I.J. Wireless and Microwave Technologies, **2017, 3, 36-48**
Published Online May 2017 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2017.03.04

Available online at http://www.mecs-press.net/ijwmt

Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey

Akash Vaibhav[a], Dilendra Shukla[b], Sanjoy Das[c], Subrata Sahana[d],Prashant Johri[e]

[a,b,c,d,e]*School of Computing Science and Engineering, Galgotias University,Uttar Pradesh and 201310,India*

Abstract

Vehicular Ad hoc Network could manage the various critical issues of road transport. That is why it is the most crucial field of research for most of the researchers. This survey paper discusses various issues related to Security Challenges, Security Architecture actors, Security Authentication, Application Constraints, various trust models etc. this paper encourages you to think about various fields of work need to be carried out in this field for the better VANET environment. Various schemes have been mentioned which could be improved further as per considering various real time conditions.

Index Terms: Authentication, Trust model, Vanet, security challenges, response time.

1. Introduction

Transportation, be it passenger or vehicles, is a significant aspect of development. One of the major concerns world-wide is that of road traffic. To avoid this traffic and ensure 'safety driving' aspect is to be considered and effective driving technique is the need of the hour. To reduce the traffic congestion and ensure safety, accurate weather description, early warning of upcoming dangers, detection of traffic further and other concerned issues, through an automated network would be highly useful to the drivers. Greater advancement in technologies have enabled many vehicles to have GPS and Wi-Fi device to promote inter-vehicular communication forming a vehicular ad-hoc network that is called VANET [1].

VANET (Vehicular ad hoc Network), is a kind of information Technology which allow inter-communication of vehicles for the update of information regarding road and traffic conditions to minimize accident. VANET (Vehicle Ad hoc network) is the sub group of the MANET (Mobile Ad hoc Network) consisting of vehicles as the communication nodes. VANET technology allows for vehicles to vehicles communication (V to V) Vehicles to infrastructure communication that is Road Side Units (RSU) and Road

* Corresponding author. Tel.: +91-9289043931
E-mail address: sdas.jnu@gmail.com

side units to Road side units' communications located along the Road [3]. VANET, Vehicles with provision of wireless communication are one of the rising technology for a better traffic management promoting wireless mobile communications among the dispersed vehicles through generation and broadcast of messages by the help of network setup. Thus, VANETs are supposed to be significant technologies towards effective traffic management and safety applications provided the messages generated are trustworthy. Thus issues of reliability of communication among the vehicles holds a question marks 'Is the information coming from any of the nodes trustworthy?' is an issue challenging the effectively functionality of the vehicular ad hoc network. Since interchange of information among the vehicles forms the basis of working of VANETs, it is important to develop a provision for the detection of false messages in receiver's node. Tremendous efforts are being made in this regard and the government is also largely spending on the development of such network to ensure effective functioning of VANETs, to achieve the desired safety applications and traffic management. The security issues in the VANETs require a serious concern, as if, overlooked these might be devastating in nature causing a serious threat to safety of the drivers, vehicles as well as the passengers and might be use repeatedly for the personal benefits of the attackers.

2. Security Challenges within VANET

There has been diverse challenge within VANETs environment for the construction of a safe and trustworthy communication architecture. Security challenges within these vehicular ad hoc network may prove to be a devastating and would thus inhibit the effective working of this technology. The security challenges within the vehicular ad hoc networks can thus, be summarized as follows:

2.1 Dynamic nature and high mobility of the vehicles: Since the vehicles of the network are in constant motion with average speed being about 100 km/hrs, it becomes highly problematic to react to an immediate situation and in such cases if the incoming messages are not verified within certain duration of time, it may lead to severe accidents. Thus security setup within the VANETs should have provisions for such problems [2].

2.2. Large number of peers in the VANET: In dense urban areas where millions of vehicles would constitute the network, the problem of network congestion may occur due to information overload, thus making it difficult to recognize the peers to be communicated to. Hence the network setup must have smart provision for an easy detection of the required information to react accordingly and thus avoid the hazard situations [2].

2.3. Decentralized: VANET network setup being an open system with no centralized infrastructure provides the participating vehicles an ease of joining and leaving the network respectively as per their convenience. Such system, does not guarantee the interaction of same vehicle in near future thus making it difficult to rely on mechanisms with centralized systems or social network and also creating uncertainty in deciding the reliable peers [3].

2.4. Bandwidth Limitation: This challenge arises when the wireless network is occupied by the competing nodes causing interference, insufficient signal strength, delay in message transmission etc. [4]. This increases complexity in the functioning of the VANET environment.

2.5 Malicious Attackers: This is one of the most challenging security issues in VANET networks. This is carried out by the attackers by disrupting the network functionality by gaining control over the network and thus manipulating, suppressing altering the message or by dropping the packet from network and later using these packets to draw personal benefits out of these. This may include Sybil attack, ID disclosure [3], etc.

2.6 Wireless Links: the wireless links within the VANETs are liable to certain passive attackers such as incriminating confidential information from the network or by manipulating the messages to be transmitted [3].

Table 1. Various Issues in Security Challenges and their possible solutions:

Challenges	Issues	Possible Solutions
Dynamic Nature and high mobility of vehicles	Response time need to be very low otherwise lead to accidents.	There should be time constraint for decision making.
Large no of peers in VANET	• Network congestion • Information overloading • Difficult to detect node	There should be unique Authentication identify for each node.
Decentralized	• Openness • No centralized infrastructure • Any vehicle can join network	Various Schemes are proposed PKI, TESLA, etc.
Bandwidth Limitation	• Network congestion • Interference • Insufficient signal strength • Message delay	Allocation of Bandwidth According to possible traffic
Malicious Attackers	• Security Threat • Message alteration • Sybil Attack • Id Disclosure	New Vehicles need to be authenticated very carefully before accessing the network

3. Security Architecture Actors

It is important that the vehicles and the infrastructure units in a vehicular ad hoc network (VANET) communicate to each other in a safe and secure manner. The various entities of the security architecture within VANET can be enlisted as below [12]:

3.1 Certification Authorities (CAs): It is a part of the security architecture of VANET that is responsible for issuing certificate to the vehicles and the road side units (RSUs). These certificate serve as an identity for these units and help them prove their identification when they communicate with the other units. It also becomes the responsibility of the CA to ensure security within its region. To accomplish this the CA has added responsibility of revoking the certificate in case it is made use by intruded users.

3.2 Road Side Units (RSUs): RSUs stands for the road side units are an important part of the security architecture of VANET. They carry out several security functionalities and are delegated by the corresponding CA. they ensure that all the vehicles approaching it must update their certificate revocation lists as soon as the certification authority confirms to have revoked a certificate.

3.3 Vehicles or On Board Units (OBUs): These may be of different types ranging from ambulances, firemen vehicles, official cars, buses or personal cars etc. the type of information that is exchanged and the type of application the vehicle is authorized for accessing is dependent highly upon the type of the vehicle. Each vehicle is provided with a tamper Proof Security Device (TP-SD) to ensure confidentiality of personal and sensitive Information of the vehicle.

4. Security Authentication

In order to make the user have complete trust and confidence in the system, reliability of the message and the

authentication of the user are important. There are a number of protocols and algorithms that play a key role in user authentication. Some of them have been described in brief below: -

Authentication schemes

PKI scheme:

One of the efficient ways to authenticate the secure operation of VANET is the use of the PKI (public key infrastructure scheme) [19] [20]. To guarantee the validity of the user, PKI scheme is used in the VANET network. The scheme basically utilizes the notation of asymmetric key cryptography, the scheme involves the use of (i) public key (ii) private key, the key can be represented in a PKI scheme as below: -

$$PKI: (X, Y)$$

Where, X denotes private key and Y denotes public key

All the participating vehicles or nodes have each one of the two keys. As the name suggest public key is the one that is shared to all the participants where as private is the one that remains with the user. Using these keys the message that are to be transmitted are:

$$EM= Pr(Pu(M))$$

Where Pr() represents a private key function
Pu() represents a public key function.
M- denotes the message
EM- encoded message

The reality and the integrity of the message that are to be transmitted can be obtained by the use of the Digital signature. In order to ensure authenticity of the user and the trustworthiness of the message, there comes a role of the certificate authorities, which effectively bind the public and the private keys as well as digitally sign the data. Any government authority or the manufacturing organization is well suited to perform the task of CA which involves validating the users providing them proper certificate. However, to avoid any disturbance or confusion a centrally managed CA is more desirable. Ideally a temporary certificate can be issued by the vehicle manufacturer that ought to be validated by the concerned authority. The certificate must hold information like the public keys, lifetime of the certificate, and the digital signature of the commissioning authority. Now, the revocation of these certificates is also possible under the following circumstances:

- Compromise relating cryptographic keys.
- A signed certificate being misused to transmit fake and fraudulent information.

The certificate revocation leads to creation of a certificate revocation list (CRL). the CRL is generally issued by a trusted authority and contains all the revoked certificated. It is updated after each revocation. When authentication of a message is undertaken in PKI system, it is done by firstly verifying the revocation status of the sender's certificate using the CRL which is followed by the verification of sender's certificates and finally checking the sender's signature on the received message [13]. In order to secure user identification and location privacy the PKI scheme [21] also makes use of Anonymous public keys. The basic disadvantage with these schemes is that they result in storage problems as they make use of large number of keys and certification. All these concepts have been purposefully explained in [18].

TESLA

TESLA stands for Timed Efficient Stream Loss Authentication. This is basically utilized as an authentication tool for multicast and broadcast network [14]. TESLA is completely a different technique as compared to PKI when it comes to user authentication TESLA makes use of symmetric cryptographic function with delayed key disclosure that provides the necessary elements of asymmetry. The design of TESLA is done basically for the broadcasting authentication in wireless ad-hoc network. TESLA is resilient to computational DOS attack because the technique symmetric cryptography is swifter than the use of signature which helps a great deal avoiding the delays, however TESLA is prone to attacks due to memory based denial of services [14] and this is the basic reason behind the development of TESLA++. The main concept behind TESLA is that to each packet a MAC (Message authentication code) is attached which is computed with a key K which is known to the user itself. Initially the received packet is buffered by the receiver and it isn't able to authenticate it After some time when the sender discloses K the receiver is in a position to be able to authenticate the packet. Thus we see that a single MAC per packet becomes sufficient to insure broadcast authentication. One of the shortcoming in TESLA is that a large number of attackers can flood the receiver's memory with large number of invalid messages without a corresponding key leading to a situation termed as pollution attack. Pollution attack affects the system's performance and at times even lead to the crashing the system. All this has been described in detail in [16] [17].

TESLA++

TESLA ++ is a modified version of TESLA Timed Efficient stream loss tolerant authentication and it successfully exploits the advantages of both ECDSA (Elliptical Curve Digital Signal Algorithm) and TESLA. TESLA++ has an edge over TESLA when compared to it. TESLA ++ has more advantages in having a shorter hash message authentication code(HMAC) for verifying the message integrity that contributes a great deal in cutting down the transmission overheads of the RSU's [17]. TESLA++ when proposed lead to VAST (VANET Authentication using signatures and TESLA) VAST utilized both the ECDSA signatures and TESLA++ for verifying each packet and user validation [18]. In this modified scheme of TESLA that is TESLA++, the receiver shall store only the MAC address until it obtains the delayed key.

This is done basically to reduce the memory requirement as just the shortened version of the sender's data is stored by the receiver [14]. Moreover, TESLA++ is much more secure method of authentication than TESLA. It is resilient not only to the computation based DOS but also to the memory based DOS (Denial of services). TESLA++ utilized much simpler cryptographic technique when compared to that used in TESLA. The procedure for authenticating user validity in TESLA++ is detailed in. The paper [14] also proposes method to reject the unimportant MAC's that helps release memory in case of flooding that served to be a disadvantage in TESLA encoding. A mathematical representation of the encoded message using the two keys is given as.

ECDSA

The Elliptic Curve Digital Signature Algorithm is basically a mathematically deduced form of Digital Signal Algorithm. ECDSA is basically a mathematical depiction of the Elliptic curve analysis of the Digital signal algorithm. ECDSA has been detailed clearly by Don Johnson and his colleagues [15]. As per the paper ECDSA makes use of an asymmetric key pair obtained as a combination of a public key and a private key. The validation scheme in ECDSA basically consists of two steps. In the first step the sender's public key is validated. This thus helps in preventing attacks from invalid public keys. Next step is user Authentication by private key validation. This method ensures greater reliability.

5. Applications of VANET

There are a number of Applications to which vehicular ad hoc network VANETS can be put into. VANET focuses mainly on improving traffic safety and efficiency. It enhances security, promotes intelligent transportation and helps even in environment protection to a certain extent. All the applications make use of control functions that help in collecting and exchanging data between vehicles [6][7]. Information Dissemination, driving alerts and warnings, technical supports for accident and criminal investigation, electronic toll collection (ETC) and entertainment are some of the uses VANET can be utilized for. Based upon the type of communication that is vehicle to infrastructure (V to I) or vehicle to vehicle (V to V), the various applications of VANET can be classified into the following sub classes: -

1. Safety oriented sub classes
2. Commercial oriented
3. Convenience oriented and
4. Productive applications

5.1 Safety Applications

These basically involve special emphasis in increasing public safety and reducing the loss of lives. Such applications involve the use of Assistance Message (AMs), Information Message (IMs) and Warning Message (WMs). Safety applications can be grouped as under.

5.1.1 Real-Time traffic- The data relating to real-time traffic is stored at the road side units and is shared to the vehicles and as a result plays an important role in solving problems of jams and traffic congestions.

5.1.2 Co-operative Message Transfer- The vehicles that are slow or are stopped, co-operate and exchange messages to other vehicles to avoid potential accidents by automating applications like emergency.

5.1.3 Post crash notification- In case a vehicle is involved in an accident, it issues warning messages to the traveling vehicles so as to prevent any further mishap. The condition is well depicted in fig [1]

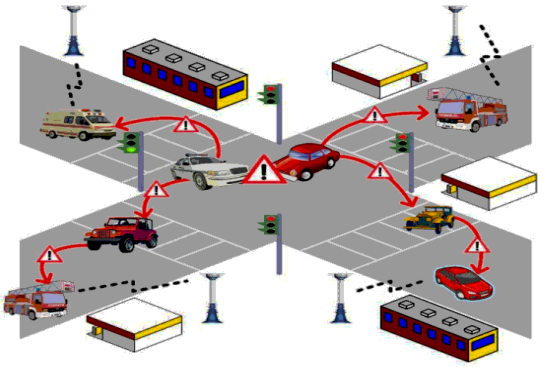

Fig.1. VANET Scenario

5.1.4 Road Hazard Control Modification- The vehicle leading other vehicles can easily notify them about the condition of the road, its nature or about the occurrence of a landslide.

5.1.5 Co-operative collision warning - Vehicles are issued to all devices to avoid crash router [23].

5.1.6 Traffic Vigilance – The cameras installed at the road side units shall help a great extent in reducing driving offences [22].

5.2 Commercial Applications

These basically involve the value added services (VASs) that emphasis on improving passenger comfort. Commercial applications can be grouped as under [22].

5.2.1 Remote Vehicle: personalization/Diagnostics- It helps to download personalized vehicles setting or upload vehicle diagnostics from/to infrastructure.

5.2.2 Internet Access: When the Road side units (RSUs) of a VANET work as router, then they can be judiciously used by the passenger to access the internet.

5.2.3 Digital map downloading: Depending upon the requirement, the driver while driving to a new area can download the map of the region for personal assistance.

5.2.4 Real time video Relay: The multimedia files like music, movies, news, e-lectures, e-books etc. can be accessed by the vehicles and moreover be shared or transferred even to other vehicles [9]

5.2.5. Value added advertisements: the services provides which may be shopping malls, petrol pumps, gas station or highways restaurants can proclaim their services to all the drivers or passengers within range even in absence of internet.

5.3 Convenience Application

These application forces on increasing the convenience of the driver, they deal with an effective traffic management. Convenience applications can be grouped under:

5.3.1 Router Diversions: with prior information the driver can modify the planning of a trip in case of traffic jams and road congestions.

5.3.2 Electronic Toll collection: It is one the important applications of VANET with such a facility, the drivers, without stopping can make the payment electronically making use of the network at the toll collection points.

5.3.3 Parking Availability: Whenever slots would be available for parking in an area, the vehicle would be notified about the availability through the use of the network.

5.4 Productive Applications

The productive applications can be grouped as under:

5.4.1 Time utilization – The accessibility of web and other entertainment facilities lets a traveler utilize his/her time even if he/she is stuck in a jam.

5.4.2 Fuel saving- since with the help of the electronic toll system vehicles pay the toll without stopping, so around 3% of fuel is saved [22].

6. Trust Evaluation

VANET is a highly open network. The validation of a new vehicle node trying to access the network is highly important to ensure the security of network. A trust evaluation based security authentication is proposed solution .it consists of two parts:

(i) Direct trust evaluation based secure authentication
(II) Indirect trust evaluation based secure authentication

The present trust management researches focus on evaluating the message and protecting the privacy.

6.1.1 Direct Trust Evaluation

A direct trust evaluation method is basically based on the historical security event record whenever the vehicles nodes and the authority units interact, the events relating security get recorded to the database. All the AUs (authentication units) that belong to a particulars organization can share the same database. The AU's can easily access the web. The recorded events in the database prove handy in evaluating the newer vehicle node and determining its credibility.

6.1.2 Indirect Trust Evaluation

For a group of vehicles communicating in a wireless network, it is their right to find out if they are to accept a new vehicle node or not. The vehicle network is analogous to an interpersonal network. The trust value and the recommendation of the other individuals decides the acceptance of the newer node. It is possible that some of the selfish nodes could deny the new vehicle node. Such a condition is undesirable for VANET. The malicious nodes thus need to be distinguished before calculating the indirect trust value in the indirect trust evaluation method. In this scheme correlation coefficient of the recommendation trust value is used for distinguishing the malicious nodes. All the recommendation trust values that are obtained from the malicious nodes are removed. Hence the malicious nodes aren't taken into consideration while the calculations of the indirect trust value.

Trust evaluation based on the historical security events and trust evaluations based on the recommendation trust value have been detailed in [25].

7. Existing Trust Models

Trust management in the vehicular ad hoc networks is one of the major concern for the establishment of a secure VANET environment. few trust models have been laid down by the researchers to promote the reliability of shared information within the vehicular networks. The proposed models can be grouped under three major categories that is entity oriented, data oriented and combined trust models [5].

7.1 Entity oriented trust model: this kind of model focuses on the authenticity of vehicles. For achieving this substantial information about the nearby vehicles as well as the sender is required by the trust models which is not obtained due to high mobility of the vehicles. So far, there are two typical entity oriented models: sociological trust models proposed by Gerlach [26] and multi-faceted trust management models proposed by minhas et al. [3] [28].

7.1.1 Sociological trust model: This model is based on hypothetical principal of trust and confidence without the formation of the architecture on how to identify from different types of trust at a time [3].

*7.1.2 Multi- faceted trust management mod*el: The multi-faceted trust models withholds a framework to deal with the selfish notions of the nodes which aims at maximizing a car owner's utility by transmitting false or manipulated messages questioning the authenticity of the received message. The model focuses on the role, experience, priority and majority based trust [5]. In this model a number of participating nodes are listed and in case of any discrepancy the information received from the various nodes is collected and scrutinized on the basis of past experience with nodes and trust the driver, on this basis decide on what massages to trust and react

accordingly. Mostly the information coming from the majority of the nodes is trusted and thus followed by the driver. One shortcoming of the model is that robustness has not been extensively addressed.

7.2 Data oriented trust model: Unlike the entity oriented model which aims at verifying the trust worthiness of the nodes or participating vehicles [27]. Data oriented trust model aims at the verification of the authenticity of incoming messages some data oriented trust model has been proposed like RMCV intrusion trust model, reputation based trust model, event based reputation system and road side aided data centric trust establishment [5].

Some of them discussed as follows:

7.2.1 Data centric trust establishment: Raya-et-al proposed a model to determine the authenticity of the data interchange with in the network this aims at the aggregation of the transmitted messages regarding the similar event and then combining them in to a robust decision scheme. These reports are then passed on to a decision logic module [5]. This module then evaluates the authenticity of the dynamic messages.

7.2.2 Information oriented trust model: Information oriented trust model is proposed by Gurung-et-all [5]. This model provides, the provision for incorporating into each participating node, a network setup with in

the VANET networks to detect the authenticity of the multiple messages received independently without relying on any centralized infrastructure. VANET's being ephemeral in nature limit the worthiness of this model which does not provide provisions to detect the trust worthiness of every part of the received message.

7.2.3Event based reputation model: Proposed by Ding-et-al [5] This model is aimed at detecting bogus warnings. This model assigns different rolls to the participating vehicles based on reputation mechanism like event reporter, observer and participant and each of them have their own way of determining the trust worthiness of the incoming messages.

7.3 Combine based trust: Aims to detect the authenticity of the massages through combined opinion of the various participating nodes. If the incoming messages is considered trust worthy by a majority of vehicles, then the message is evaluated to be authentic. In this regard a beacon trust management model [BTM] has been proposed [5].

Table 2. Comparison Between various trusts Model:

Trust Model	Types	Advantage	Disadvantage	Scenario
1. Entity oriented trust model	1. Sociological trust model. 2. Multifaceted trust management model.	1. Focuses on authentication of the vehicles. 2. Focuses on role, experience majority based trust 3. Verify trustworthiness of node.	1. Hard to obtain trust in the high mobility. 2. Robustness has not been extensively addressed.	Difficult to implement due to high mobility vehicles.
2. Data oriented trust model	1. Data centric trust establishment. 2. Information oriented trust model. 3. Event based reputation model.	1. Focus the authenticity of incoming messages. 2.Data bogus warnings	1. Does not detect trust worthiness of every part of the received messages.	Many vehicles take part with their specific task to do.
3. Combine based trust model	1. Beacon trust management model	1. Aims at authenticity of messages of the through opinion of other nodes. 2. Inhibit the attackers from broad casting messages.	1. Repeated opinion from different nodes may not be worthy for long term.	When various vehicles take part for better trust calculation trough opinions.

7.3.1 Beacon trust management model: Proposed by chain and wei [5]. Data authenticity depends on direct and indirect event based trust [5]. Authenticity of direct event based message is proposed by the position and motion justification of the vehicle. The receiving node analyses both the incoming message and beacon message to evaluate the authenticity of the messages. The evaluation of the authenticity through indirect event based involves the aggregation of opinions from various participating nodes. This model involves both the OBUs and RSUs to establish trust to propagate the opinions and inhibit the attackers from broad casting messages. One drawback of the model is that repeated opinions from different nodes may not be worthy for long term [3].

8. Conclusions and Future Work

After studying the various aspects of VANETs there lies a big scope of improvement in various areas which may include the time constraint, more security, flexibility, and much better response. This paper opens up the various areas of work for VANETs. There are various short comings in the various trust models previously proposed as mentioned in the review paper. One most important thing is the response time between the vehicles and this open up the big are of research work in various aspects of trust based computation. As the delay in response may lead to late decision making which will ultimately be a reason of hazardous situations like accidents, traffic etc.

In combined based trust model there is a huge scope of work in case of improving its response time, and there are lots of issues regarding calculation of trust during high mobility of nodes which need to be tackle more smartly, with better schemes.

There is huge scope of improvement in case of authentication schemes as there is large number of attacking ways. This review paper will allow you to understand the various area and the various scope of improvement in various techniques and schemes.

References

[1] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, Arturo Ribagorda, “Overview of security Issues in Vehicular Ad-hoc Networks,” Handbook of Research on Mobility and Computing , pp. 101-106, 2009

[2] Jie Zhang, “A survey on Trust Management for VANET,” International conference on Advanced Information Networking and Applications, IEEE computer society, pp. 105-112, 2011

[3] Shrikant S. Tangade, Sunil kumar S. Manvi, “A survey on Attacks security and Trust Management Solutions in VANETs,” Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE computer society, 2013

[4] Mohamed Salah Bouassida, “Authentication vs. Privacy within vehicular Ad hoc networks,” International Journal of Network Security, vol 13, no. 3, pp.121-134, Nov 2011

[5] Ahmad Soleymani et al “Trust Management in Vehicular Ad-hoc Network,” EURASIP Journal on wireless communication and Networking, 2015

[6] Xu,Y.N.,Fu,R.Z.,&Xu,Y.H. “Hardware design of noble MAC protocol for vehicle system,” Modern Applied Science, vol. 5, no. 3, pp 33-38 , 2011

[7] Chen, Y., Jian, W.,& Jiang, W.(2009) “An improved AOMDV routing protocol for V2V communication,” In IEEE intelligent vehicles symposium (IV”09, June 2009,pp. 1115-1120), 2009

[8] Vishal Kumar, Shailendra Mishra, Narottam Chand., “Applications of VANETs: Present & Future,” Communications and Network, 2013, vol 5, pp- 12-15

[9] Saleh Yousefi , Mahmoud Siadat Mousavi, Mahmood Fathy, “Vehicular International Conference on Advanced Information Networking and Applications,” IEEE Computer Society, pp. 105-112, 2011

[10] Shuai Zhangm, Jun Tao and Yijian Yuan, “Anonymous Authentication- Oriented Vehicular Privacy

Protection Technology Reserch In VANET," 2011 IEEE, pp. 4365-4368, 2011
[11] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE Journal on selected areas in communications, Vol. 25, No. 8, Oct. 2007
[12] Mohammed Salah Bouassida, "Authentication vs. Privacy within Vehicular Ad Hoc Networks," International Journal of Network Security, vol. 13, No.3, pp.121-134, Nov 2011
[13] C. SelvaL akshmi et al "Secured Multi Message authentication protocol for Vehicular Communication," International Journal of Advanced Research in computer and communication Engineering. vol-2, Issue 12, December 2013
[14] Na Ruan, Yoshiaki Hor, "Dos attack-tolerent TESLA- Based broadcast authentication protocol in Internet of Things," International Conference on Selected Topic in Mobile and Wireless Networking, pp-60-65, IEEE 2012
[15] Chen Lyu et al, "Efficient, Fast and scalable Authentication for VANETS," IEEE Wireless Communications and Networking Conference (WCNC): Networks, pp. 1768-1773, 2013
[16] Fei wang, "2FLIP: A Two-Factor Lightweight Privacy Preserving Authentication Scheme for VANET," IEEE transactions on Vehicular Technology, vol. 65, no. 02, pp. 896-911, 2015
[17] Yiliang Liu , Liangmin wang, "Message Authentication using Proxy Vehicles in Vehicular Ad Hoc Networks," IEEE Transactions on vehicular technology, vol.64, No.8, August 2015
[18] Smitha. A et al, "An Optimized adaptive algorithm for authentication of safety messages in VANET," 8th International Conference on communications and Networking in china (CHINACOM), pp.149-154, IEEE 2013
[19] M. Raya and J. P. Hubaux, "securing vehicular ad hoc networks," J. Computer Security, vol. 15, no. 1, pp.39-68, Jan 2007
[20] A. Studer et all, "Flexible, extensible, efficient VANET Authentication," J. communication Networking, vol. 11, no. 6, pp. 574-588, Dec. 2009
[21] C. Zhang et al., "An efficient message authentication scheme for vehicular communication," IEEE Trans. Vehicular Technology, vol. 57, no. 6, pp-3357-3368, Nov. 2008.
[22] Vishal kumar et al., "Applications of VANET: Present and Future," Communications and Network, 2013, vol. 5, pp. 12-15
[23] X. Yang, L. Liu and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," 1st Annual International conference on Mobile and Ubiquitous Systems: Networking & Services, MOBIQUITOUS' 2004, pp. 114-123, 2004
[24] http://www.teletrafficuk.com/products-concept-ii.htm
[25] Ao Zhou et al., "A security authentication method based on trust evaluation in VANETs," EURASIP journal on wireless communication and networking, pp. 1-8, Springer 2015
[26] M. Gerlach, "Trust for vehicular applications," in proceedings of the International Symposium on Autonomous Decentralized System, AZ, USA, pp. 295.304, 2007
[27] M. Raya et al., "on data-centric trust establishment in ephemeral ad hoc networks," Technical Report, LCA-REPORT-2007-003, 2007, pp. 01-11.
[28] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," International Journal of Computational Intelligence Theory and Practice (IJCITP), vol. 5, no.1, 2010.

Authors' Profiles

Akash vaibhav, Received the Bachelor of Technology in computer science and Engineering in 2014. He is a pursing Master of technology in Computer science and Engineering from Galgotias University, Uttar Pradesh India. His interest area is Mobile ad hoc Network.

Dilendra Shukla, Received the Bachelor of Technology in computer science and Engineering in 2014. He is a pursing Master of technology in Computer science and Engineering from Galgotias University, Uttar Pradesh, India. His interest area is Mobile ad hoc network and wireless sensor Network

Sanjoy Das did his B. E. and M.Tech, Ph.D in Computer Science. Presently, he is working as Associate Professor, School of Computing Science and Engineering, Galgotias University, India since September 2012. Before joining Galgotias University he has worked as Assistant Professor G. B. Pant Engineering College, Uttarakhand, and Assam University, Silchar, from 2001-2008. His current research interest includes Mobile Ad hoc Networks and Vehicular Ad hoc Networks, Distributed Systems, Data Mining.

Mr. Subrata Sahana received his M.Tech in Computer Science and Engineering form B.I.T. University, Mesra in 2010 and B.Tech degree in Computer Science & Engineering from West Bengal University of Technology in 2007.He was a Lecturer of Computer Science & Engineering department in RVSCET, Jamshedpur from 2007-08 and in V.I.T. University as Asst. Professor from 2010-2012. He is currently working as Assistant Professor at School of Computing Sciences and Engineering, Galgotias University and perusing Ph.D from School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi. His research area is Underwater Wireless Sensor Networks, Pattern Matching, Bio-informatics and Algorithm Design. Mr. Subrata Sahana has published numerous papers in International journals and conferences including IEEE and Springer.

Prashant Johri is Professor & Director GIMT(MCA), Galgotias Institute of Management & Technology UP Technical University, Greater Noida, India. He has published several papers in International/National Journals and Proceedings. His areas of research are Software Reliability, Data Mining and Warehousing, Big Data Security & Privacy, Big Data Open Platform and Pattern Recognition.

How to cite this paper: Akash Vaibhav, Dilendra Shukla, Sanjoy Das, Subrata Sahana, Prashant Johri,"Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.3, pp.36-48, 2017.DOI: 10.5815/ijwmt.2017.03.04