# Comparative Study on Security Protocols for VANET's

**Nandini Prasad K S, Pavan Kumar S**

***Abstract*— Wireless technology has been gaining rapid popularity in the current years. Adoption of standard depends on the ease of use and level of security it provide. The era of vehicular ad-hoc network (VANETs) are receiving increasing attention from academia and deployment effort from industry. In a VANETs, vehicles will depend on the integrity of data for deciding when to alerts to drivers. The VANETs provide an intelligent communication among vehicles and also between vehicle and roadside infrastructures. The communication in VANETs is done between vehicle to vehicle, vehicles to roadside unit through wireless communication. Network attack like man in middle, masquerading can attain in VANETs, so security must be consider for vehicular ad-hoc network. Security is the major concern for various VANETs applications where a wrong message may directly or indirectly affect the human lives. Certificate distribution, revocation and communication bottlenecks, are the main challenges in the VANETs. If message integrity is not sure in VANETs, an unknown vehicle may modify the content of a message which will affected to the behavior of other vehicles. In this paper, we are comparing different security protocol that is needed to consider in VANETs.**

***Index Terms*— Wireless Technology, VANETs, Security, Certificate Distribution.**

## I. INTRODUCTION

VANET- Vehicular Ad-Hoc Network is a technology that uses moving vehicles as nodes to create a mobile network, communication in VANET's has been done in between road side units to cars, car to car in a short range of 100 to 300 m. Vehicular ad hoc networks (VANETs) provide various applications and also benefits for future VANET's user which increase deployment efforts from industry. In VANET's the drivers can be alerts since the vehicles depend on received data. Since wireless communication is taken place in VANET's so security is major concern. If any misinformation is available then, there will be erroneous warnings to their drivers. If any attacks is done on VANET's that may lead to losses of lives like accident which also cause a financial losses. There are challenges like certificate distribution and revocation avoidance of communication in the existing protocols which reduces the bottlenecks. VANET's are also information oriented, since application can be added. VANET aims at enhancing driving safety through inter-vehicle or vehicle-to-infrastructure communications. Safe driving is the milestone application for VANETs.

In general, a secure network should have the following attributes: (i) authentication (ii) non-repudiation (iii) confidentiality (iv) data integrity (v) access control (vi) availability.

A General Architecture for VANET's is shown below ,The communication may be of 3 types-1.inter-vehicle communication i.e. vehicle to vehicle communication 2.vehicle to roadside communication i.e. communication between roadside unit(RSU) and vehicles 3.inter-roadside communication i.e. communication between roadside unit and the base station. Applications based on vehicular communication range from simple exchange of vehicle status data to highly complex, large-scale traffic management including infrastructure integration. The communication channel that can support VANET's is IEEE 802.11-like technology.

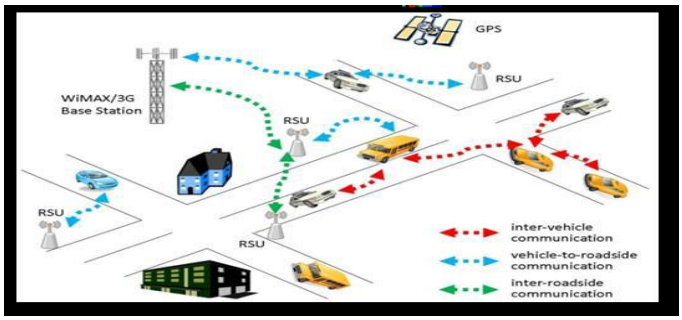


Fig. 1 VANET's Architecture

The communication in VANET's is local although it provides real world mobile ad hoc network. Since we will having hundreds of node by partitioning it we can make a network scalable. It provides maximum power resources and good computational power over the ad hoc networks.

For a secure messaging, the VANET's must satisfy the following requirements.
1) *AUTHENTICATION*: It is required because the vehicle reaction is based on the legitimate message so this is needed
*2) AVAILABILTY*: Since because of some robust attack which can down the network, so availability could be supported.
*3) NON-REPUDIATION*: The sender one who send the



ISSN: 2278 – 7798 

message should not delay the transmission of a message which may driver can cause an accident

*4) PRIVACY*: There must be privacy so that the drivers will fail to access the information from the unauthorized access.

*5) REAL-TIME CONSTRAINTS*: VANET's must be strict time constraints so that data manipulation can be avoided.

## II. RELATED WORK

Kenneth P. et al., [4] have given an idea for improving distribution speed and distribution of CRLs by using vehicles in an epidemic fashion. In this paper nodes are not confirmed about the bandwidth and hardware restrictions and the method that only employs at RSU distribution points. M. Raya et at., [5] have proposed about developing infrastructure based revocation protocol. They have also given an idea of MDS, enabling the neighbors of misbehaving or faulty nodes to detect its deviation from normal behavior. For the purpose of security they provide a LEAVE protocol to safeguard the system operation, but false rate has been provided by Bloom's Filter. Jean-pierre Habaux et at., [9], discusses about the vehicular communication that exhibits unique security challenges, where their will have sporadic connectivity of the vehicles. But these network solutions cannot be implemented in the present scenario Philippe Golle et al., [2] gave an idea of Sensor driver technique that allows nodes to detect incorrect information and identify the node or nodes that are the source of this incorrect information with high probability. Jyoti Grover et al., [6] proposed the parameter ANGLE for RSUs, to detect Sybil nodes. They assume that the angle value remains unique for each node at any instant of time and they found that 99% is accurate with approximate. As there is no well-defined processing time, storage and number of RSU, hence it results to 0.5% error rate.

## III. COMPARISION OF DIFFERENT SECURITY PROTOCOL IN VANET'S

The spectrum for vehicular wireless communication is available in the US in the 5.9 GHz band and is called Dedicated Short Range Communications (DSRC). The radio technology chosen for operations in this spectrum is based on IEEE 802.11a and is expected to be standardized as IEEE 802.11p. The nodes of the network are made up by OBEs in vehicles and RSEs on the road-side. The number of deployed nodes is assumed to be in the range of several hundred millions or even billions. This data is as given by Vehicle Safety Communications – Applications (VSC-A).Research on VANETs security started in the middle of 2000s and grew from 2007.

Three properties regarding security that cannot be ignored are confidentiality, integrity, and availability.

The main factors that influence the adoption of VANET architecture for future vehicular applications would be:

- Low latency requirements for safety applications
- Extensive growth of interactive and multimedia applications
- Increasing concerns about privacy and security

Fig. 2 indicates the classification of Wireless Ad hoc Networks.

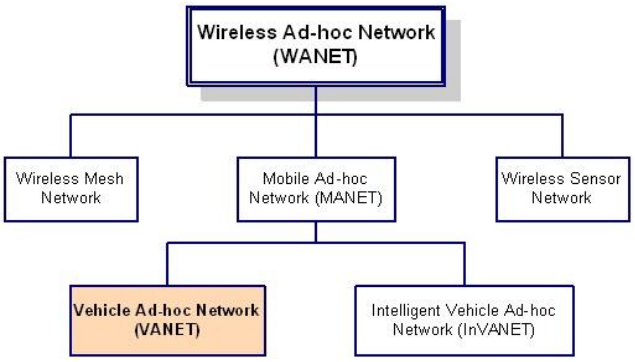


Fig. 2 Wireless Ad hoc Network Classification

Routing protocols in VANETs can be broadly classified into following five categories based on area application where they are most suitable: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Geocast routing protocol and Broadcast routing protocol.

Vehicular networks need to be secured [9], and this problem requires a specific approach. The authors have proposed a model that identifies the most relevant communication aspects and have also identified the major threats. They have then proposed security architecture along with the related protocols and also explains about the privacy. They have come to the certainty that existing network security solutions cannot be readily applied to VANET's, given the radically different nature of new type of networks. A good example is that of authentication mechanisms, where digital signatures showed to be the most suitable approach despite their seemingly high overhead. A model which is proposed [9] is relevant to communication aspect and also security architecture with the related protocols. Existing network security solutions cannot be readily applied to VANET's due to radically different nature of this new type of networks. The protocol which they proposed provided privacy, robustness and efficiency. The security analysis was done with respect to the security requirement. An authentication of message is done with the digital signature of the sender along with CA certificates, this guarantees that massage coming from a vehicle could be trusted. The authors also discussed about the secure positioning where vehicles cannot be cheat about their respective position.

An implementation of a certificate [1] which reduce a certification revocation lists size when their will be high



ISSN: 2278 – 7798 

traffic. The authors also proposed a mechanism to determine the certificate on the CRL, they also discussed about the revocation key approach along with a bloom filter for the fast certificate acceptance. The storage mechanisms of certificate identifier with respect to real world performance are also discussed, and calculated computational power using storage mechanism.

A system provides a unique security challenges [8] which will have the high speed connectivity to the vehicle. A mechanism where CRL will break into pieces and the breakable pieces can be encoded using fountain coded is provided. The author also has discussed about the bandwidth of the message which is to be transferred. The simulation of RSU's is done at every 1, 2, and 3 km.

Attacks perpetrated against the message includes: Fabrication Attack, Alteration Attack, Replay Attack and Sybil Attack.

VANET's depends heavily on node-to-node communication to meet the performance goal thus allowing for malicious data traffic [2]. At the same time, the easy access to information afforded by VANETs potentially enables the difficult security goal of data validation.

A protocol is proposed [7] to provide secure communication which is secure, scalable and also exploit a vehicular mobility. The authors have also proposed a magic ink mechanism which deals with blinded signature that can be detected by the signer if malpractice is achieved .The signer can either be centralized or distributed. The integrity of blinded signature is based on the threshold scheme. Magic ink provides a concept by using procedure signature.

An idea about the delta certificate revocation lists [6] which is efficient way for the distribution of the status information. The author has analyzed delta CRL to narrate the problem associated with delta CRL which is in traditional manner. The author also proposed a technique for issuing delta CRL using sliding window concept in which problem could be minimum overhead.

A framework [11] which is proposed that can be a trust based and that is used for message propagation and evaluation where the information can be exchange on road safety and that information can be trusted. The evaluation of the trust based framework is done by collaborative fashion. This framework provide an idea regarding trust opinion, role based trust .This trust based framework will detect malicious data.

## IV. CONCLUSION

In our paper, we had compared the different security protocol for VANET's. In our comparison we have come across with a feature which is less acceptable, so security is an important concern.

In future, we would like to propose an algorithm which will be secure and cost effective which will prevent all possible attack in VANET's and make it secure and reliable network which provide better performance.

## REFERENCES


[1] Jason J. Haas, Yih-Chun Hu, Kenneth P. Laberteaux ―Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET‖ in VANET'09, September 25, 2009, Beijing, China. 2009 ACM.

[2] P. Golle, D. Greene, and J. Staddon, ―Detecting and correcting malicious data in vanets, in VANET '04: Proceedings of the 1st ACM international workshop on Vehicular Ad hoc networks, (New York, NY, USA), pp. 29–37, ACM, 2004..

[3] Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu, ―Security Certificate revocation list distribution for VANET. In VANET '08 Proceedings of the fifth ACM international workshop on Vehicular Inter-NETWORKING, 2011.

[4] M. Raya, P. Papadimitratos, I. Aad, D.jungels, and J.P. Habaux), ―Eviction of misbehaving and faulty nodes in vehicular networks, in IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, 2013,vol. 25, num. 8, p. 1557-1568.

[5] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, A Novel Defense Mechanism against Sybil Attacks in VANET, in Proceeding SIN '10 Proceedings of the 3rd international conference on Security of information and networks,2011.

[6] D. Cooper, A More Efficient Use of Delta-CRLs‖, in IEEE Symposium on Security and Privacy,2010.

[7] Lei Zhang, Qianhong Wu, Agusti Solanas A Scalable Robust Authentication Protocol for Secure Vehicular Communications,2012.

[8] M. Raya, Papadimitratos and J.P Habaux‖ Special issues on Inter-Vehicular Communication‖,2009.

[9] M. Raya, and J.P Habaux, Securing Vehicular ad hoc networks, 2012.

[10] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

[11] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho. Secure and efficient trust opinion aggregation for vehicular ad-hoc networks. In Proceedings of the IEEE 72nd Vehicular Technology Conference (VTC), 2010.



**First Author** Associate Professor Dept. of ISE, Dr.AIT, Bangalore.
**Second Author** M .Tech Student Dept. of ISE, Dr.AIT, Bangalore.




ISSN: 2278 – 7798 