Challenges in Securing VANET: The Intelligent Transportation System

Anil Kumar Dhami *anildhami.jk@gmail.com*
Dept.of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad
Allahabad, India

Neha Agarwal *nehaagarwal.jk@gmail.com*
Dept.of Computer Science and Engineering
Motilal Nehru National Institute of Technology Allahabad
Allahabad, India

Abstract

With the advancement in the wireless communication, various technologies have been deployed for managing efficient vehicular communication. Such system for vehicular communication can be considered as an intelligent transportation system. VANET is emerging as the most challenging technology integrating ad hoc network, WLAN and cellular technology. It is helpful in developing intelligent transportation system for improving traffic management, roadside safety, cooperative driving etc. VANET is an application or subset of MANET.

For the implementation of VANET, security is an important constraint. Most of the research concerted efforts in academics and industry are focused to provide efficient security architecture for VANET; to protect the network from adversary nodes and attacks. This paper focuses on the security challenges in VANET, especially for achieving privacy and their possible solutions.

Keywords: VANET (Vehicular ad hoc network), MANET (Mobile ad hoc network), WLAN (Wireless LAN), CRL (Certificate revocation list), VPKI (Vehicular public key infrastructure), TPD (Temper proof device).

1. INTRODUCTION

The growing population and mobility of people, vehicles, and goods on the roads makes the worst transportation situation for driving. Traffic congestion on the roads makes a situation like battlefield which makes the huge wastage of time and fuel. The road deaths has crossed the limit of about 1.2 million people yearly worldwide [1] and road injuries, fatalities are more than these numbers. Numerous efforts have been introduced to overcome this problem and to provide secure, safer and efficient driving conditions but they are not sufficient to solve these road or transportation related problems.

VANET is the most challenging instantiations of the MANET [2], which incorporates new generation wireless technologies and step towards intelligent transportation system. It provides efficient vehicular communication, cooperative traffic monitoring, and collision prevention which makes driving conditions safe and secure.

In the year 1998, engineers from Delphi Delco Electronics System and IBM Corporation proposed a network vehicle concept to provide various range of applications [3] and with the advent of wireless technology concept of new car came into existence. In the recent years many projects have been launched in the direction of achieving the successful implementation of vehicular networks.

Car to Car communication consortium developed by European industry for car to car communication [4] (C2C-CC) is one of the most well known project for vehicular communication systems, active safety applications prototyping and demonstrations. SEVECOM [5] is a European Union project for ad hoc networking, accurate relative localization, dynamic local traffic maps, and sustainable deployment strategy. IEEE P1609 [6] is an another standard for wireless access in vehicular environment(WAVE) – resource manager, security services, physical and medium access control for V2V and V2I communication. Except these there are many other projects like NOW, VSC and DSRC consortium [7] in USA etc working on VANET.

There are various aspects of vehicular communication. The radio used for the communication is referred as DSRC (dedicated short range communication), in the US a new band is allocated (in 1999) by the FCC (Federal communications commission) for these application. The allocated band was 75 MHz at 5.9 GHz frequency for Intelligent Transportation System [7].

Our paper is organized as follows. Section 2, discusses about the system model of VANET, applications and characteristics of VANET. Section 3, consists security issues of VANET. Section 4, explains security requirements and architecture of VANET. Section 5, includes the possible security solutions to improve the functioning of VANET. Finally section 6, discusses the conclusion and direction for future scope of the VANET solutions.

2. SYSTEM MODEL: VANET

The complete architectural model of VANET is represented in fig. 1. This section introduces the network architecture and applications of VANET.

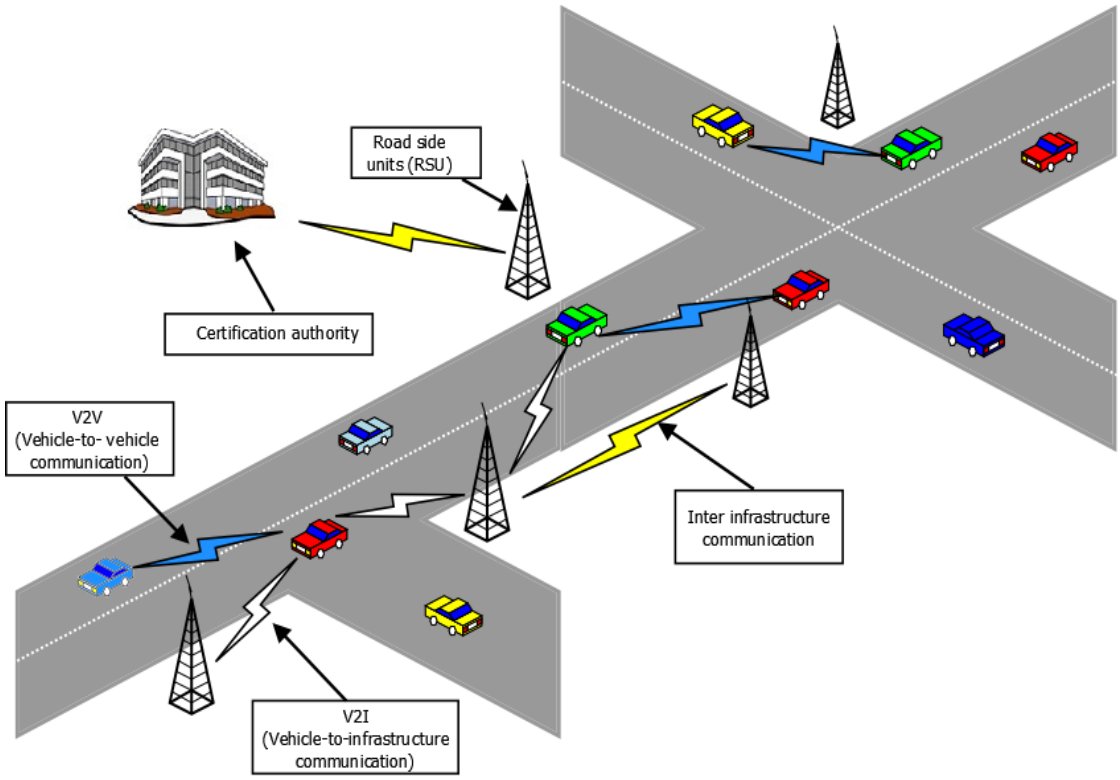

FIGURE 1: VANET architecture with vehicles and RSUs.

2.1 Network architecture and vehicular communication

VANET consists of two types of communicating nodes one is vehicles, which are infrastructure-less and another is road side units i.e. road side infrastructure like – base stations, access points

etc. The road side infrastructure (RSU) connects the vehicular network to a central system or to the Internet. Vehicles are equipped with OBUs (on board units) for communicating among vehicles and with RSUs. OBU consist set of processors and sensors for collecting data, GPS (global positioning system) for vehicle speed, direction and position and EDR (event data recorder) [8]. The network architecture of VANET can be of three categories:

1. Pure cellular/WLAN (fixed cellular gateways and WLAN access points)
2. Ad hoc
3. Hybrid architecture (combination of pure cellular/WLAN and ad hoc) [9].

The communication between the nodes can be either V2V (vehicle- to-vehicle communication) or V2I (vehicle-to-infrastructure). The communication can be felicitated by either DSRC (dedicated short range communication) or IEEE 802.11 technology family. Cellular communication can be used for long range communication (V2I) and Wi-Fi IEEE 802.11 may provide short range communication (V2V). IEEE 802.11p WAVE is defined to allow both V2V and V2I communication

2.2 Characteristics and challenges of VANET

- **Mobility:** In VANET the communicating nodes are vehicles so mobility of the nodes are very high in such networks. The connection between nodes exists for very short time period, thus the mobility induces another challenge in security of VANET.
- **Scalability** is another major challenge in VANET, because in the world such network is having more than 750 million nodes [2] and the numbers of nodes are increasing day-by-day.
- The connectivity between nodes is volatile, which change frequently with connection exist for a short time period.

2.3 Application of VANET

The main purpose of VANET is to provide intelligent transportation system. The application can be categorized as below [10]:

- Safety related messages
  1. Traffic information messages: used for traffic condition in a particular region.
  2. General safety messages: used for cooperative driving, collision avoidance i.e. public safety messages.
  3. Liability messages: most important messages exchange at the time of accidents which needs real time consideration.
- Other application
  1. Toll application (electronic toll collection system).
  2. Gaming, exchange of multimedia content etc.

3. SECURITY ISSUES IN VANET

Security is a major challenge in vehicular networks and needs more attention. VANET application like safety related messages, which consists life critical information needs real time consideration. So, one has to make sure that such messages cannot be modified by the attacker and at the same time reliability of message, privacy and liability of driver is also important.

Characteristics of VANET like size of network, mobility of nodes, frequent short term connections between nodes, geographical positions of nodes adds more challenges to secure the VANET rather than other networks. Security attacks and requirements are discussed in this section.

3.1 Attacks on VANET

This section introduces the security threats face by VANET, since the application of vehicular network is concentrated on safety related message, cooperative driving etc. So we focus on the attacks only against messages, privacy of user, not the physical attacks against vehicles.

The capacity of an attacker is defined by four dimensions i.e. [11] the attacker can be either an *insider*, a valid authenticated user of network or an *outsider*, a user from outside of the network,

having *malicious behave* (attacker only perform network monitoring without harming it) or *rational behave* (attacker harms the network for personal benefits) by applying *active method* (done by generating signal like physical jamming) or *passive method* (only listening the network) and the scope of attacker can be local within V2V or extended [11].

- **Denial of service Attack**

DoS attack is performed by attacker against the availability of the network resource. In this, attacker jams the channel and prevents the critical information from arriving. Attacker take the control of network resource which may cause an accident and injects false traffic information [12] [11].

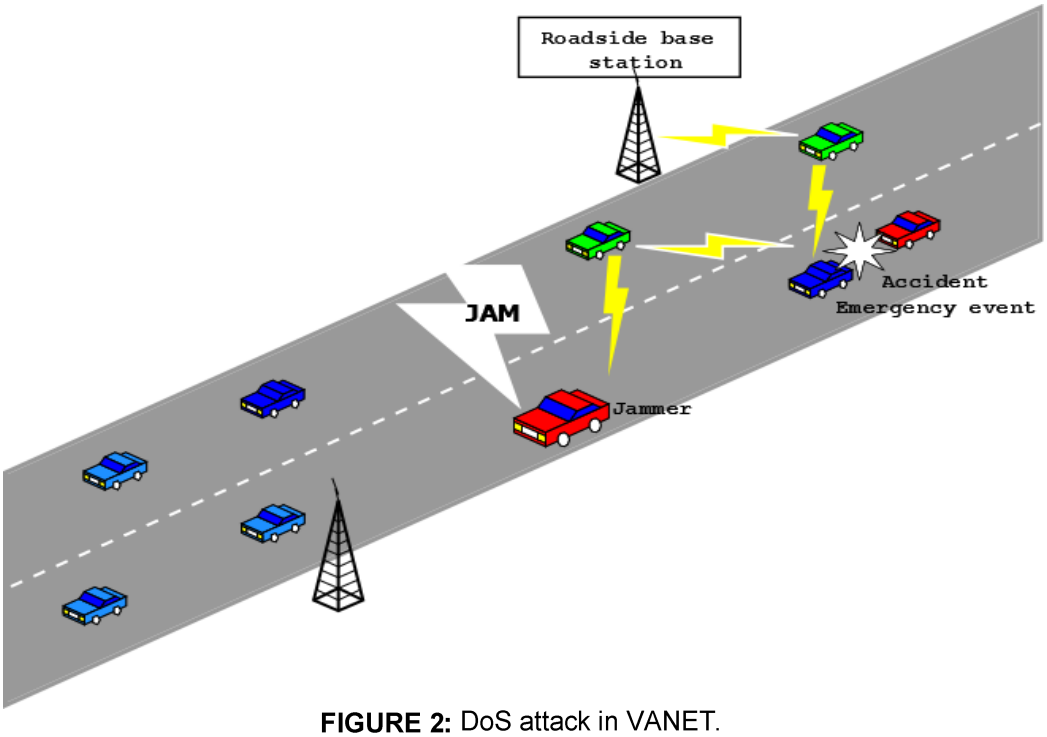

FIGURE 2: DoS attack in VANET.

- **Sybil attack**

This attack can be perform by attacker by creating fake information [11] i.e. the attacker creates a large number of pseudonymous, and acts like more than hundred vehicles and creates bogus or falsify traffic info message to convey other vehicles.

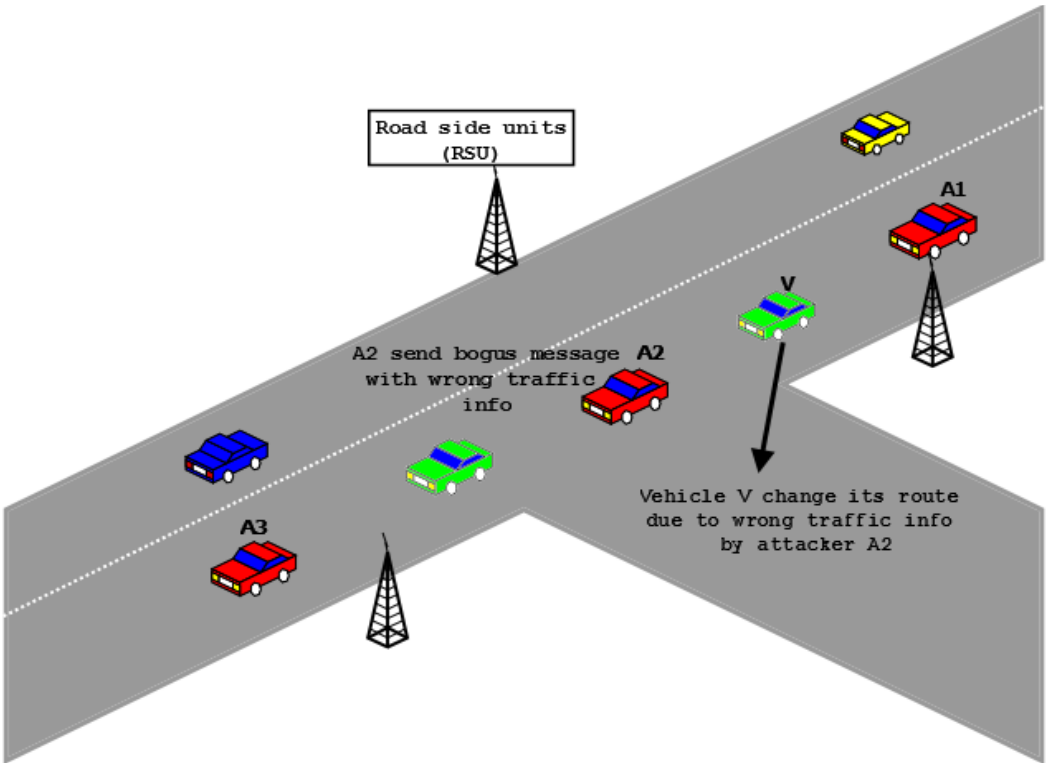

FIGURE 3: Sybil attack in VANET

- **Replay attack**

In this attack the attacker replay the transmission of earlier information or delay the transmission for confusing the road side authorities [12]. This attack is possible because the security architecture of 802.11 doesn't contain sequence number or timestamp and has no protection against replay attack.

- **Wormhole attack**

Wormhole attack [11] is performed by tunneling of packets, done between two colluding attacker controlling at remote locations in vehicular communication.

- **Alteration attack**

In this attack, the attacker alters the original data of the transmission, delays the information and replays the earlier transmission [12].

- **Message suppression attack**

An attacker selectively drops the packets which consists life critical information messages for the receiver, or suppress them, use them at another time [12]. The main aim of such attack is to restrict form registration and to ensure the authorities from learning about the collision involving vehicle to avoid the delivery of liability messages.

4. SECURITY REQUIREMENTS OF VANET

As far as security requirements are concerned the applications of VANET are focused on safety messaging, cooperative driving, toll application etc. Therefore the integrity, liability of message, liability of the user has to be ensured and at the same time privacy has to be looked upon. A secure VANET system should satisfy following requirements:

- **Authentication:** In vehicular communication source of the message should be legitimate i.e. authenticated user, because decisions are made by the vehicles on those messages. So we need to authenticate the user [10] [12]. The legitimacy of message is also necessary because the source can be authentic but message consists false data [11].

- **Availability:** VANET needs real time considerations so communication channel and resources needs to be available all the time. Denial of service kind of attack on the network brings it down, so availability should be also supported by alternative means [11].
- **Non Repudiation:** It felicitates the ability to identify the attackers even after the attack, as the attacker or user can't deny the transmission [12].
- **Privacy:** Keeping the information of the drivers away from the unauthorized attackers like info of driver, position etc. [11].

4.1 Analysis of current security solutions in VANET

In VANET many security solutions have been proposed, this section introduces the possible solutions with respect to message legitimacy, authentication, achieving privacy and misbehaves detection.

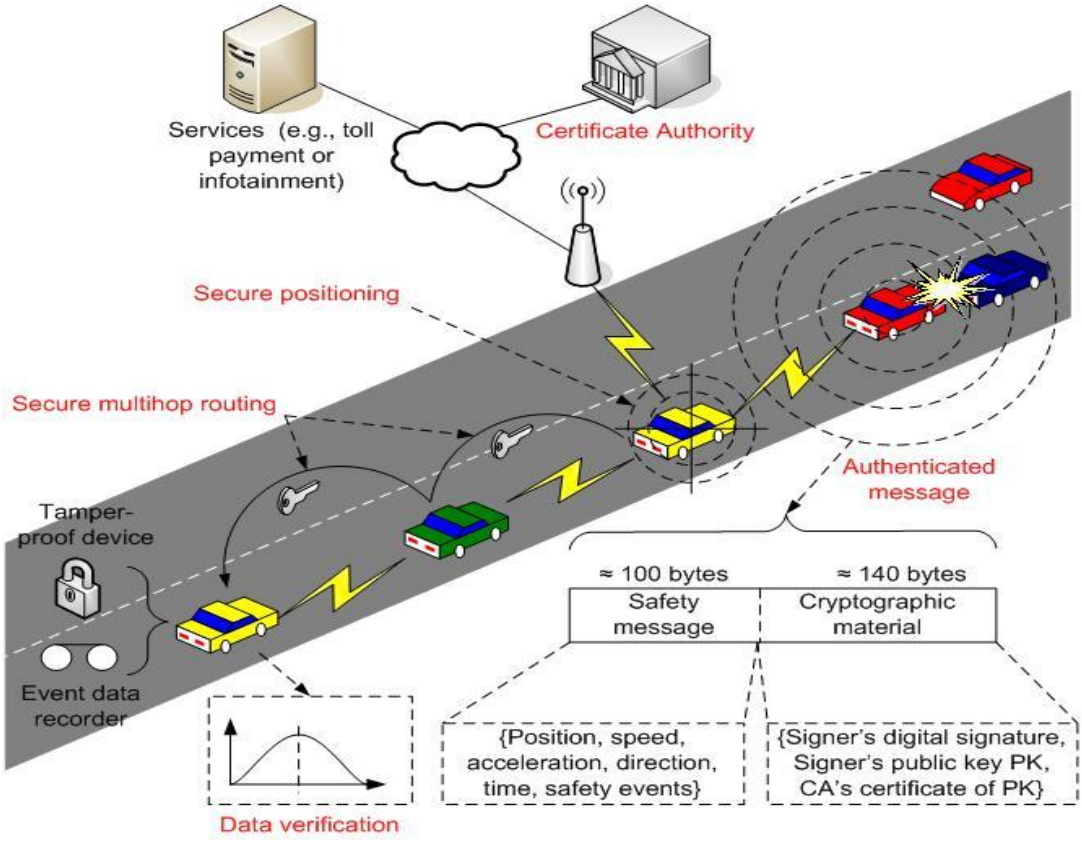

FIGURE 4: PKI Based Security Architecture in VANET [19]

- **VPKI**

PKI is widely accepted solution [13] [14], as described in IEEE 1609 family of standards for WAVE. Fig 4 [19] shows the PKI based architecture for VANET [12]. Under the VPKI solution each vehicle has a public/private key, a unique and certified identity given by CA (Certification Authority). Vehicle sends the message by signing (message is hashed before sign) with its private key and includes the CA's certificate as below [11]

$V \rightarrow *: M, Sig_{PrKv}[M|T], Cert_V$, where vehicle V sends the message (M) by signing it with private key (PrKv) and message is concatenated with timestamp (T)

obtained from TPD for message freshness then include certificate ($Cert_V$). Receiver verifies the message using its certified public key [11].

The certificates are valid for limited time period, after their generation CA have the authority to revoke vehicles certificate. In paper [17] [18] authors talk that vehicles can carry trusted component TPD in which the secret information like cryptographic key, certificates is stored. This device is responsible for signing outgoing message. If the sending message is Liability related message then this should be stored in EDR (Event Data Recorder) including signature for further investigation if needed.

Vehicular public key infrastructure met approximately all the security requirements of VANET but with its disadvantages it throws some major challenges notably certificate revocation. The most common way of certification revocation is the distribution of CRL which consist revoked certificates [19]. IEEE 1609.2 draft standard [16] proposes the distribution of CRLs and short lived certificates but doesn't propose any mechanism of achieving this. Due to the scalability of the system with millions of nodes, the main concern of using PKI system is to manage CRLs.

To overcome the problem of managing CRLs some solutions has been proposed which includes certain protocols namely RTPD (revocation of temper proof device), RCCRL (revocation protocol using compressed certificate revocation list), and DRP (distributed revocation list) [2]. RCCRL presents a way to compress the CRLs using *bloom filter* [2] and it revokes the certificates just similar to CRLs, RTPD is applied whenever it needs to revoke all the certificates of a vehicle i.e. CA can directly instruct the TPD to erase it's all cryptographic detail.

[20] Proposed another scheme based on TACK (temporary anonymous certified keys) for message authentication, who's CRLs is linear with respect to revoked certificates. It uses the concept of group signature, having three main entities managing authority (root of trust), set of valid regional authorities (intermediary authority) and a set of vehicles. Similarly [21] proposed another scheme based on pseudonymous authentication scheme for achieving smaller CRL, its architecture consist of trusted authority (issues certificate for certain RSU and series of pseudonymous certificate for vehicles) and vehicles or OBUs.

- **Secure group communication:**

Group communication is another attempt to achieve privacy and authentication in VANET. Secure communication can be achieve by using shared secret group key, use of symmetric key [11] for authentication can reduce the security overhead. [22] Propose the concept of location based groups for communication in which group is define by dividing the road into cells and vehicle closest to the center of the cell is group leader dynamically. Vehicles periodically broadcast their public key, and group leader distributes the group key among its members. This technique improves the performance when vehicle travels together in platoon form.

The scheme has some drawbacks like it put some extra overhead when each time a new vehicle joins or leave the group, lack of group boundaries due to the high mobility and less effective when there is less number of vehicles.

- **Privacy through pseudonyms certificates:**

Pseudonyms certificate is another widely accepted solution; many schemes are based on this. [23] Proposed a scheme in which security architecture is organized in certain layers i.e. lower layers and higher layers. Higher layers consists pseudonym and revocation layer while lowest layer is used for vehicle registration and identification. Pseudonym layer provide anonymity similar to certificate given to node, scheme used dynamic pseudonyms to provide privacy and escrow authority for revoking while revocation layer is responsible for excluding nodes. [24] Proposed another scheme based on pseudonyms and group signature, which referred as baseline pseudonyms (BP).

The solutions which we have focused above provide secure and reliable network and try to keep attackers away from disrupting the network. There are certain schemes for detecting and evicting the faulty or misbehaving nodes [25].

5. DISCUSSION

This section discusses some other critics for possible solution and some of our proposals, which are extension of existing solutions. VPKI (Vehicular Public Key Infrastructure) is most widely accepted valid solution but still certain issues like node revocation, and CRL size needs to be addressed. Some solutions are proposed for both issues, like minimization of CRL size with pseudonymous certificates. Due to the scalability issue in VANET the size of CRL is still very large, so solution like use of bloom filter together with the pseudonyms approach may prove good. Instead there's need of some research for minimizing the size of CRL and verifiability of pseudonyms. One solution may be use of hierarchical CRL list distribution by the issuer i.e. local and global management of CRL list. Denial of service and Sybil attack are most vulnerable to the network, so misbehave detection and revocation is necessary for defending it. RSU should be provided more functionality and utilize them in more managed way, to achieve secure vehicular communication.

Since liability messages needs real time consideration but each time when any message is send it needs to be signed and then broadcast, so cryptographic process may take some time in message authentication and verification. This delay is painful in case of such messages. So some mechanism needs to address this problem. One possible solution is to issue some special certificates by CA, which are on the shelf and can be used in such scenario by the vehicle. But if this certificate is hacked by any adversary node it can be used for personal benefits in the network so such message should have less life time, so there must be proper solutions for such scenarios.

6. CONCLUSION & FUTURE WORK

VANET is most emerging and promising technology, security is an important aspect in its deployment. Due to characteristics of VANET many attacks are possible on the network and tough to provide a secure architecture. In this paper we have introduce most of the trends in the research area of VANET security and analyzed it with the security requirements of the system. In the future work we want to expand our idea about the minimization of CRL, management of liability message and test it by simulation.

7. REFERENCES

1. "*Road safety: A public health issue" Internet:* http://www.who.int/features/2004/road_safety/en.

2. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., & Hubaux, J. P. (2006). "Certificate revocation in vehicular networks". *Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland*.

3. Lind, R., et al. "The Network Vehicle-a glimpse into the future of mobile multi-media." *Aerospace and Electronic Systems Magazine, IEEE* 14.9 (1999): 27-32.

4. *"Car to car communication consortium." Internet:* http://www.car-2-car.org/.

5. "*Seveco Global Limited." Internet*: http://www.sevecom.com.

6. "*ITS standard fact sheet." Internet*: http://www.standards.its.dot.gov/fact_sheet.asp?f=80.

7. Jiang, Daniel, Vikas Taliwal, Andreas Meier, Wieland Holfelder, and Ralf Herrtwich. "Design of 5.9 GHz DSRC-based vehicular safety communication."*Wireless Communications, IEEE* 13, no. 5 (2006): 36-43.

8. Papadimitratos, Panos, A. La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation." *Communications Magazine, IEEE* 47, no. 11 (2009): 84-95.

9. Namboodiri, Vinod, Manish Agarwal, and Lixin Gao. "A study on the feasibility of mobile gateways for vehicular ad-hoc networks." In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pp. 66-75. ACM, 2004.

10. Maxim Raya and Jean-Pierre Hubaux. "The security of Vehicular Ad hoc Networks." In *Proceedings of the 3rd ACM workshop on Security of ad hoc sensor networks*, pp. 11-21. ACM, 2005.

11. Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks."*Journal of Computer Security* 15, no. 1 (2007): 39-68.

12. Parno, Bryan, and Adrian Perrig. "Challenges in securing vehicular networks." In *Workshop on Hot Topics in Networks (HotNets-IV)*, pp. 1-6. 2005.

13. Bellur, Bhargav. "Certificate assignment strategies for a PKI-based security architecture in a vehicular network." In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pp. 1-6. IEEE, 2008

14. Papadimitratos, Panagiotis, Levente Buttyan, J-P. Hubaux, Frank Kargl, Antonio Kung, and Maxim Raya. "Architecture for secure and private vehicular communications." In *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*, pp. 1-6. IEEE, 2007.

15. Papadimitratos, Panagiotis Panos, Ghita Mezzour, and Jean-Pierre Hubaux. "Certificate revocation list distribution in vehicular communication systems." In *Proceedings of the fifth ACM international workshop on Vehicular Inter-Networking*, pp. 86-87. ACM, 2008.

16. IEEE P 1609.2 Version 1- Standard for wireless access in vehicular environment- Security services for application and management messages.

17. Calandriello, Giorgio, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. "Efficient and robust pseudonymous authentication in VANET." In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pp. 19-28. ACM, 2007.

18. Raya, Maxim, Daniel Jungels, Panos Papadimitratos, Imad Aad, and Jean-pierre Hubaux "ECertification revocation in vehicular networks.", 2006b.

19. Raya, Maxim, Panos Papadimitratos, and J-P. Hubaux. "Securing vehicular communications." *Wireless Communications, IEEE* 13, no. 5 (2006): 8-15.

20. Studer, Ahren, Elaine Shi, Fan Bai, and Adrian Perrig. "TACKing together efficient authentication, revocation, and privacy in VANETs." In *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*, pp. 1-9. IEEE, 2009.

21. Sun, Yipin, Ronxing Lu, Xiaodong Lin, Xuemin Shen, and Jinshu Su. "A secure and efficient revocation scheme for anonymous vehicular communications." In *Communications (ICC), 2010 IEEE International Conference on*, pp. 1-6. IEEE, 2010.

22. Raya, Maxim, Adel Aziz, and Jean-Pierre Hubaux. "Efficient secure aggregation in VANETs." In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 67-75. ACM, 2006.

23. Gerlach, Matthias, Andreas Festag, Tim Leinmüller, Gabriele Goldacker, and Charles Harsch. "Security architecture for vehicular communication." *WIT 2005*(2007).

24. Calandriello, Giorgio, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. "Efficient and robust pseudonymous authentication in VANET." In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pp. 19-28. ACM, 2007.