IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

VANETs Applications, Challenges and Possible Attacks: A Survey

Abdul Quyoom[1], Mohd Saleem[2], Mudasser Nazar[3], Yusera Farooq Khan[4]

Department of Computer Science, BGSBU, Rajouri, India[1]

Department of Computer Science Engineering, BGSBU, Rajouri, India[2,4]

Department of Information Technology, BGSBU, Rajouri, India[3]

Abstract: Vehicular Ad hoc Network (VANET) is an emerging sub-class of MANET. Recently VANET have emerged to turn the attention of researchers in the field of wireless and mobile communications. It is distinguished from other kinds of ad hoc networks by their hybrid network architectures, node movement characteristics, challenges and new application scenarios. It cellular technology to achieve intelligent inter-vehicle communications and improve road traffic safety and efficiency. Intelligent transportation and active security are important applications of VANET, which need suitable vehicle-to-vehicle communication and vehicle and roadside infrastructures technology, especially routing technology. It poses many unique networking research challenges and the design of an efficient routing protocol for VANETs is very crucial. The mobility models are used during the simulation of protocols. Routing protocols are design to address challenges, which includes heterogeneous networks, random topology and high mobility of nodes. They should generate movement pattern which reflects real world behaviour of vehicles on the roads. It has a very high dynamic topology and constrained mobility which makes the traditional MANET protocols unsuitable for it. In this article, we discuss some challenges, applications and various kind of attack with respect to security principles.

Keywords: VANET, routing protocols, possible attacks, Security.

I. INTRODUCTION

VANETs are considered as a sub-class of mobile ad-hoc networks (MANETs) [1], due to some similar characteristics they possess such as infrastructure independence, self-organization and management, low bandwidth and short-radio transmission range. However, existing MANET routing protocols cannot be applied directly in VANETs, and when deployed in VANET environments result in poor route convergence, low communication throughput and frequent route disruptions. This is mainly due to the high mobility of vehicles and the dynamic network topology of VANETs [2][3]. This technology is primarily developed to enhance road safety and provide traffic efficiency. VANETs allow vehicles not only to communicate between them (V2V), but also with an installed infrastructure (V2I), which enables a variety of interesting applications. These applications can be ranging from safety-related applications, such as collision warning and emergency reporting to non-safety applications like infotainment [2]. In VANETs, network topology is highly dynamic due to fast movement of vehicles, and topology is often obstructed by road structure. Vehicles are likely to encounter many obstacles such as traffic lights, buildings, trees, and road junctions, which result in poor channel quality and connectivity. Safety-related applications are usually based on beaconing i.e. the process of periodically broadcasting safety messages. Safety messages include sensitive information about the current state of vehicles such as their identifiers, positions, and velocities. The encryption of these messages is not recommended since many VANETs' participants are concerned by them [8]. VANET provides intelligent transportation systems (ITS) [3]. The ITS, aiming to improve the safety and efficiency of transportation systems, supports two types of wireless communications: long-range and short-range. Long-range communication mainly relies on the existing infrastructure networks, such as cellular networks. Short-range communication, on the other hand, is based on emerging technologies such as IEEE 802.11 variants, and forms an ad-hoc network that comprises mobile vehicles and stationary roadside equipments, collectively referred to as vehicular ad-hoc networks (VANETs) [3].

In addition, decrypting safety messages can add a latency in the processing of them, which may not meet with real-time requirements of safety-related applications [12]. However, due to security threats such as false data injections, disseminated messages modifications, and reply attacks, safety messages must be authenticated. The aim of safety messages is to make vehicles aware about their surrounding environment, which significantly improves road safety. For example, using these messages, vehicles can expect or detect dangerous situations that can cause serious damages on VANETs such as collisions and accidents. As a result, vehicles can then make decisions to prevent such bad consequences. However, although, safety messages are beneficial for road safety, they may also be exploited by adversaries for unauthorized location tracking of vehicles [10]. It can then collect these safety messages and determine

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

the locations visited by vehicles over time. The location tracking of vehicles could violate driver's privacy since one vehicle is usually associated only to one driver [10]. Therefore, knowing vehicle's position can lead to disclosure critical information about driver's life.

II. ANET ARCHITECTURE

In VANET technology, moving vehicles are used as nodes and the network structure is mobile in nature. Though it is a subclass of mobile ad hoc network (MANET), the characteristics and features of VANET are different [12].

2.1 System Architecture

VANET system can be partitioned into three domains according to the IEEE 1471-2000 and ISO/IEC 42010 Architecture standard guideline.

- Mobile Domain
- Infrastructure Domain
- Generic Domain

Mobile Domain

Mobile domain is also divided into two parts. First, Vehicle domain consisting of all kind of vehicles, second, Mobile device consisting of all kind of personal navigation devices.

Infrastructure Domain

The infrastructure domain is also divided into two parts. First, Roadside infrastructure domain consisting of roadside unit entities like traffic lights. Second is, central infrastructure domain consisting of infrastructure management centres and vehicle management centres [9].

Communication Architecture

This architecture plays a vital role in VANETs architecture shown in fig 1. This can be categorized into four types [12].

1. In vehicle communications: Using this communication system, vehicle's performance specially driver's fatigue and drowsiness can be measured.
2. Vehicle to vehicle communications: Drivers can share information and warning message by using this communication system.
3. Vehicle to road infrastructure: Drivers can get real time traffic update or weather update using this V2I communication system.
4. Vehicle to broadband cloud: Using this communication system vehicle can communicate via wireless broadband. This type of communication can be useful for active assistance and vehicle tracking Drivers can get real time traffic update or weather update using this V2I communication system.

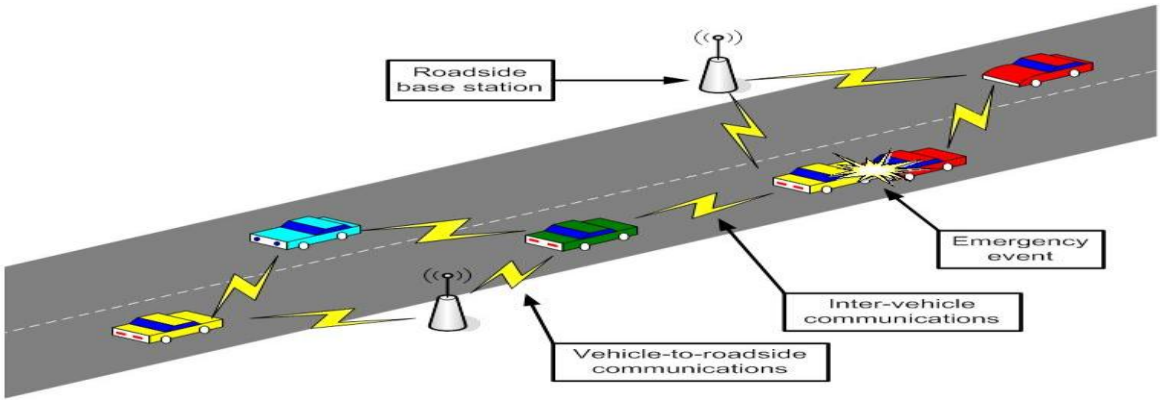

Fig 1: VANET Architecture

III. EXISTING WORK

Survey work in [3], [8], [11], and [12] give detailed overviews of VANETs. Work in [13] and [14] discuss the characteristics and challenges of routing in VANETs, general classification of routing protocols. Goudarzi et al. [1] presents a methodical literature review to provide complete and balanced material about various present trust conceptions in VANETs to upsurge excellence of data in transportation. The authors proposed a Trust model using the fuzzy logic to detect the misbehaviour nodes. The authors also stated that there is no lightweight intelligence trust model available for VANETs that satisfies all the desired properties of a trust model. Rabayah et al. [2] proposed a

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

routing protocol for VANET which associates the features of location based and topology based routing protocol. They integrate the protocol in such a way that if the location information is degraded, it automatically uses the reactive routing protocol to transmit the packet from the source to the destination. The author state the protocol is accessible and scalable and has an overhead over the new scalable Hybrid Routing does not include any Trust model to reduce the selfish nodes. Pophali et al. [4] proposed a trusted opportunistic routing protocol for VANET to improve the communication security and to safeguard the network from mischievous nodes. The author derives the minimum cost opportunistic routing to calculate the node cost to forward the packet from the source node to the destination. The malicious node has been strictly restricted from joining the network. Here, there is a chance of selfish nodes can be present in the network which restricts the transmission from the source to the destination vehicle. Wu et al. [6] proposed a new trusted routing protocol in VANET based on GeoDTN+Nav by using a greedy model which is associated with the four steps for initializing the routes, trusted routing establishment and the deletion of routes. As the greedy model [6] has more communication overhead, this model larger number of route discovery to establish the trusted route. In Yang [9] framework, the author describes a correspondence mining technique which is used for classifying similar information or same vehicles. The author proposed a reputation evaluation algorithm based on similarity theory. The reputation of each vehicle has been derived from the recommendation of other vehicles based on the weights calculations are made on which the selfish nodes are and other malicious nodes create a confusion instead of a reference given to a particular vehicle waiting for the reputation values.

The main characteristics of the VANET are the infrastructure absence, such as existence of Wi-Fi, GSM, access point or base station and Wi-Max. Communication between nodes that lies beyond the transmission of radio signals is made in multi hops. Due to self oragniseined network topologies, vehicle can move dynamically. On the other hand in the absence of infrastructure and the multi hopes routing transforms these networks in posses various types of attacks, such as modification of messages, eavesdropping passive of the massage until active interference with creation

IV. APPLICATIONS

VANET applications can be classified into four categories [11] [12].

1. DRIVING IMPROVEMENT

Such applications aid in improving traffic efficiency and management. Driving improvement applications update local information and street-maps. These applications would decrease congestion on the road and maintain a smooth flow of traffic, thus cause to increasing the capacity of the roads and preventing traffic jams. It also could have the indirect effect of reducing traffic accidents [13]. Some of applications are: road guidance and navigation, traffic information services, traffic assistance, left turn assistant, GPS Correction, Visibility Enhancer, Cooperative Collision Warning, cooperative cruise control, Banning the vehicle driver's license if violates numerous traffic laws and submit a report to the police officer, tracking the offender vehicle, tracking car thieves, Cooperative Vehicle-Highway Automation System and traffic coordination.

2. PUBLIC SERVICE

These applications support the work of public services such as police, ambulance and other emergency units. Usage of virtual sirens or signal pre-emption enables the emergency units to reach their destination faster [5]. Other public services include traffic surveillance applications such as electronic license plate.

3. COMFORT SERVICES

These services provide infotainment applications to drivers and passengers, either by enabling passengers to communicate with each other or by offering entertainment services such as internet connectivity and media downloading. These applications are also used for commercial purposes such as advertisements and electronic toll [3]

4. SAFETY

Road safety applications send warning messages to drivers about dangerous situations in order to make driving safer. Serious situations may include dangerous road features [7]. According to the vehicular safety communication consortium, there are eight safety related applications: pre-crash sensing, curve speed, lane change, traffic signal violation, emergency electronic brake light and cooperative forward collision alert, stop sign movement and left turn assistance assistant. One possible future safety application is to collect drivers behavioural and physiological information recorded by sensors located at various parts of the driver's body through in-vehicle communication, and then, transmit the data to a monitoring centre using vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Warning signals are sent to driver and the authorities in case of driver's abnormal health conditions. Apart from this, other safety related applications, such as overtaking vehicle warning, emergency vehicle warning, hazardous location notification and control loss warning. Since these applications are critical, their messages should have a deep penetration across the entire network and must be reliably delivered within a short time.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

A. Hard safety applications:
These are avoiding dangerous crashes or at least minimizing the damage if crashes are unavoidable. Example of hard safety applications are emergency electronic brake light (EEBL) that broadcast messages for neighbouring vehicles of a hard braking manoeuvrer specially when obstacles are blocking the line of sight of the driver, intersection movement assist (IMA), Lane Change Warning, Pedestrian Crossing Information and Approaching Emergency Vehicle Warning and Blind Spot Warning.

B. Soft safety applications:
These applications are less time critical in comparison with hard safety applications. Examples are applications that warn the driver about weather, road, traffic, and other hazardous driving conditions such as icy roads, construction zones, reduced visibility, potholes, drowsy driver advisory and distracted driver advisory at designated Intersections Wrong Way Driver Warning and traffic jams. These applications increase driver safety but do not require immediate driver reaction because the hazards are not imminent [12]. Focus on making driving more enjoyable and providing greater convenience to the driver and passengers.

V. CHALLENGES AND DESIGN ALTERNATIVES OF ROUTING

Specific characteristics of vehicular environments pose significant challenges for efficient communication in VANETs. Some of these, derived from [11], are explained here. Vehicles will last only for small amount of time because each vehicle goes in opposing path and never meet again so mobility is one of the major issue in VANET [12]. Network scalability This network is scalable up to millions of nodes app. 7.2 millions and the scale is growing day by day rapidly but there is no global or central authority that governs standard of this type of network. For e.g DSRC of North America and Europe are different not same. Volatility In case of high mobility of cars connection will be lost, so personal details of user's equipments to a host location requires a long password but this will be unrealistic for securing network. Efficient Channel Utilization Broadcasting and multicasting are widely used methods in VANETs. But there is limited available bandwidth of nodes and broadcast applications demand high bandwidth [15]. These packets are used for disseminating safety traffic messages or alerts and route discovery.

1. MOBILITY
Nodes in VANET environment can be RSUs, vehicles in traffic jam or fast moving vehicles. These extreme cases graphs must be indented. This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. Have their own challenges in the communication system between the nodes [16]. In case of high velocity, the mutual communication window will be small (few seconds) due to small transmission range. Also, for high relative velocity, the communication system has to cope with the Doppler Effect, frequent link failures, wastage of network bandwidth, and high end-to-end (ETE) delay [17], Although nodes have high period of message exchange, they must deal with the problems related to high vehicular traffic density such as frequent data collision, channel fading, message dropping due to expired waiting time, and other interference problems.

2. TRAFFIC DENSITY
A node may be in high density network, i.e., in a traffic jam, or in low density network, i.e., on a highway with no or very few vehicles around. In case of low density, instead of immediate message forwarding, an advance information message dissemination using store-and-forward message must be done [10,16]. Also, the same message may be repeated by the same vehicle multiple times. In case of high density, the opposite must be achieved with only selected vehicles allowed to send repeated messages. Node density not only depends on the road but also on time. Node density is usually high during day hours when compared to night time [12].

3. MOVEMENT PATTERN
Node movement is not arbitrary but follows a predefined path. However, different roads have different characteristics. Urban roads are denser in nature, with many vehicles, buildings and other obstacles when compared to rural and highway roads. These variations in characteristics may also pose some challenge for efficient communications [16]. For instance, highway roads are highly ordered whereas the urban roads are the opposite.

4. HETEROGENEITY
Different nodes have different characteristics in VANETs depending upon their applications. They may be stationary, such as RSUs, or moving, such as vehicles. In addition, they may be categorized into different levels based on their application requirements [6]. For instance, vehicles can be classified into private, authority and maintenance vehicles whereas RSUs can be those that emit data or those that are equipped with complete ad-hoc features [15]. Also, unlike

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

vehicles, RSUs do not require a privacy feature. Hence, a VANET system must provide services based on requirements of a node.

VI. SECURITY REQUIREMENTS

Availability, various applications in VANET requires real time environment, so any information must available at any time. This security is essential in time varying environment any delay in a second or a millisecond will make the message meaningless [7]. Authentication, In VANET, each vehicle message is assigned with a private key and its certificate. At receiving end vehicle receive the message from sender, it first checks the key and certificate attached with a message and then verification procedure takes place. Confidentiality, in VANET each driver's privacy is protected by encrypting the message in order to prevent outsiders accessing driver's critical information [13]. Location and anonymity are main issues for vehicular users. Privacy: this type of attacks is identity revealing attack and is related with unauthorized accessing of important data or information about vehicles [14]. In case the car's owner is driver, if the attacker gets the owner's identity then indirectly vehicle may put its privacy at risk. Non Repudiation, when two or more users share the same key then non repudiation occurs [18]. Even after the attack happens this facilitates the ability to identify the attackers and also prevents cheaters from denying their atrocity.

VII. POSSIBLE ATTACKS

Various attacks wreak against message itself rather than materialistic security in vehicles are described here.

A. Availability

Denial of service attacks, vehicle resources are controlled by the attackers. This type of attacks also prevents arrival of critical information by jamming the session or communication medium [7]. Jamming attack: the attacker interferes with the radio frequencies used by VANET nodes. Malicious attacker: he has specific targets. He causes damages and harms via applications in VANET [13]. Greedy behaviour, drivers try to attack for their own benefits. For example: sending accident message may cause congestion on road or sending false messages for freeing up the road [11]. Malware and Spamming Attack, here digital signature of software and sensors is a must. Using trusted hardware make impossible to change existing protocols and values, except by authorized nodes.

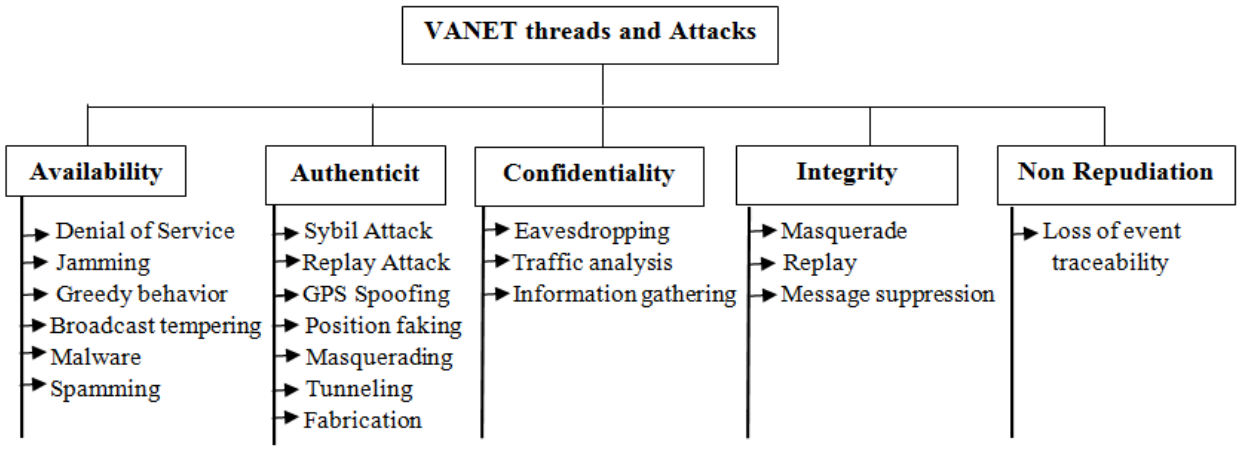

Fig: Categorization of VANET Attack

B. Authentication

Sybil attack, attacker generates huge amount of pseudonymous and pretends like conveying the information to others that there is heavy jam ahead in the communication medium and also force the vehicles to take an alternative route for their own benefits. For GPS spoofing and faking position: Use signature with positioning system to accept only authentic location data [6], or implement differential monitoring to identify unusual changes in position [6]. GPS spoofing; there is disclosure of targeted node ID in order to track the current position of that particular vehicle [3]. Generally this tracked information or data is used by car rental companies for tracking of vehicles. Replay attack, in this attack previous Information is transmitted again by the attacker in order to get the benefit of current situation at the time of message forwarding. Basic 802.11 provides no securities against this attack due to the absence of unique sequence numbers or timestamp [12]. The main motive of this attack is to avert vehicles identification in hit and run event. Masquerading, propose to include an authoritative identity in each message and authenticate it, by using the digital signature and sequence number.

C. Confidentiality

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message and video-conference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside [13]. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. Information gathering, An attacker employs various means of gathering information about a target company or organization [15]. These techniques may range from using telephones, gathering trash or other discarded information, intrusion within company property, using the Internet for research, to querying individuals under false or misleading pretences. A social engineer can use many small pieces of information to combine into a useful vulnerability of a system [3].

D. Integrity

A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed [7].

E. Non-Repudiation

Loss of event traceability: a trace is a sign of past events, traceability is provided by good long information, when we design any system, you must determine which information is relevant and provide proper infrastructure, good log information is useful for many purposes, to detect error and deliberate, to analyse effect of attack and to identify source of attack [13].

VIII. CONCLUSION

This paper presents VANETs highlighting current challenges and applications. The applications envisioned are likely to find their place in inter vehicular communication, hence making the widespread VANET deployment deployment possible in near future. Security attacks are also discussed which affects the principles of security such as availability, authenticity, confidentiality, integrity and non repudiation. Although significant research has already been done many keys factors for their success are still open. Here is lack of profound performance evaluation of different schemes and versatile and comprehensive real-life scenarios in VANET; concept of efficient routing in VANETs still remains a key and widely open research issue.

REFERENCES

[1] Goudarzi, M. A. R. Baee, S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. and S. Mandala, Trust management in vehicular ad hoc network: A systematic review", EURASIP Journal on Wireless Communications and Networking, DOI:10.1186/s13638-015-0353-y, Dec. 2015.
[2] M. Al-Rabayah and R. Malaney, A new hybrid location-based ad-hoc routing protocol," IEEE Global Telecommunications Conference (GLOBE-COM'10), vol. 1, no. 6, pp. 6-10, Dec. 2010.
[3] N. Patel, R.H. Jhaveri, Trust Based Approaches for Secure Routing in VANET: A Survey, Elsevier, 2015.
[4] M. Pophali, S. Mohod, T. S. Yengantiwar, Trust based opportunistic routing protocol for VANET communication," International Journal Of Engineering And Computer Science, vol. 3, no. 8, pp. 7408-7414, Aug. 2014.
[5] F. G. M armol and G. M. P erez, Trip, A trust and reputation infrastructure-based proposal for vehicular ad hoc networks," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 934-941, May 2012.
[6] W. Qiwu, Q. Liu, L. Zhang, Z. Zhang, A trusted routing protocol based on GeoDTN+Nav in VANET," China Communications, vol. 11, no. 14, pp. 166-174, 2014.
[7] R. Waghmode, R. Gonsalve, "Security enhancement in group based authentication for VANET", International Conference on Recent Trends in Electronics, Information & Communication Technology, IEEE, January 2017.
[8] D. Kushwaha, P.K. Shukla, A survey on Sybil attack in VANET, Int. J. Compt. Appl. 98 (15), 2014.
[9] N. Yang, A similarity based trust and reputation management framework for VANETs," International Journal of Future Generation Communication and Networking, vol. 6(2), 2013.
[10] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux, "Certificate Revocation in Vehicular Networks", Laboratory for computer Communications & Applications, School of Computer and Communication Science, EPFL, Switzerland, 2006.
[11] R. Raiya, Sh. Gandhi, Survey of various security techniques in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 4(6), 2014.
[12] V. La Hoa, at all, Security attacks and solutions in vehicular ad hoc networks: a survey, Int. J. Netw. Syst. Vol : 4(2) April 2014
[13] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for Dos attacks in VANET, Int. J. Comput. Appl. ISSN 0975-8887, vol: 66 (22), 2013.
[14] A.M. Malla, R.K. Sahu, A review on vehicle to vehicle communication protocols in VANETs, Int. J. Adv. Res. Computer. Sci. Softw. Eng. Vol: 3(2), 2013
[15] H. Hasrouny, C. Bassil, A. Samhat, Security risk analysis of a trust model for secure group leader-based communication in VANET, in: Second International Workshop on Vehicular Adhoc Networks for Smart Cities, IWVSC', 2016.
[16] H. Hasrouny, C. Bassil, A.E. Samhat, A. Laouiti, Group-based authentication in V2V communications, in: DICTAP, Fifth International Conference, IEEE, pp. 173–177, 2015.
[17] K. Lim, D. Manivannan, An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks, Veh. Commun. Pp: 30–37, 2016.
[18] M. Mejia and R. Chaparro-Vargas, Distributed trust and reputation mechanisms for vehicular adhoc networks," Vehicular Technologies – Deployment and Applications, vol. 1(6), pp. 6-10, Dec. 2013.