An Analytic Study of Security Solutions for VANET

Indu Bhardwaj
Ph.D Scholar
Galgotias University,Greater Noida, U.P.

Sibaram Khara, PhD
Dean Academics
Galgotias University,Greater Noida, U.P.

ABSTRACT
Vehicular ad-hoc networks (VANETs) are renowned form of mobile ad-hoc networks. In VANET, wireless device sends information to nearby vehicles, and messages can be transmitted from one vehicle to another vehicle or roadside infrastructure. So, using VANET can increase safety and traffic optimization. Similar to other technologies, in VANET there are some important and noticeable issues. One of the most important of them is Security. Since the network is open and accessible from everywhere in the VANET radio range, it is expected to be an easy target for malicious users. Therefore there is a need for optimizing the Security of vehicular Ad-hoc networks by Mitigating malicious attacks. This paper presents a review of security requirements, attacks and security challenges to implement the security measures in the VANET. Existing solutions proposed by different researchers are also reviewed and compared to find out the research gaps and scopes in the field of VANET security.

Keywords
VANET, Security, Attacks, RSU, Attack, Blackhole, Grayhole, DOS, Illusion, Wormhole, Sinkhole

1. INTRODUCTION
Traffic accidents are a serious problem globally. Approximately 1.2 million people are killed every year by road accidents. More health care money is spent treating crash victims than any other cause of illness [1]. Moreover traffic accidents result in long traffic jams, wasting many hours for peak time travelers. Road traffic safety has become major challenging issue worldwide. One possible way to enhance traffic safety and efficiency is to provide the prior traffic information to the vehicles so that they can use them to analyze the traffic scenario ahead. It can be achieved by exchanging the information of traffic environment among vehicles. All the vehicles are mobile in nature, consequently a self organized mobile network is needed which can be capable of operating without infrastructure support. With the advancement of microelectronics and wide deployment of wireless technology, it becomes possible to integrate node and network device into single unit and wireless interconnection, i.e. ad hoc network. Further this network is evolved as mobile ad hoc network [2].

Vehicular ad-hoc networks abbreviated as VANETs forms a novel class of mobile ad-hoc networks that uses moving cars as nodes in a network to create a mobile network. It turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range.

As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is expected that the police and fire vehicles will be the first to integrate this technology to communicate with each other for safety purposes.

VANET provides two types of communication. First is a pure wireless ad hoc communication where vehicle communicate with each other using short radio signals DSRC (5.9 GHz) without any support of infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle. Each node in VANET is equipped with two distinct units i.e. On Board Unit and Application Unit (AU) as shown in fig.1. OBU has the communicational capability whereas AU executes the program making OBU‘s communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the Internet [3].

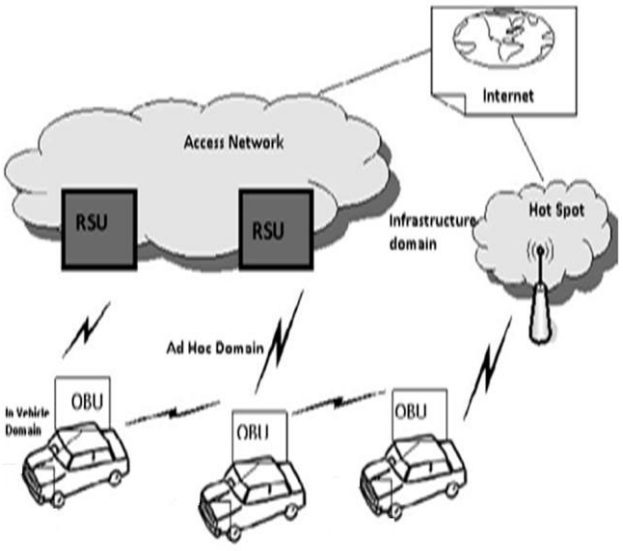

Fig.1: Conceptual model of VANET [3].

To create a VANET, 802.11p or 802.16 (WiMax) standard has been defined by IEEE. A Dedicated Short Range Communication (DSRC) is proposed which operates on 5.9GHz band and uses 802.11 access methods. It is standardized as 802.11p which provides short range communication with low latency. Europe has allocated 30 MHz of spectrum in the 5.9GHz band for DSRC to be used by Intelligent Transportation Systems (ITS). Also, USA has allocated 75MHz of spectrum in the 5.9GHz band for ITS. [4].

Several research projects have focused on this interesting and useful area in order to implement it in the best possible way. NOW (Network on Wheels), which is associated with Car-2-Car Consortium, has developed some protocols. Ford and General Motors have also created a Crash Avoidance Metric Partnership (CAMP) [5] in order to improve the VANET services.

The ultimate goal of all works toward VANET is to provide road safety information among the vehicles without negotiating security. Consequently the frequent exchange of information on the network clearly signifies the role of the security. Any successful attack can cause loss of lives or financial loss. Hence the security of the information exchanged between nodes in VANET is quite crucial need to be addressed including the security challenges and major attacks on VANET.

The paper is organized as follows: section two discusses the security concerns in VANET. Section three discusses the motivation behind this research area. Section four explores previous related works in the field of VANET security. In section five, we provide a comparison of various security protocols in VANETs and research gaps. Then later ending of the paper covers future research scopes and conclusion.

2. SECURITY CONCERNS IN VANET

Among all the challenges of the VANET, security got less attention so far. VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security.

2.1 VANET Security Requirements

In order to have a secure and dependable vehicular network, a number of security requirements must be considered. Some of these security requirements are the same for all networks but some are valid and specific to vehicular networks only.

1. **Authentication:** In Vehicular Communication every message must be authenticated, to make sure for its origin. Without authentication, illegitimate and malicious users can inject false messages into the network and confuse other vehicles by distributing false information.
2. **Integrity:** All messages which are sent and received on the network should be protected against alteration attacks. Integrity for all messages should be protected to prevent attackers from altering them, and message contents to be trust.
3. **Non Repudiation:** Non-repudiation will facilitate the ability to identify the attackers even after the attack happens. This prevents cheaters from denying their crimes.
4. **Privacy:** Driver privacy is an important issue in vehicular communications. Drivers don't want their personal and private information to be accessible by others. Since the vehicle information such as location, speed, time and other car data are transmitted via wireless communication, there should not be possible to infer the driver's identity from this information. Among this information, driver's location and tracing vehicle movements are more sensitive and must be taken into consideration carefully [7].
5. **Availability:** Vehicular network must be available all the time, for many applications vehicular networks will require real-time, these applications need faster response from sensor networks or even Ad Hoc Network, a delay in seconds for some applications will make the message meaningless and maybe the result will be devastating.

2.2 Security Challenges in VANET

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges [2]

1. **Real time Constraint:** VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.
2. **Data Consistency Liability:** In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.
3. **Low tolerance for error:** Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.
4. **Key Distribution:** All the security mechanisms implemented in VANET are dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.
5. **High Mobility**: The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces. Hence the design of security protocols must use the approaches to reduce the execution time. Two approaches can be implementing to meet this requirement.
6. **Low complexity security algorithms**: Current security protocols uses RSA based public key cryptography. But decryption of the message that used RSA algorithm becomes very complex and time consuming. Hence there is need to implement alternate cryptographic algorithm like Elliptic curve cryptosystems and lattice based cryptosystems.
7. **Attacks control**: Since VANET is open and accessible from everywhere in radio range so is prone to various attacks. These attacks are responsible for degrading the network performance and so need to be controlled.

2.3 Attackers on Vehicular Network

To secure the VANET, first we have to discover who are the attacker, their nature, and capacity to damage the system. On the basis of capacity, attackers may be three types.

1. **Insider and Outsider:** Insiders are the authenticated members of network whereas Outsiders are the intruders and hence limited capacity to attack.
2. **Malicious and Rational:** Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal profit hence they are predictable.
3. **Active and Passive:** Active attackers generate signals or packet whereas passive attackers only sense the network.

2.4 Attacks in the VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below [8]

1. **Denial of Service (DoS) Attack**
   In Denial of Service (DoS) attack, attacker takes control of the vehicular resources to transmit dummy messages or disseminate forged messages which make the network unusable to the legitimate vehicles. It means that the attacker jams the vehicle's communication channel by creating so many messages under attack that legitimate messages are not transmitted. The attack causes VANET to lose its ability to provide services to the legitimate vehicles resulting in decreased network performance.
2. **Black Hole Attack**
   In Black Hole attack, attacking node pretends to have shortest path to the destination and fascinates the source node to route through this node by providing the fake routing information. This way the source node transmits the data through malicious node considering the path as the shortest route between the source and destination. This attack results dropping or misuse the intercepted packets by malicious node without forwarding them.
3. **Wormhole Attack**
   In Wormhole attack, a tunnel is created by two or more malicious nodes in the network. The packets received by any malicious node at one end of the tunnel in the network are tunneled to another malicious node at other end of the tunnel and then these packets are retransmitted into the network. This attack prevents the discovery of valid routes in the network.
4. **Grayhole Attack**
   The grayhole attack resembles the black hole attack in a manner that it doesn't absorb or drop all the incoming packets as in backhole attack but it drops selective packets and forward rest of packets to the destination node. Grayhole attack is hard to detect because initially the attacking node behave as an honest node during the route discovery process, but then silently drops some of the data packets not only due to its malicious nature but also some times due to selfish nature, congestion or overload.
5. **Illusion Attack**
   In illusion attacks, the adversary deceives purposefully the sensors on his car to produce wrong sensor readings and thus incorrect traffic information. As a result of this, the corresponding system reaction is invoked and then it broadcast the incorrect traffic warning messages to neighbors. Thus, illusion Attack is successfully launched by the Attacker.
6. **Sybil Attack**
   In Sybil attack, the attacking node sends messages with multiple identities to other nodes in the network and creates an illusion of existence of multiple vehicles in the network. In this way the attacker takes the control of complete vehicular network to inject fake messages in the network. This attack impairs the functionality of whole network.
7. **Sinkhole Attack**
   In Sinkhole attack, all the network traffic is attracted by the attacker by broadcasting the fake routing information. This attack results in degradation of the network performance either by dropping the data packets or by modifying them.

3. MOTIVATION

Traffic congestion on the roads is today a large problem in big cities. The congestion and related vehicle accommodation problem is accompanied by a constant threat of accidents as well. Absence of road traffic safety takes a toll of precious human lives. Other negative consequences are related with time wastage, fuel waste and environmental pollution etc.

According to National Highway Traffic Safety Administration, the following figures indicate some of the consequences of recent car accidents [6].

- 6.3 million Police reported traffic accidents
- 43,000 people were killed
- Millions of people were injured

With these terrific numbers considerable governmental and other related agencies' as well as investments of vehicles manufacturers have been there trying to safety of roads. Accordingly, vehicle manufacturers are competing in equipping their vehicles with devices that collect data from the interior and exterior of vehicles and deliver it to a central processing unit that can analyze this data to boost the road safety while increasing the on-board luxury.

With increasing number of applications in VANETs, the various types of attacks on VANETs are also increasing. Due to these attacks, data confidentiality is threatened, life of the passenger may be at risk, and services may be denied to the authenticated users. Hence, importance has to be given to secure these networks from malicious users that threaten the security goals.

We know that most of the road accidents coverts into loss of life when proper medical aid is not given in minimum time. But With increase in security of VANET, the urgent piece of information will reach to the destination in the shortest time from shortest path. Hence information related to traffic, accidents, fire etc can be sent safely, securely and speedy so that the necessary action can be taken within the time without taking toll of precious life and resources.

4. RELATED WORKS

The problem of securing communications in VANETs against malicious attackers has been previously explored by various authors in research literature. Table 1 summarizes some previous works related to VANET security in the research community.

Table 1. Literature review on VANET security

Sr. No.	AUTHORS	TITTLE	TECHNOLOGY/ TECHNIQUE USED	ATTACKS COVERED	SECURITY DIMENSIONS (SD)	REVIEW
1	Shiang-Feng Tzeng, et al. [10] (2015)	Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET	The system initialization, anonymous identity generation, message signing, and message verification.	Forgery attack	Message authentication, integrity, non-repudiation	Effective solution for forgery attacks only. No solution for other attacks.
2.	Yiliang han, et al. [11] (2014)	Aggregate syncryption based hybrid authentication protocol for VANET	Aggregate signature and Batch-verification	No specific attack is covered	Privacy, Authentication	Good privacy scheme with less overhead No solution for attacks
3	Pouyan, et al. [12] (2014)	Sybil Attack Detection In Vehicular Networks	Tracks the irregularities in the vehicular movement to track the malicious nodes	Sybil attack and prankster attack	Privacy	Effective against the Sybil and Prankster Attacks
4	Manish Kumar Soni et al. [13] (2014)	HAP: Hybrid Authentication Protocol for Vehicular Ad Hoc Network	combines the concept of anonymous certificate scheme with the group signature scheme	black hole attack	Authentication and reliability	Effective against black hole attack. No solution for other attacks
5	Adetundji Adigun, et al. [14] (2013)	Protocol of Change Pseudonyms for VANETs	Asymmetric and symmetric cryptography	No solution against attacks.	Privacy, authentication Non-repudiation	Solution for data privacy not against attacks
6	Ghaleb, Fuad A., et al. [15] (2013)	Security and privacy enhancement in vanets using mobility pattern	Mobility pattern based Misbehavior detection	No solution against attacks.	Privacy	Effective for anonymous message detection. No solution against attack
7	Alam, Nima, et al. [16] (2013)	Relative positioning enhancement in VANETs: A tight integration approach	Realistic Vehicular movement on Road network	No solution against attacks	Privacy	Solution for filtering malicious nodes, no sol. against attack
8	Tong Zhou et.al. [17] (2011)	P2DAP – Sybil Attacks Detection in VANET	passive overhearing by s set of fixed nodes	Effective against Sybil attack	Privacy	Effective against the Sybil. No solution for other attacks
9	Priya Karunanithi, et al. [18] (2011)	Efficient Distributed Group Authentication Protocol for VANET	The group signature and batch verification schemes	No solution against the Malicious attacks	Authentication and conditional privacy	Solution for conditional privacy but not effective against attacks.
Sr. No.	**AUTHORS**	**TITTLE**	**TECHNOLOGY/ TECHNIQUE USED**	**ATTACKS COVERED**	**SECURITY DIMENSIONS**	**REVIEW**
10	Catalin Gosman, et al. [19] (2010)	Security protocol for vehicular distributed systems	DSA key pair	avoids DOS attacks	Data integrity, Authentication, non-Repudiation	More overhead and time delay

11	X. Lin, et al. [20] (2007)	GSIS: A secure and privacy-preserving protocol for vehicular communications	group signature and identity (ID)-based signature techniques	No solution against attacks	security, privacy,	Good for security and privacy but not effective against attack.
12	P. Papadimitratos et al [21] (2003)	Secure Data Transmission in Mobile Ad Hoc Network	MAC (Message Authentication Code)	Information Disclosure	Authentication	Provides authenticity not other security dimensions.
13	Y. C. Hu et al [22] (2003)	SEAD: Secure efficient distance vector routing for mobile wireless ad-hoc networks	One Way Hash function	DoS, Routing Attack, Resource Consumption	Authentication, Availability	Effective solution for DOS & replay attacks but achieve all security dimensions.
14	Y. Chun Hu et al [23] (2002)	Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks	Symmetric Cryptography	DoS, Routing Attack, Replay Attack	Authentication	Provides authenticity not other security dimensions.
15	B. Dahill et al [24] (2002)	A Secure Routing Protocol for Ad Hoc Networks	cryptographic certificate	Replay Attack, Impersonating, False warning	Authentication, Message Integrity, non-Repudiation	Address some attacks only.

5. COMPARISON AMONG THE EXISTING TECHNIQUES AND RESEARCH GAPS

As discussed in table 1, there are many solutions provided to secure VANET by mitigating attacks. These solutions are compared on basis of some security parameters to obtain the research gaps. Comparison of some security solutions is shown table 2.

Table 2. Comparison of some security solutions of VANET

Security parameters	**Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET**	**Aggregate syncryption based hybrid authentication protocol for VANET**	**Protocol of Change Pseudonyms for VANETs**	**P2DAP – Sybil Attacks Detection in VANET**	**Security protocol for vehicular distributed systems.**
Authentication	√	√	√	×	√
Integrity	√	×	×	×	√
Non-repudiation	√	×	√	×	√
Privacy	×	√	√	√	×
Availability	×	×	×	×	×
No. of attacks covered	One (Forgery attack)	No	No	One (Sybil)	One (DOS Attack)

The existing VANET techniques have been studied in the collective manner in order to understand their shortcomings in comparison with other similar techniques. The comparison presents the following Gaps.

1. In VANETs, attackers can inject, forge, replay, and drop messages in order to violate information integrity, authenticity, user privacy, and system performance. But no security solution satisfies all primary security requirements together.
2. Some of the existing solutions to attain security dimensions contain drawbacks, which makes them

vulnerable to attacks. So a balance between attacks solution and security dimension is missing.

3. There is no central solution for VANETs which offers a complete VANET security.
4. Mitigation of one attack does not create secure VANETs. It requires mitigating most of the prominent attacks with one solution in order to facilitate the stable movement.
5. Security solutions are lacking to provide communication between vehicles in minimum time. The delivery delay sometimes makes the accident messages meaningless.

6. RESEARCH SCOPES

The future of VANET is very bright as new ideas and scopes are coming up in recent times. Some research scopes and enhancements possible in area of literature survey are as follows.

1. **Central solution for secure VANETs by balancing the routing techniques without negotiating security and overhead**
   Researchers are working in VANET to provide safety and security to mankind. But till date no fully developed vehicular network exists for security purpose around world. Consequently, there is a scope to develop central solution for VANETs which offers a complete VANET security. In the field of Information Technology, it is argued that a guaranteed 100% security is not realistic and besides security, the mechanism should preserves privacy, information authenticity tracking with minimum data storage and cryptographic overhead Therefore the best approach to provide a central solution for VANET security is to make a perfect balance between the routing techniques, security dimensions including attacks and overheads as shown in fig.2. The intersection point of these three issues will able to achieve an acceptable level of security and satisfy effectively all the design requirements for deployment of VANET in real scenario.

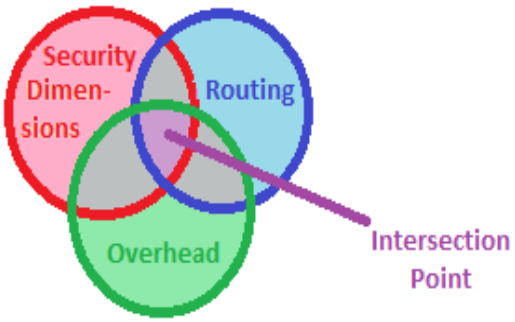

Fig. 2: Central solution for VANET

2. **Mitigating most of the prominent attacks with one solution**
   Lot of research work has been done by researchers to mitigate attacks but the proposed solutions are attack specific i.e. different approach for each attack. There is no mechanism till date which can mitigate all attacks or most of the prominent attacks with single approach.
3. **Image processing**
   Image processing is a wide area of research with a huge scope. By using advanced image processing algorithms, the vehicles can track a person by using cameras on the vehicles. This application is used for tracking terrorists on the roads. If a terrorist's image matches with the database image then the vehicle suddenly broadcasts the information to the nearby police station. The videos of the street can also be recorded for criminal investigation.
4. **Vehicular cloud**
   Implementation of cloud computing concepts can provide services in software, hardware and platform level. The main use of cloud computing is to provide on-demand resources to the users using virtualization. By using cloud, many applications are projected like multimedia services, content delivery, location sharing, e-applications, P2P services (Peer-to-Peer) and so on. The vehicles with internet access can form a network cloud to provide content delivery and information sharing. The storage can also be used as a service because cars have terabytes of memory. This technology can be used for many applications and it will be an emerging area of research.
5. **Fault tolerance**
   VANET is a network and it consists of vehicles which act as nodes. The nodes can fail at any time because of hardware tampering or software fault and this leads to the generation of faulty nodes in the system. At the time of routing, if a vehicle sends data to a faulty vehicle then the data may be dropped and delay increases. Hence, there should be a recovery mechanism which recovers to protect the network from these faults. The generation of new fault tolerance techniques nowadays is also an emerging area of research.
6. **Seamless interfacing of the VANETs with existing infrastructure**
   Most of the schemes for VANETs assume the use of Roadside Units (RSUs) that are deployed to assist the vehicles in performing the protocols. However, the deployment of RSUs is costly. Interfacing the VANETs with existing wireless infrastructure, such as the cellular network or the satellite network can improve the cost-effectiveness, but will gives rise to new security, privacy, and access control concerns.

7. CONCLUSION

Security is the major issue to implement the VANET. In this paper, the security requirements, attacks and security challenges to implement the security measures in the VANET are discussed. Also the various solutions proposed by different researchers to secure VANET are reviewd and compared. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data. The study of attacks revealed that the attacker generally targets the network layer directly or indirectly hence the routing protocol must be secure enough to prevent the most types of attacks. Security solution must preserve all the security requirements like authentication, integrity, availability and privacy which are more targeted.

8. REFERENCES

[1] Yih-Chun Hu; Kenneth P. Laberteaux. 2006. Strong VANET Security on a Budget" In Proceedings of Workshop on Embedded Security in Cars (ESCAR).

[2] S. Sesay, Z Yang and Jianhua He, 2004. A survey on Mobile Ad Hoc Network, in Information Technology Journal, (2004) 168-175,

[3] Moustafa,H.;Zhang,Y. 2009. Vehicular networks: Techniques, Standards, and Application. in CRC Press, (2009).

[4] Y.- C. Hu and K. Laberteaux, 2006. Strong Security on a Budget, in Workshop on. Embedded Security for Cars, (Nov. 2006).

[5] Maxim Raya e al., 2005. The Security of Vehicular Ad Hoc Networks, SASN'05, (Nov 2005) , Alexandria, Verginia, USA, 11-21.

[6] ElmarSchoch, Frank Kargl, Michael Weber, and Tim Leinmuller, Communication Patterns in VANET, IEEE Communications Magazine, 46, (Nov 2008),119–125.

[7] T. Leinmüller, E. Schoch, C. Maihöfer, 2007. Security requirements and solution concepts in vehicular ad hoc networks, in Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services, (2007), 84–91,.

[8] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, 2010. Overview of Security issues in Vehicular Ad Hoc Networks, Handbook of Research on Mobility and Computing, (2010).

[9] Murthy, C. S. R.,Manoj, B. S. 2011, Ad Hoc Wireless Networks: Architectures and Protocols" . PEARSON,ISBN 81-317-0688-5, (2011).

[10] Horng, S.; Tzeng, S.; Li, T.; Wang, X.; Huang, P.; Khan, M., 2015. Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET, IEEE Transactions on Vehicular Technolog, (2015).

[11] Yiliang Han; Dingyi Fang; Zelun Yue; Jian Zhang ,2014. SCHAP: Aggregate syncryption based hybrid authentication protocol for VANET in Springer international publishing Switzerland, (2014).218-226.

[12] Pouyan, Ali Akbar, and Mahdiyeh Alimohammadi. 2014. Sybil Attack Detection in Vehicular Networks In Computer Science and Information Technology journal, (2014). vol.2 , no.4, pp. 197 – 202.

[13] Manish Kumar Soni and Ashish Vashistha. 2014. HAP: Hybrid Authentication Protocol for Vehicular Ad Hoc Network in IJCA Proceedings on National Seminar on Recent Advances in Wireless Networks and Communications NWNC(3):10-14, (April 2014).

[14] Adigun; Bensaber.;Biskri. 2013. Protocol of Change Pseudonyms for VANETs in IEEE 38th Conference on Local Computer Networks Workshops (LCN Workshops), (2013).

[15] Ghaleb, Fuad A., M. A. Razzaque, and Ismail Fauzi Isnin. 2013. Security and privacy enhancement in vanets using mobility pattern. In IEEE Fifth International Conference on Ubiquitous and Future Networks (ICUFN), (2013).

[16] Alam, Nima, A. Tabatabaei Balaei, and Andrew G. Dempster. (2013). Relative positioning enhancement in VANETs: A tight integration approach. IEEE Transactions on Intelligent Transportation Systems , vol.14, no.1, (March 2013) 47,55.

[17] Tong Zhou; R.R Choudhury; Peng Ning; K Chakrabarty. 2011. P2DAP – Sybil Attacks Detection in VANET in IEEE Journal on Selected Areas in Communications Volume:29 , Issue: 3 (2011).

[18] Priya Karunanithi, Komathy Karuppanan. 2011. Efficient Distributed Group Authentication Protocol for Vehicular Ad Hoc Network In Proceedings of International Conference, ACC 2011, vol 192, (2011) 624-633.

[19] Catalin Gosman, Ciprian Dobre, Valentin Cristea, 2010. A Security Protocol for Vehicular Distributed Systems, in 12th international conference on symbolic and numeric algorithms for scientific computing (SYNASC), IEEE digital library (2010).

[20] X. Lin, X. Sun, P. H. Ho, and X. Shen, 2007. GSIS: A secure and privacy-preserving protocol for vehicular communications, IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, (2007).

[21] P. Papadimitratos and Z. J. Haas, 2013. Secure Data Transmission in Mobile Ad Hoc Network, in ACM Workshop on Wireless Security, San Diego, CA, (September 2003).

[22] Y. C. Hu, D. B. Johnson and A. Perrig, 2003. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, in Elsevier B. V. (2003) 175-192.

[23] Y. C. Hu, A. Perrig and D. B. Johnson, 2002. Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks, MobiCom'02, (2002) 23-26.

[24] Dahill, B.N. Levine, E. Royer and Clay Shields, A Secure Routing Protocol for Ad Hoc Networks, in Proceeding of IEEE ICNP (Nov. 2002), 78-87.