mechanism is also proposed for calculation of trust value for existing vehicles.	<ol style="list-style-type: none"> 1. Malicious nodes can be easily avoided during communication. 2. TruVAL results in lesser number of packet drops and lesser end-to-end delay. 3. The layered structure helps to diminish the problems of centralized mechanisms such as performance bottlenecks.
5	Prevention of DoS Attacks in VANET [16]	Availability	The author has proposed the mechanism to analyse forged identities of malicious vehicles with the help of consistent existing IP address information. If similar IP addresses are found on multiple vehicles, it is identified as DoS attack.	<ol style="list-style-type: none"> 1. Proposed approach is able to filter the IP packets based on identification. 2. Any malicious vehicle taking part in DoS attack can be easily traced back with the help of proposed method. 3. Given method is also able to prevent small scale and large-scale DoS attacks.
6	Detection and Prevention of Distributed Denial of Service Attacks in VANETs [17]	Availability	The author has proposed a method to differentiate between an attacker and a normal node based on comparison of their communication period within a threshold time and basically keeping a check on the number of packets being injected into the	<ol style="list-style-type: none"> 1. Proposed method is capable of minimizing the flooding of packets efficiently. 2. Packet delivery ratio of proposed algorithm is better than the existing algorithms in the field. 3. The proposed method of this

			network.	paper causes almost no overhead on the network resources.
7	Privacy-Preserving Authentication Scheme with Full Aggregation in VANET [18]	Confidentiality	The author has proposed certificate-less aggregate signature based mechanism to achieve message authentication without creating overhead for system resources.	<ol style="list-style-type: none"> 1. Proposed method use aggregate signatures which provide authentication and does not create overhead by creating signature for individual messages. 2. Length of aggregate signatures is constant which reduces the communication and storage overhead. 3. Proposed mechanism uses the pre-calculation method to reduce the computations during sign phase.
8	A Ticket-Based Authentication Scheme for VANETs Preserving Privacy [13]	Authentication, Confidentiality	The author has proposed the scheme based on the use of temporary tickets to retain the privacy of the vehicles and use of identity-based signature mechanism for authentication of nodes in VANET.	<ol style="list-style-type: none"> 1. Proposed method is resistant to Impersonation and Identity resolution attacks. 2. Each message is signed by the nodes, retaining nonrepudiation in the system. 3. In given scheme, each vehicle has in its own set of credentials and only one credential (ticket) can be used for each time slot. So, malicious node cannot perform DoS attack.
9	EIAS-CP: New efficient identity-based authentication	Integrity, Confidentiality	The author has proposed to use Identity-based signatures to ensure	1. The computation cost decreases dramatically by using Elliptic

	scheme with conditional privacy preserving for VANETs [19]		reliability and integrity of messages for vehicle-to-vehicle communication and vehicle-to-infrastructure communication with conditional privacy preserving, constructed on ECC (Elliptic curve cryptography).	curve cryptography and batch verification of multiple messages. 2. The proposed scheme satisfies all the security and privacy requirements for VANETs. 3. The computation cost of verification and message signature is reduced by 93% and 88% respectively.
10	D&PMV (Detection and Prevention of Malicious Vehicles): New Approach for Detection and Prevention of Misbehave/ Malicious Vehicles from VANET [20]	Authentication	The author has proposed misbehaviour Detection scheme for detecting malicious vehicles using the monitoring process over the VANET and application of proposed algorithm to prevent those malicious nodes.	1. Detection of malicious vehicles can detect malicious vehicles prior to the number of dropped or duplicated packets becomes greater than a given number of drops or duplicates. 2. In proposed method a distrust value has been introduced that can be used to determine trustworthiness value of each vehicle when it forwards the message. 3. Proposed algorithm is able to improve the performance of verifier selection at high speed.

4. FUTURE SCOPE OF SECURITY TECHNIQUES IN VANETS

Number of researchers have provided different solutions to enhance important parameters regarding security of VANETs. Researchers also have optimized their solutions to ensure less consumption of resources. Still there is always a scope of improvement in this field because of limited resources and short span of time. Most of the

time security functions requires heavy resources due to large operations. So, there are some ideas that may enhance secure communication in VANETs.

4.1. INTEGRITY IN VANETS

There is a research gap in the field the Integrity in VANETs. A lot of research is yet to be done for Integrity of received messages. Most of researches have worked on Confidentiality and Authentication for mitigation of malicious and selfish nodes. Availability is also somewhat dependent on Authentication especially in VANETs, this is because dynamically changing topology due to which only authenticated nodes can perform denial of service attacks in VANETs for so long time. Outside attackers cannot remain connected to same network for so long. But Integrity of messages should also be preserved to prevent dissemination of misleading information which may lead to huge loss in terms of traffic management system or vehicle safety.

Integrity can be ensured by hashing. In VANETs hashes need to be precalculated because of limited time. There is merely a chance of hash collision because data transmission is done in lesser time than an average time to crack a hash. So, there is a scope of use of hashing in VANETs for integrity. To take an extra benefit small length hashes may be used to save the consumption of resources.

4.2. NON-REPUDIATION IN VANETS

There should be some sort of mechanism to keep a record of message transactions. Somehow, if some false information is spread by some malicious node or vehicle and some loss happens, there must be a method to trace the culprit. This ensures Non-repudiation in system. Although, like conventional network system, digital certificates are not possible due to ad hoc property of VANETs. There is no central mechanism to take care of signatures of nodes, but Infrastructure can be used to take care of these uncovered things. Infrastructure has a benefit of ample resources, so there is possibility of use of central management system, traffic management system for ensuring non-repudiation in VANETs.

4.3. MORE APPLICATIONS

Although there are lots of application of VANETs, that is the prime reason of its popularity. Several applications can still be designed with use of VANETs for safety of human beings. Using In-vehicle communication, sensors can be used detect and identify to identify drunk drivers and nearby vehicles can be informed with immediate distribution of messages using RSUs. It can insure people's and vehicle's safety.

In another application, accidental information can be transmitted to nearby ambulances and police stations with RSU's rather than using Infrastructure for immediate actions and victim's safety. As soon as vehicle enters accident prone area, driver should be informed to take careful actions for his and vehicle's safety.

Vehicles may be forced to be driven at limited speed depending on the area, for example near to school, vehicles must be driven at reduced speed to avoid accidents, pressure horn must be reduced near to the hospitals. To force this, a trust value mechanism should be maintained, and that value can be used to resolve accidental conflicts under certain situations.

So, there are number of such application other than these which may be designed to increase the popularity of VANETs and its applications.

5. CONCLUSION

VANET will become an important asset for Internet of Things and Intelligent Transport System in near future. For this to happen, we must ensure its security for safety of people and vehicles. The presented paper is an extensive overview of VANETs Architecture and different Security Techniques proposed for VANETs. Targeted Security Services in existing literature has been discussed with benefits of the proposed solution. A short comparison between different security challenges and their solution has been done. Finally, some ideas for security of VANETs has been discussed which may give direction to research in near future. Therefore, presenting VANET as a trustworthy and safe vehicle assistant for improved transportation system.

REFERENCES

- [1] Sivasakthi, M., and S. R. Suresh. "Research on vehicular ad hoc networks (VANETs): an overview." *International Journal of Applied Science and Engineering Research* 2.1 (2013): 23-27.
- [2] Liang, Wenshuang, et al. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." *International Journal of Distributed Sensor Networks* 11.8 (2015): 745303.
- [3] Maier, Mark W., David Emery, and Rich Hilliard. "Software architecture: Introducing IEEE standard 1471." *Computer* 4 (2001): 107-109.
- [4] Maier, Mark W., David Emery, and Rich Hilliard. "ANSI/IEEE 1471 and systems engineering." *Systems Engineering* 7.3 (2004): 1-23.
- [5] Emery, David, and Rich Hilliard. "Every architecture description needs a framework: Expressing architecture frameworks using ISO/IEC 42010." 2009 Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture. IEEE, 2009.
- [6] Timo Kosch, Christoph Schroth, Markus Strassberger, and Marc Bechler. *Automotive internetworking*. Vol. 4. John Wiley & Sons, 2012.
- [7] Kumar, Gulshan, et al. "Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication." *IEEE Access* 6 (2018): 46558-46567.
- [8] Laurendeau, Christine, and Michel Barbeau. "Threats to Security in DSRC/WAVE." *International Conference on Ad-Hoc Networks and Wireless*. Springer, Berlin, Heidelberg, 2006.
- [9] Rahim, Aneel, and Fahad bin Muyaha. "Impact of Malicious Node on Broadcast Schemes." *International Conference on Security Technology*. Springer, Berlin, Heidelberg, 2009.
- [10] Yan, Gongjun, Weiming Yang, Earl F. Shaner, and Danda B. Rawat. "Intrusion-tolerant location information services in intelligent vehicular networks." *International Conference on Intelligent Computing and Information Science*. Springer, Berlin, Heidelberg, 2011.
- [11] DasGupta, Suparna, Rituparna Chaki, and Sankhayan Choudhury. "TruVAL: trusted vehicle authentication logic for VANET." *International Conference on Advances in Computing, Communication and Control*. Springer, Berlin, Heidelberg, 2013.
- [12] Zhong, Hong, et al. "Privacy-preserving authentication scheme with full aggregation in VANET." *Information Sciences* 476 (2019): 211-221.
- [13] Chikhaoui, Ons, Aida Ben Chehida, Ryma Abassi, Sihem Guemara, and El Fatmi. *Ad-hoc, Mobile, and Wireless Networks* 6811, (2011): 77-91.
- [14] Xue-wen, Wu, Yan Wei, Song Shi-ming, and Wang Hui-bin. *For vehicular Ad Hoc networks* (2010): 294-309.
- [15] Huang, Dijiang, and Mayank Verma. "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks." *Ad Hoc Networks* 7.8 (2009): 1526-1535.
- [16] Verma, Karan, Halabi Hasbullah, and Ashok Kumar. "Prevention of DoS attacks in VANET." *Wireless personal communications* 73.1 (2013): 95-126.
- [17] Shabbir, Munazza, et al. "Detection and Prevention of Distributed Denial of Service Attacks in VANETs." 2016 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2016.
- [18] Zhong, Hong, et al. "Privacy-preserving authentication scheme with full aggregation in VANET." *Information Sciences* 476 (2019): 211-221.
- [19] Xie, Yong, et al. "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs." *Telecommunication Systems* 65.2 (2017): 229-240.
- [20] Kadam, Megha and Suresh Limkar. *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications* 515 (2017): 293-303.