INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

A SURVEY ON VARIOUS ISSUES AND CHALLENGES IN VANET SECURITY AND ITS SOLUTIONS

Sonam Kumari[1], Dr. Harsh Lohiya[2], Dr Rajendra Singh Kushwah[3]

[1]Research Scholar, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India.

[2]Associate Professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India.

[3]Professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India.

ABSTRACT

The Vehicle Private Network (VANET) is a transaction-free network. Increases safety in terms of technology and comfort while driving. It allows vehicles to share data for security and vehicle identification purposes. With the advancement of technology in the world and the development of smart cities, the application of VANET continues to become widespread. VANET provides self-awareness, which has a great impact in improving traffic services and reducing traffic congestion.

The information displayed on this system is time sensitive and requires a strong and fast network connection. VANET serves this purpose as a wireless private network, but with security measures. The network's highly interconnected nature, sensitive data sharing, and time-sensitive nature make it a target for attackers. This article is a research paper on VANETs focusing on security issues and challenges. This survey covers VANETs features, architecture, security requirements, attack types and potential attacks on VANETs.

Keywords: VANET, Architecture of VANET, Sybil, ARAN, SEAD

1. INTRODUCTION

Vehicular Ad hoc network consist of mobile nodes (vehicles embedded with sensors), fixed infrastructure (Road Side Access Point) and wireless interconnection to them to talk with each other. The most important service provided by these networks is driving safety. Almost 1.3 million people die in road accidents and additional 20-50 millions are injured worldwide. Road Traffic crashes ranked as 9th leading cause of death [1]. Some survey shows that 60% of accidents can be avoided if the driver gets the warning even before half a second of the accident [2]. VANET are subset of ad-hoc network working over vehicular domain. VANET has emerged as a solution and become a key component of Intelligent Transportation System (ITS).

Main objective of ITS is improving traffic efficiency and providing better road safety. VANET serves the purpose by sharing road safety information, information related to traffic analysis, normal data (files, audio, video etc) using uninterrupted internet connectivity.

VANET differs from other ad-hoc wireless networks of the same class in these terms:

- High processing power
- Large storage capacity
- Energy sufficiency (as work over battery of vehicle).
- Predictable movement of nodes (as vehicles are bound to follow a certain path along the road).

According to architecture of VANET, it has following components:

1.1 Ad hoc environment:

It consists of intelligent vehicles (nodes) that have basically two components:

On Board Unit: It has communicational capabilities.

Application Unit: work behind OBU and executes program that enable OBU to communicate.

1.2 Infrastructure environment:

It consists of Road Side Units and Access network.

Two type of communication occur in VANET:

V2V: Pure wireless communication between vehicles.

V2I: Communication between mobile nodes and infrastructure unit RSU.

Main concern in VANET is spontaneous networking, use of infrastructures like RSU or cellular network is less concerned

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

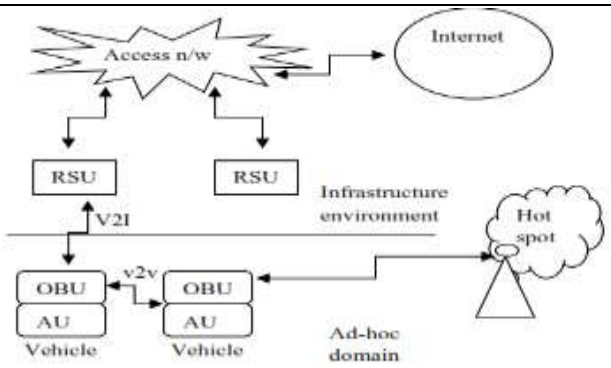

Fig.1: Architecture of VANET

VANET has vast application area classified as Security based application (covering Collision Avoidance, traffic analysis and interactive driving.) and User based application (covering entertainment domain, internet connectivity on roads and other road side services such as providing restaurant or fuel pump information).

For easy and effective communication VANET use two prominent technologies; IEEE 802.16 (Wireless MAN/WiMAX): Wireless communication standard for MAN, designed to enable multimedia application over wireless connections ranging up to 30 miles. IEEE 802.11p (WAVE): Specially used for wireless access in vehicular domain. It enable V2V and V2I communication in the licensed ITS band of 5.9 GHz. VANET require quick establishment of network due to high dynamicity of node. WAVE allows vehicles to communicate directly without prior authentication and association. Security measures provided by 802.11 standards cannot be applied in such circumstances. For ensuring confidentiality and authentication of data and nodes in VANET, a lot of research is going but it still requires more attention of research community. The remaining part of the paper is organized as follows: Section II explains the need for security in VANET, security prerequisites of the system and security challenges of VANET. Section III specifically focuses on attackers and their classification, type of attacks in VANET and prevention measures. Section IV includes possible solutions for those attacks. Finally, section V concludes the paper.

2. SECURITY REQUISITES AND CHALLENGES

Insecure transmission of information through VANET communication may result into catastrophe. So these information need to be accurate, efficient and reliable. Every single work in domain of VANET has an objective to provide road safety efficiently through frequent sharing of information among nodes of the network. Any successful attack can lead to serious accidents, loss of life or economical loss.

Security is needed in Vehicular Ad-hoc network for following reasons [25]:

- Sensitive information is being broadcasted in VANET which in turn attract various attackers.
- No authentication and association measures are provided in WAVE standard due to fast network establishment need.
- Easy to attack due to infrastructure less model.
- Very high chances of threat to privacy.
- Connections intrusion is very easy due to frequently changing topology.
- Vanet Focuses On Improving Transportation Safety, Collision Avoidance, Traffic Efficiency And Providing Entertainment. So, Some Prerequisites Must Be Ensured By The Deployed Security System.
- **Authentication:** Authentication gives us an assurance that the information/message is generated by a genuine user. In VANET nodes respond according to the information received from the other end, so it is very necessary that the information propagating in the system is true and generated by a legitimate user.
- **Reliability:** Data receive in communication should be correct and factual. Periodic verification of the system is done to eliminate the factually incorrect information.
- **Integrity:** The information received should not be altered by any unauthorised user. Such alteration can harm the system and can cause serious catastrophic casualties.
- Anonymity: Most of the time owners are driving vehicles in such environment. So security measure must ensure privacy of all genuine nodes.
- **Availability:** These system handle urgent data, so data should be available to all authorised user easily and efficiently.
- **Delay handling:** Safety information is time sensitive, so latency should be avoid and handled.
- **Confidentiality:** Sensitive data should not be accessed by unauthorised user.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

VANET has a set of various features that provides the base to stand alone in the field of its class. But sometimes these features create obstacle in deployment of VANET.

Such challenges are categorised as Technical challenges(covering management of dynamicity of network, latency management, congestion and collision analysis, atmospheric impact and Security challenges) and Social and Economical Challenges (covering cost impact and social acceptance of VANET) [5]. VANET provides safety and traffic analysis measures, so the information communicated must stay secure and the network needs to be robust [24].We have considered the security challenges to attain an efficient and secure VANET system. Major securities challenges need to be conquered by security system of VANET are [6]:

- **Consistency of data:** Any malicious alteration in life critical information can lead to accidents, to avoid malicious activity from authenticated and non- authenticated nodes that cause inconsistency in data, some mechanism need to be designed. Cross checking of received information from various nodes is done to avoid such activities.
- **High Mobility:** VANET are highly mobile network so they need less complex algorithm for security in spite of being capable of high processing and storing power.
- **Error Tolerance:** Receive and response action in VANET is very quick, so any mistake in protocols or algorithm can harm the system harshly. So protocols need to be designed taking this issue in consideration.
- **Latency Control:** Information shared in this network is time sensitive. To achieve real time restraint, cryptographic and other algorithm used in security must be fast and efficient.
- **Key Management:** All algorithms used in VANET security are key dependent. So creation, maintenance and distribution of keys need to be handled specially.

3. ATTACKS IN VANET, THEIR CLASSIFICATION AND PREVENTIVE MEASURES

Different types of attacks are possible in ad-hoc environment, especially in vehicular domain. Impact of these attacks over the system primarily depends over the intensions of the attackers behind it. Attackers can posses' malicious behaviour for several reasons such that to get benefit of the system facilities for which he is not a legitimate user, to get confidential data of the system or just to disturb the efficient functionality of the network. These attackers can be classified [2]:

On the basis of Membership: Any authorised or unauthorised node can perform malicious activity in the network. Membership function highly affects the impact of the attack and its prevention. There are two types of attackers on this basis;

- **Internal Attackers (Im):** These are the authorised member nodes that perform malicious activity to gain personal benefit or just to disturb the network. These attackers put stronger impact than the external one.
- **External Attackers (Em):** They are the intruders who try to enter in network either by impersonation or other attacks.
- **On the basis of Activity:** Whether an attacker is active and makes frequent changes to network or not, the attackers are classified as:
- **Active Attacker (Aa):** These types of attackers try to alter the network information and generate malicious packets and signals. Attacks made by them are more effective than that made by passive attackers.
- **Passive Attackers (Pa):** These types of attackers do not alter the network information. They silently sense the network.
- **On the basis of Intensions**: Any attack is associated with the intension of the attacker, i.e. main objective of the attacker behind that attack. Following type of attackers are identified on this basis:
- **Rational Attackers (Ri):** These attackers seek personal benefit from the attacks and hence are more predictable.
- **Malicious Attackers (Mi):** These attackers not gain personal benefit from attacks. Their main motive is to create obstacle in proper network functionality.

VANET operates over life critical and sensitive information. This information seems attractive to attackers; so this network serves as a fertile region for such malicious attackers. We are classifying VANET networks in five different classes as follows [7];

Network Attacks (NA):

These are the most serious attacks. The whole network got affected from this. They are the direct attacks over functionality of network and nodes. Attacks like DoS, Sybil etc are the example of this class.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

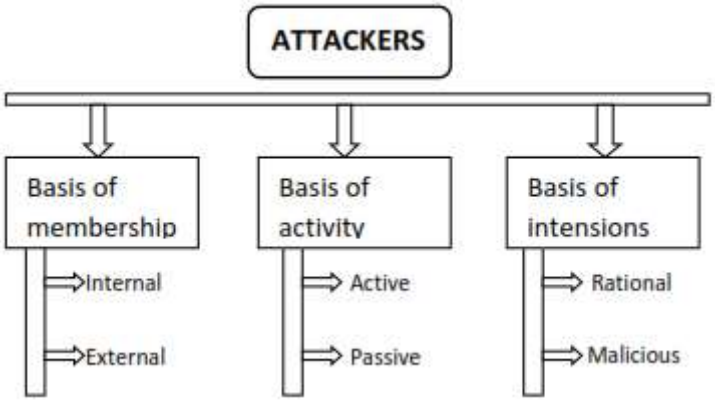

Fig.2: Classification of attackers

Application Attack (AA): These types of attacks are primarily concerned with the information being shared and with the application being served. Bogus information, eavesdropping are the example of this class.

Timing Attacks (TA): These attacks perform alteration in time slots of messages to add some delay.

Social Attacks (SA): All such messages or attacks that create emotional imbalance in other drivers come into this category. In this class of attacks unethical messages are sent to vehicles that disturb the driver and hence esults into driving disruption, loss of other prerequisites of security system.

Monitoring Attacks (MA): In these attacks, attacker silently monitors and tracks the whole system and can perform malicious activities based on those observations. All passive attacks come into this category. Impersonation and session hijacking can also be counted under this class.

Major attacks in VANET with some general prevention schemes are as follows:

Sybil: In this attack the compromised node declares itself as several node, i.e. the vehicle announce its various position at the same time or with frequent interval of time. It possibly creates confusion and security risk in network. Sybil attacks harm network topology and can cause bandwidth consumption [8].

Network can be secured by this attack through [9]:

• **Registration:** Register vehicles in network with unique id associated with it.

• **Position Verification:** Position of vehicles verified to ensure that each node represent only one id.

Table 1. Classification of attacks and their impact

Classes of attacks	Prerequisites compromised
Monitoring Attacks	Authentication, Anonymity
Social Attacks	All Requisites May Affected
Timing Attacks	Delay Handling
Application Attacks	Authentication, Reliability, Confidentiality, Integrity
Network Attacks	Authentication, Availability, Integrity

• **Radio Resource Testing:** This approach works on puzzle and assumes that computational resources are limited to node and hence any Sybil attacker node will get too many puzzles and not be able to solve them and get identified [8].

This is not an effective measure as in VANET node can have additional computational resource. The second approach has assumption that 'there is only one radio in each node' and 'a radio can send or receive only on one channel at a time'. So Sybil node working over different channel gets identified [10].

Impersonation: In impersonation attack, the attacker represents itself as an authorised node. These attacks can have objective of either to disturb the network or to gain access to network privileges. These attacks are possible through identity theft or false attribute possession.

Impersonation attacks can be avoided by using Trust Authority (TA) and a Public Key Infrastructure (PKI) [11]. TA knows the real identity of all the nodes. Whenever a vehicle communicates to any new RSU it first verifies its identity through TA and then shares the key to vehicle.

Bogus Information: Attacker sends false information in the network for personal benefit. For example a malicious node can send false information of heavy traffic due to an accident over road and can make its route clear.

Hashing and asymmetric cryptography is used for their handling.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

Denial of Service attacks: DoS attacks have serious impact in any network. These attacks make the victim node unavailable to other legitimate user. This can be performed by Jamming, SYN flooding or distributed DoS attacks.

Prevention to these attacks can be done through IP-CHOCK model. In this OBU analyse and update the IP information and on finding any duplicate IP it identifies the chances of DoS attacks [12].

Routing Attacks: These attacks exploit the routing protocol's loopholes and their vulnerability. Major attacks of this category are:

- **Blackhole Attack:** In this attack, the compromised node send false route with lower hop count to the source in order to attract it and when source node send data packet to that route, the compromised node drops the packet.
- **Grayhole Attacks:** This attack is similar to black hole attack in term of dropping the packets but differ in a context that these dropping are selected; i.e. only some selected type of packets are dropped and this selection is made according to need and intensions of the attacker.
- **Wormhole Attack:** The compromised nodes (two or more nodes are evolved to make tunnels) receive the packets at one end and tunnel it to the other end of the network. Through tunnelling, hop count of the route containing the compromised node decreased and hence the route attracts packets toward it. In this way compromised node get stronger position than other node and can perform attack like DoS, replay etc. For prevention cryptographic techniques, hashing and digital signature are used.
- **Eavesdropping:** This is a threat to confidentiality and is often occurred. The main objective of these attacks is getting confidential and sensitive data for which attacker is not a legitimate person. These attacks fall in category of passive attacks where attacker silently sense the channel and get the information and further use that information for his own benefit.

These attacks can be prevented by encryption of sensitive and confidential data.

Location Trailing: These attacks directly target the privacy. In this attack position or path followed by the vehicle is illegally trailed to trace the vehicle and to get private information about the driver.

For prevention of such attacks ID-based security systems can be used [13].

Replay Attacks: In these attacks the attacker imitates itself as legitimate user or as RSU and replay the transmission of a previously captured packet. Replay attacks target the authenticity and confidentiality of the system.

By using timestamps and global clock for all the nodes, system can be prevented from these attacks.

Session Hijacking: In this attack the attacker get the unique Session Identifier (SID) assigned for each new session and through that get the control over the session. Network layer session hijacking has an advantage that at network layer only one time authentication is performed. After generation and assignment of the SID, no authentication is done and hence this attack takes advantage of this feature [14].

Encryption, dual authentication, random SID generation etc are some preventive measures for these types of attacks [14].

Timing Attacks: In this attack the malicious node when receive any data packet, it just not forward it but it alter the timeslot of the packet to create delay. As a result of it neighbour of the compromised node get the message after the time they supposed to receive it. Since information traversed in the network may be a sensitive information, especially in VANET information are time critical, so any latency can result into major accidents and casualty and serious traffic issues. Use of cryptographic solution such as TPM (Trusted Platform Module) can be used to prevent such attacks [15].

Table 2 represents the summarized view of attacks, attacker types, attack class, their preventive measures in the basis of properties violated. Attacker type defined here, as (membership, activity and intensions) function (as explained in section III).Parameter 'both' represents the fact that both type of attacker of that class are capable

Table 2. Summary of various attacks in VANET

Property Violated	Attacks	Attack Class	Attacker	Preventive Measures
Privacy	Location Trailing	MA	(both, both, Pi)	ID based system
Availability	DoS	NA	(both, Ma, Ai)	IP info. Handling
	Routing Attacks	NA	(Im,Ma, Ai)	Cryptography, hashing etc.
Integrity and Confidentiality	Eavesdropping	NA,	(Im, both, both)	Creation of Cipher
	Replay	NA, AA, SA	(both, both, Ai)	Time-stamping

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

	Bogus Info.	AA	(Im, Ra, Ai)	Hashing, asymmetric crypto.
Authenticity	Sybil	NA	(Im, both, Ai)	Registration, Position Verification, Radio Resource Testing etc.
	Impersonation	NA, MA	(both, both, Ai)	Trust Authority, PKI
	Timing attack	TA	(Im, Ma, Ai)	Encryption solution (TPM)
	Session hijacking	NA,	(both, both, Ai)	Encryption, Random SID generation

4. VANET SECURITY SOLUTION

As discussed above, VANET are susceptible to various kinds of attacks. Since research in this field has new and interesting scope, various effective works has been done to provide security solution in VANET. In this section some solution are being discussed for VANET security.

ARAN:

This routing protocol, named as Authenticated Routing for Ad-hoc Network (ARAN), is an AODV based protocol [16]. In this approach, a third party CA is present that provide signed certificate to nodes. Each node coming into the network need to sent request certificate to CA. Public key of CA is known to all authorized nodes. Asymmetric cryptographic technique is used for authenticated secure route discovery and timestamps are used for freshness of route.

ARAN basically has 5 steps [16];

- Certification
- Authenticated Route Discovery
- Authenticated Route Setup
- Route Maintenance
- Key Revocation

Route authentication process is done at each step, through addition of sign and certificate of each intermediate node, so Impersonation problems are solved by this protocol.

SEAD:

Secure and Efficient Ad hoc Distance vector protocol work over DSDV. It uses one way hash function for authentication process. This protocol protects against incorrect routing. It uses destination-sequence number to ensure freshness of the route and to avoid long lived route. At each intermediate node hashing is applied to ensure the authenticity of routes.

of doing attack.

Ariadne:

This protocol works over on-demand routing protocol DSR [19]. Symmetric cryptographic operations work very efficiently in this protocol. One way hash function and MAC are used for authentication and are communicated between nodes using shared key. TESLA broadcast authentication technology is basis of this protocol. In route discovery and authentication process TESLA time interval are used.

SAODV:

This protocol was proposed to embed security measures in AODV protocol [20]. All routing messages are digitally signed to insure authenticity and to protect hop count hash functions are used. In this approach intermediate node cannot send route reply even if the fresh route is known to them. Through Double Signature this problem can be solved but it increases the complexity of the system.

A-SAODV:

This protocol is an extension to SAODV that has an experimental feature of adaptive reply decision. Each intermediate node can decide whether to send reply to source node or not, depending on the queue length and threshold conditions [21].

One Time Cookie:

Generally for session management, cookies are assigned per session. But to prevent the system from session hijacking and theft of SID, this protocol gives the concept of OTC (one time cookie) [22]. OTC generate token for each request and these token are tied to request using HMAC to prevent the re-use of the token.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 105-112

Table 3. Summary of security solutions

Solution	Technology	Attack
ARAN	Cryptographic Technique	Replay attack, Impersonation, Eavesdropping
SEAD	One way hash function technique	DoS, Routing attack, Impersonation
Ariadne	Symmetric cryptography technique, MAC	DoS, Routing attack, Replay attack
SAODV	Digital signature, hash function	Routing attack Impersonation Bogus information
A-SAODV	Digital signature, hash function	Routing attack, Impersonation, Bogus info.
One Time Cookie	Random cookie generation	Session hijacking
ECDSA	Elliptical curve parameter, digital signature	Bogus information, Impersonation
RobSAD	Motion pattern analysis	Sybil Attack
Holistic Protocol	ID Registration Technique	Impersonation

ECDSA: Elliptical Curve Digital Signature Algorithm [23], as the name suggests this algorithm use digital signature. With hash function and asymmetric cryptographic operations authenticity and security is provided in this system. Both the sender and receiver need to be agreed upon elliptical curve domain parameters.

RobSAD: Robust method for Sybil Attack Detection [17], the main concept behind this method is that two different vehicles cannot have same motion pattern while driven by different drivers, since each person drive according to his comfort and need. Identification of Sybil node is done by finding two or more nodes having same motion trajectories.

Holistic Protocol: This protocol defines the authentication technique by registering vehicle by RSU [3]. In registration phase vehicle send Hello message to RSU then in response RSU prepares Registration id (consisting licence number and vehicle registration number) and send to vehicle. Further the authentication is done through certificate provided by RSU. If the node is authenticated then only data is shared with it otherwise the node is blocked.

5. CONCLUSION

VANET being a safety information sharing medium, needs secure and safe environment. VANET has very wide scope for attacks due to its highly dynamic nature, wireless medium of communication and frequently changing topology. Security issues and challenges related to VANET have very high impact on efficient functionality of the system. Today, VANET are being widely deployed due to its enhancing features of providing safe, secure and comfort driving. VANET, features of VANET, need of security in VANET are the hot topics related to the current scenario. In this paper, we have done a literature survey about various types of attacks, their preventive measures, type of attackers and some existing security solution for attacks in VANET.

6. REFERENCES

[1] Road Crash Statistics- Association for Safe International Road Travel. Available: http://asirt.org/initiatives/informing-road-users/road-safety-facts/road- crash-statistics

[2] Maxim Raya et al., “The Security of Vehicular Ad Hoc Networks”, SASN’05, Nov 7 2005, Alexandria, Virginia, USA, pp. 11-21

[3] K. S. Tamil Selvan, R. Rajendiran, “A Holistic Protocol for Secure Data Transmission in VANET in International Journal of Advanced Research in Computer and Communication Engineering, 2013, pp. 4840-4846.

[4] Yaseer Toor, Paul Miihlethaler, Anis Laouiti, Arnaud De La Fortelle, “Vehicle Ad Hoc Networks: Applications and Related Technical issues”, IEEE Communications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3, pp. 74-88.

[5] Hannes Hartenstein, K.P. Laberteaux, “A tutorial survey on vehicular Ad Hoc Networks”, IEEE Communication Magazine, June 2008, pp. 164-171.

[6] H. Moustafa, Y. Zhang,“Vehicular networks: Techniques, Standards, and Applications”. CRC Press, (2009).

[7] Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, “Classes of attacks in VANET”, in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.

[8] J. Douceur, “The Sybil Attack”, in First International Workshop on Peer-to-Peer Systems, 2002, pp. 251-260.

[9] Bin Xiao, Bo Yu, Chuanshan Gao, "Detection and localization of Sybil nodes in VANETs", in DIWANS '06, pp. 1-8.

[10] J. Newsome, E. Shi, D. Song, A. Perrig, "Loc & Defenses", in International symposium on information processing in sensor networks, 2004, pp. 259-268.

[11] T.W. Chima, S.M. Yiu, Lucas C.K. Hui, Victor O.K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs", in Journal of Ad Hoc Networks 9, 2011, pp. 189-203.

[12] Karan Verma, Halabi Hasbullah, Ashok Kumar, "Prevention of DoS Attacks in VANET", in Wireless Personal Communications, November 2013, Volume 73, Issue 1, pp 95-126.

[13] Jinyuan Sun, Chi Zhang; Yanchao Zhang; Yuguang Fang, "An Identity Based Security System for User Privacy in Vehicular Ad Hoc Networks," Parallel and Distributed Systems, IEEE Transactions on, vol.21, no.9, pp.1227, 1239.

[14] Rashmi Mishra, Sweta Singh, Akhilesh Singh, "Session Seizure: Hijacking" in National Conference on Contemporary Computing and Informatics, May 8, 9 2015, pp 227-229.

[15] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs) ",in IFIP 2008, WISTP 2008, LNCS 5019, 2008, pp.106-116.

[16] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceeding of IEEE ICNP 2002, pp 78-87, Nov 2002.

[17] I. Chen Chen, Xin Wang, Weili Han, Binyu Zang, "A Robust Detection of the Sybil Attack in Urban VANETs", in Distributed Computing Systems Workshop, ICDCS Workshops '09. 29th IEEE International Conference, 2009, pp. 270-276, 2009.

[18] Y. C. Hu, D. B. Johnson, A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", Elsevier B. V.,pp 175-192, 2003.

[19] Y. C. Hu,A. Perrig, D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", MobiCom'02, pp. 23-26, 2002.

[20] [20] M. Guerrero, N. Asokan, "Securing Ad hoc Routing Protocols," Proc. 1st ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[21] Davide Cerri, Alessandro Ghioni, CEFRIEL — Politecnico di Milano, "Securing AODV: The A-SAODV Secure Routing Prototype", in IEEE Communication Magazine, Feb 2008.

[22] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, Patrick Traynor, "One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens" in Converging Infrastructure Security (CISEC) Laboratory Georgia Institute of Technology.

[23] S. S. Manvi, M. S. Kakkasageri, D. G. Adiga, "Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach", in International Conference on Future Computer and Communication, 2009, pp. 16-20.

[24] S. Yousefi, M. S. Mousavi, M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives", in ITS Telecommunications Proceedings'06, pp. 761-766, 2006.

[25] M. Feiri, J. Petit, R. K. Schmidt, F. Kargl, "The impact of security on cooperative awareness in VANET", Vehicular Networking Conference (VNC), 2013 IEEE, pp. 127-134