ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Security and Privacy Issues in Vehicle Ad Hoc Network

Sandeep Maan[1], Pooja Rani[2]

Associate Professor, Department of Computer Science, Gov Girls College Sec14, Gurgaon, Haryana, India[1]

Research Scholar, Singhania University, Rajasthan, India[2]

ABSTRACT: Vehicular ad hoc networks (VANETs) is one of the emerged technology where roadside units (RSUs) and vehicles communicate with each other. Vehicular ad hoc network can be categorized as a kind of mobile ad hoc networks (MANETs). Vehicular ad hoc network confronts many challenges in terms of security and privacy, due to the fact that data transmitted are diffused in an open access environment. Main goal in the designing of such networking is to resist security attacks and other malicious abuses. However, most of the drivers want to maintain their information discreet and protected, and they do not want to share their confidential information. So, the private information of drivers who are distributed in this network must be protected against various threats that may damage their privacy. So confidentiality, integrity and availability are the important security and privacy requirements in VANET.

KEYWORDS: VANETs, MANETs, Privacy, Security, False Message Detection

I. INTRODUCTION

VANET (Vehicular Ad-Hoc Network) is a network used for communication between vehicles and roadside units and also between vehicles. VANETs have emerged as subclass of mobile ad hoc networks (MANETs). VANETs are having various differences in properties from MANETs therefore, protocols of MANETs cannot directly be
applied to VANETs [1]. Using the VANETs technology vehicle owners could increase safety and provide many services to drivers [2]. Nowadays Vehicular ad hoc networks (VANETs) are becoming the most promising research topic in intelligent transportation systems (ITS), because they provide information to deliver comfort and safety to both drivers and passengers. It is also a key component of intelligent transportation systems to improve safety, efficiency and minimize traffic jam [3].
Each vehicle in VANET, is equipped with a sensor whereby vehicles are able to communicate with each other via inter-vehicle communication (IVC) as well as with road side equipment via Roadside to Vehicle Communication (RVC). This communication can be used for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet [4]. The main goal of VANET is to serve users across its potential applications and by providing timely information to drivers. So the network should be available every time, but if the network is unavailable for the communication, the main goal of this network has become useless [5].

The main motivation of Intelligent Transportation Systems(ITSs) is to improve road safety and driving conditions [6]. In vehicular ad hoc networks (VANETs) there are two type of communications has been established to share the critical driving information vehicle-to-vehicle (V2V) and vehicles-to-infrastructure (V2I) communication [7].
As shown in Fig. 1, in V2V communication, vehicles communicate with nearby vehicles to exchange information; and in V2I communication, vehicles communicate directly with roadside units (RSUs) [8]. Roadside Units are fix units which monitors the vehicles activities and collect all important information about nearest vehicles. Every vehicle consists of an on-board unit (OBU), which broadcasts messages about its position, speed and other events. On Board

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

Unit (OBU) used to verify incoming messages from valid entities. Dedicated short range communication (DSRC) radio [9] and a couple of IEEE standards can be used for V2V and V2I communications in VANETs.

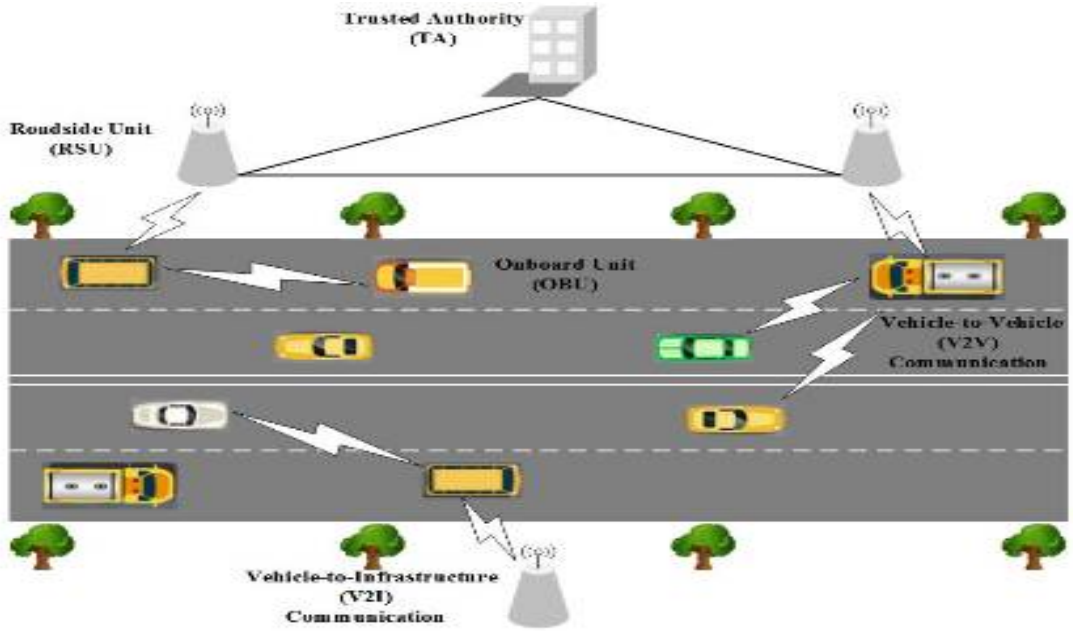

Fig. 1. System model of vehicular ad hoc networks (VANETs).

The rest of the paper is organized as follows: section 2 is an introduction of the VANETs. In Section 3 attacks on privacy and solution has been discussed. Section 4 explains security and privacy issues in VANET and we also discuss about many malicious information techniques that has been used in VANET. We discuss about some of the and finally conclusion has been drawn in section 5.

II. VEHICULAR AD HOC NETWORK (VANET)

The system model of VANETs include three major components : Road side unit (RSU), on board unit (OBU) and trusted authority (TA). OBU of each vehicle is connected with a sensor network to exchange velocity, steering information, etc. and can communicate with other vehicles' OBUs and nearby RSUs [8]. TA is responsible for the management of all the RSUs through a wired connection. All RSUs along the road are interconnected with each other.
An OBU is equipped in every vehicle as a transceiver tocommunicate with other vehicles' OBUs and RSUs. An OBU consists of a resource command processor (RCP), storage, network device, and sensors. Sensors such as global positioning system (GPS) collect information to send to the OBU. Then the OBU monitors and gathers the information to form messages, which are sent to neighboring vehicles and RSUs through wireless medium [8]. TA is responsible for the trust and security management of the entire VANETs including verifying the authenticity of vehicles and revoking nodes in the case of vehicles broadcasting fake messages or performing malicious behavior [8]. Thus, the TA needs to have high computational power and sufficient storage capacity. The RSUs are generally stationary devices deployed along the road or at dedicated locations such as at intersections or parking lots [10]. The RSUs have network devices for dedicated short range communication (DSRC) as well as communication with the infrastructural network. The main functions of RSUs include: (i) Extending the communication range of VANETs

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

by relaying the messages to other OBUs and RSUs. (ii) Running safety applications such as traffic condition reporting or accident warning. (iii) Providing Internet connectivity to OBUs.
Communication system of VANETs is standardized to integrate all the features from the physical to the application layer [6]. The main standards dealing with VANETs includes dedicated short range communications (DSRC), wireless access in vehicular environments (WAVE) and IEEE 802.11p. The communication pattern in VANETs can be divided into four categories as described by Fuentes et al. [11]

- Warning Message Propagation among Vehicles
- Beaconing among Vehicle
- Warnings between Infrastructure and Vehicles
- Group Communication among Vehicles

Compared to other type of networks such as MANETs, VANETs have some of following unique features.

- Dynamic network topology
- Computing and storage capability
- Mobility
- Real time constraints
- Volatility

III. RELATED WORK

As VANETs is very useful in many aspects of life but there are many kind of attacks which try to breach user privacy i.e stole personal information of the user and also use information of the vehicle for some kind of personal benefits. The first attack involves receiver that are connected to a central database, which stores the pseudonyms, location, and time stamp [12]. The second attack discussed is the use of third-trusted parties' application (payment methods, loyalty cards, and chat application) [12]. By using these applications, users are risking their privacy by exchanging personal information that may help trackers link previous or future pseudonyms. By accessing web applications, malware can be installed which records location of the vehicles [12] and attackers will be able to hack into the vehicle system.
Malware is a kind of attack. It includes Accessing applications such chatting, paying toll fees and connecting with the RSU can danger users of VANET. Since this network is a computer based, it is vulnerable to software attacks [12]. It can range from manipulating messages to crashing and hacking on-board units. Manipulating messages invades privacy and creates security issues to the unknown victim. A victim could receive a false accident report and be forced to travel on an unfamiliar road. A victim could also send an alert message, but have it never successfully be sent or have the message altered. An attacker could crash the on-board unit in the vehicle which would be more of an inconvenience and cost to the owner. On the other hand if an attacker could crash the system, an attacker could hack into the system. This makes drivers in VANET vulnerable to tracking, impersonation attacks; steal private keys, track past/future routes, and link pseudonyms. We considered there are two solutions of malware are silent period and group navigation.
Another kind of attack is linking pseudonyms. In this kind of attack A skillful and knowledgeable attacker can intercept radio waves to and from a vehicle using some type of compatible transmitter/ receiver [13]. With the intercepted data, an attacker could use the information a number of ways. An attacker could steal identities; steal private keys, track past/future routes, and link pseudonyms. Although pseudonyms were introduced to VANET to help drivers feel safe and comfortable that their true identity would be safe, pseudonyms do not completely prevent tracking. A determined attacker can link pre-existing pseudonyms to present pseudonyms, which will then aid to future pseudonyms [12]. There are some of solution to linking of pseudonyms are silent period, mix zones and group navigation. Random Silent Periods are randomly chosen periods which vehicles are forced to remain silent. During silent periods, vehicles have no incoming or outgoing messages using VANET and cannot access location base servers. The disadvantages to this are: vehicles can still be tracked due to time and space relations. If the silent period range longer that some x amount of feet could affect the safety and liability of drivers given there was an emergency that needed to be reported [14] [15].
Another solution is mix zones which are predetermined regions where vehicles are required to change pseudonym addresses. These regions should be placed in areas such as intersections to prevent tracking vehicles. Due to the changing of pseudonyms Mix Zones are dependent on Road side unit (RSU). The demand for RSU depends on the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

traffic flow of that region. Unfortunately it would be very costly for regions with extremely busy intersections, which become a disadvantage to Mix Zones. Another disadvantage is that the RSUs are fixed, which in return allows to easily identify the location of Mix Zones and work to intercept information [16] [17], unless there is some randomizing algorithm that allows some intersections to have mix zones at certain times. Group navigation preserves group identity and reduces pseudonyms. This solution may consist of a group leader, group members, and a group key. Group members and leaders travel in a general direction and velocity. If vehicles request to join the group, the group leader sends the group key and private key. Group keys allow members to encrypt and decrypt messages, while messages received would be untraceable. A private key for each vehicle allows the group leader to authenticate members and identify the vehicles. Members are able to communicate amongst themselves while group leaders can communicate outside the group as with Road Aide Units. All the messages group members send will have to be approved by the leader and then the leader would be able to access servers and message other group leaders. The disadvantage to group navigation is that there is no known protocol to appoint a vehicle to the position of leader and the group's leader's identity could be revealed [18] [19] [14] [15].

IV. SECURITY AND PRIVACY

4.1 Security

Despite of advantages VANET also have some issues such as security and privacy issues. One of the main security problem is how to make vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication channel secure. As VANETs help to improve traffic efficiency and safety as well. During communication the dissemination of messages must be relayed through nodes in VANETs. Many times this is possible that a node may propagate false information in a network due to selfishness or its malicious behavior. Such kind of False information in VANETs can change drivers' behavior and create disastrous consequences in the network. So such false messages may endanger human life. To avoid any lass, it is more important to detect and avoid false messages and provide better security services to the user. The key security services are confidentiality, availability , authenticity, non- repudiation and data integrity [8]. Fig. 2 summarizes security services and corresponding threats and attacks.

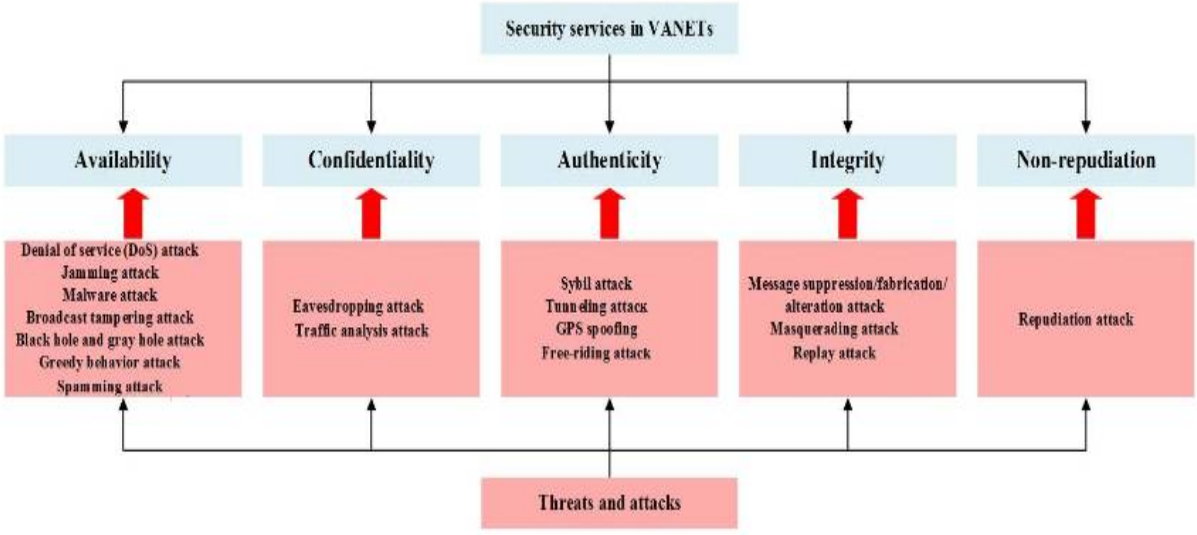

Fig 2. Security services and corresponding attacks and threats [6].

4.2 Privacy

Globally there is no set definition for privacy, causing some difficulties to study what should be kept private. The definition of privacy used for this research is from Dr. Standler. Dr. Standler defined privacy as "the expectation that

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a per son of reasonable sensitivities [20]."

The privacy information is categorized into two groups: motor vehicle records and personal information. Motor vehicle records are defined as any record that pertains to a motor vehicle operator's permit [21]. A few examples of motor vehicles records include, but not limited to: motor vehicle title, motor vehicle registration, and identification card issued by a department of motor vehicles. Personal information is defined as information used as identification. A few examples of personal information include, but not limited to: photograph, full name, routine routes and time of travel, bills, and private keys. Keys are types of pseudonyms that secure the communication between the sender and receiver. There are two ways to encrypt and decrypt messages. First is the Asymmetric key consisting of a private and public pair of keys that correlate with one another.

Public keys can represent mailbox addresses that everyone in the network can see. Private keys are like a key that can open the mailbox mentioned above. This key can open any messages that are encrypted with the corresponding public key. To encrypt a message, one needs the public key of the person that is being sent the message. To decrypt the message, the private key is used to decrypt and corresponds to the public key. The advantage of public and private keys is the ability to authenticate messages. The disadvantages are: high security overhead [22] [23] [24] and computationally costly storing large number of key pairs and keys must be changed frequently [25]. Another type of key is the Symmetric key that consists of a key to encrypt and decrypt messages. This key can only be seen by certain individuals with some sort of mutual agreement. The advantages to asymmetric keys are: more efficiency over asymmetric keys, less computational effort, and less vulnerable cryptanalytic advance [23] [24] [26]. The disadvantage is the key distribution process is currently unknown.

4.3 Malicious Information detection in VANETs

There are different kind of application for traffic management and road safety. Application can be divided in to two types such as safety application and non safety application. In both kind of application some abnormal behavior of node has been seen. Cause of such misbehavior can be divided in to two types i.e intentionally (attacker) and unintentionally (faulty). The intentional misbehavior type is further divided into selfishness and malicious intent. The unintentional misbehavior happens due to signal loss or fault in sensors [27].

The main objective is to detect those misbehaving nodes that broadcast fake data in VANETs. Revoking misbehaving nodes is a process which may prevent fake packets from further participation in network. Detection schemes are divided in two types, node centric detection and data centric detection.

In the node centric detection scheme, a security model monitors security credentials of a node, like digital signature with the help of PKI [28].The node centric mechanism is precisely concern with a participating agent (node) in the network. They verify node behavior by analyzing packet and message pattern. Node centric detection is divided in two categories

- Behaviour-based detection and
- Trust-based detection.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

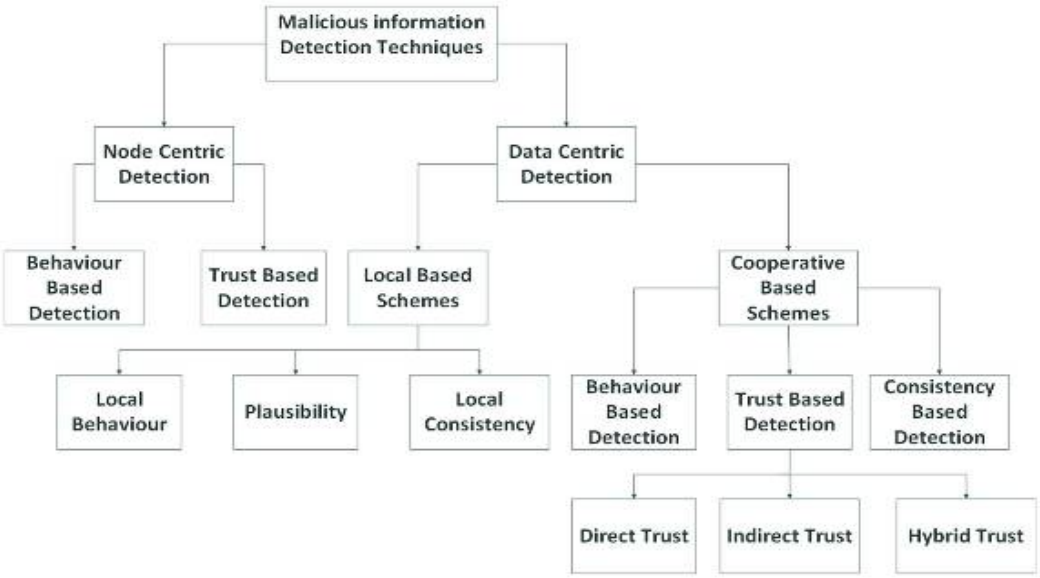

Fig 3. Malicious Information detection schemes in VANETs

In Data centric detection focuses on application data from various neighbours. Data centric misbehavior detection schemes analyze transmitted data for possible misbehaviour. The data is compared with other nodes in network to verify truism of safety messages. In data centric detection scheme, the node searches for possible evidence to verify application data locally or with the help of neighbor vehicles. The detection of false safety alerts consist of local-based detection and cooperative-based detection mechanisms.

V. CONCLUSION

Providing comfort and safety to both drivers and passengers is the major goal of VANETs, which are becoming a promising research field in ITSs. However, security, privacy and trust management are challenging issues due to the unique characteristics of VANETs. In this survey, we first review the basic knowledge of VANETs. Then the main security services with their threats and attacks are explained Considering that future applications in VANETs are required to be evaluated on aspects of performance and security. In conclusion, VANET could only be successful if vehicle owners trust the network to secure their privacy.

REFRENCES

[1] . Khan, S Agrawal, S Silakari, in Information Systems Design and Intelligent Applications . A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. (Springer, 2015), pp. 11–19
[2]. Atulya Mahaian, Niranjan Potris, Kartik Gopa lan, Andy Wang, Lehman Brothers, “Modeling VANET Deployment in Urban Settings,” MSWIM’07, 22-26 October, Chania, Crete Island, Greece, (2007).
[3]. Pallavi A Targe and M P Satone. VANET based Real-Time Intelligent Transportation System. International Journal of Computer Applications 145(4), 34-38 (2016).
[4] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan. Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems. Springer, 217–241 (2010).
[5]Irshad Ahmed Sumra, Halabi Bin Hasbullah and Jamalul-lail bin AbManan. Attacks on Security Goals Confidentiality, Integrity, Availability) in VANET: A Survey. Book: Advances in Intelligent Systems and Computing. Springer. (2014).
[6] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” Veh. Commun.vol. 1, no. 2, pp. 53–66, Apr. 2014.
[7] A. Dua, N. Kumar, and S. Bawa, “A systematic review on routing protocols for vehicular ad hoc networks,” Veh. Commun. , vol. 1, no. 1, pp. 33–52, 2014.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 9, September 2018

[8] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," IET Intell. Transp. Syst. vol. 10, no. 6, pp. 379–388, 2016.
[9] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in Proc. IEEE Veh. Technol. Conf. (VTC Spring) , May 2008, pp. 2036–2040.
[10] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in Proc. 7th Int. Conf. IEEE Wireless On-Demand Netw. Syst. Services (WONS), Feb. 2010, pp. 176–183
[11] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, Overview of Security Issues in Vehicular Ad-Hoc Networks . Hershey, PA, USA: IGI Global, 2010.
[12] M. Gerlach, "Assessing and Improving Privacy in VANETs," Published: In Proceedings of Fourth Workshop on Embedded Security in Cars (ESCAR), Hamburg, Germany, November (2006).
[13] Jerry Werner, "Details of the vii initiative's 'work in progress' provided at public meeting," http://www.ntoctalks.com/icdn/vii pubmtg v1.php.
[14] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE Journal on Selected Areas in Communications (JSAC), Special issue on Vehicular Networks, (2007).
[15] Mingyan Li, Krishna Sampigethaya, Leping Huang, Radha Poovendran, "Caravan: Providing Location Privacy in VANET," Workshops On Privacy in the Electronic Society, Proceedings of the 5th ACM workshop on Privacy in electronic society, Alexandria, VA, 30 Oct., (2005).
[16] Florian Dotzer, "Privacy issues in vehicular ad hoc networks," In proceedings of the Workshop on Privacy Enhancing Technologies, (2005).
[17] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos and J.P Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-TS) Vancouver, (2007).
[18] Maxim Raya, Jean-Pierre Hubaux, "Securing Vehicular ad hoc networks," Journal of Computer Security 15 (2007) 39-68.
[19] Jinhua Guo, P. Baugh, and Shengquan Wang, "A Group Signature Based Secure and Privacy Preserving Vehicular Communication Framework," 2007 Mobile Networking for Vehicular Environments vol.11,no.11,pp.103-108, May 2007
[20] Ronald B. Standler, "Privacy Laws in the US," http://www.rbs2.com/privacy.html, Massachusetts, (1997).
[21] Thomas R. Bruce, Emeritus Peter Martin, "US Code Collection," Legal Information Institute, Cornell Law School, Myron Taylor Hall, Ithaca, NY, (1992).
[22] Maxim Raya, Panos Papadimitratos, Jean-Pierr e Hubaux, "Securing Vehicular Networks," The 25 Conference on Computer Communications IEEE InFOCOM 2006, 23-29 April, Barcelona, Catalunya, Spain, (2006).
[23] Kewei Sha, Weisong Shi, Loren Schwiebert, Tao Zhang, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," ISADS Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, (2007).
[24] Maxim Raya, Jean-Pierre Hubaux, "Securing Vehicular ad hoc networks," Journal of Computer Security 15 (2007) 39-68.
[25] Jinhua Guo, P. Baugh, and Shengquan Wang, "A Group Signature Based Secure and Privacy Preserving Vehicular Communication Framework," 2007 Mobile Networking for Vehicular Environments vol.11,no.11,pp.103-108, May 2007.
[26] J. Choi, M. Jakobsson, S. Wetzel, "Balancing Audit ability and Privacy in Vehicular Networks," Q2SWinet, October 13, Montreal, Quebec, Canada, (2005).
[27] Ilyas, M Akbar, R Ullah, M Khalid, A Arif, A Hafeez, U Qasim, ZA Khan,N Javaid, Sedg: scalable and efficient data gathering routing protocol for underwater WSNS. Procedia Comput. Sci.52 , 584–591 (2015).
[28] van der Heijden, S Dietzel, F Kargl, Misbehavior detection in vehicular ad-hoc networks . (Proceedings of the 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013), 2013