Mobility Management in Vehicular Adhoc Network based on RSA Algorithm

Pallavi Sapkale, *Student Member, IEEE*
RAIT
Nerul Navi Mumbai , Maharashtra
pme932@gmail.com

Uttam Kolekar,
APSIT,
Thane, Maharashtra
uttamkolekar@gmail.com

Moresh Mukhedkar
DYPCE
Talegaon, Maharashtra
Moreshmukhedkar@gmail.com

***Abstract*— Vehicular Ad-hoc Network (VANET) is become very popular in academia as well as in industry. The important characteristics of VANET faces difficulties on network issues. Specifically the mobility management will helpful to provide a seamless connectivity and improve the Quality of service. So we present an overview of mobility management in VANET based on RSA algorithm. During vehicle to vehicle communication driver do not want to share his personal information like vehicle names, license, number plate, speed position, moving port routes and user information. To protect all the information and save from any external attacks such algorithm is effective. Devised work is also useful and helpful to find the cause of accident or any liabilities. Recent work on mobility management is discussed in this paper. Proposed work includes an ID based crypto system for valid user. For this paper we are implementing RSA algorithm. In which data is encrypted and then the data is converted to cipher text and then decrypted with a private key. And the receiver will get original data.**

Keywords— Vehicle ad-hoc network(VANET); long term evolution(LTE); handover; RSU node; Mobility management; RSA.

I. INTRODUCTION

The intelligent transportation system (ITS) plays an important role to replace the conventional vehicle to digital fully controlled vehicle which reduces the accident. According to WHO [3] main reason for the death is road accident in upcoming years. VANET is a vehicular ad-hoc network which basically uses a moving vehicle as a nodes to create mobile network. VANET provides a better service like pleasant driving and parking. VANET turns every participating vehicle into wireless node which allow vehicle to communicate with each other. In VANET, communication takes place between vehicles and road side unit (RSU) and certification authority (CA). VANET network generally consists of three network components: one is road side unit (RSU), second one is moving vehicles which is known as node and third one is certification authority (CA). To create a communication network geographical area is divided into three regions and each region have its own road side unit (RSU) and which is served by one certification authority (CA). When the vehicle moves from one region to another region with connected network then handover process is occurs. Basically handover is process in which connected calls and data is transfer from one base station to another base station without disconnecting the communication [1][2]. Following figure shows VANET system model. VANET system model consist of trusted certification authority (CA) and road side unit (RSU).

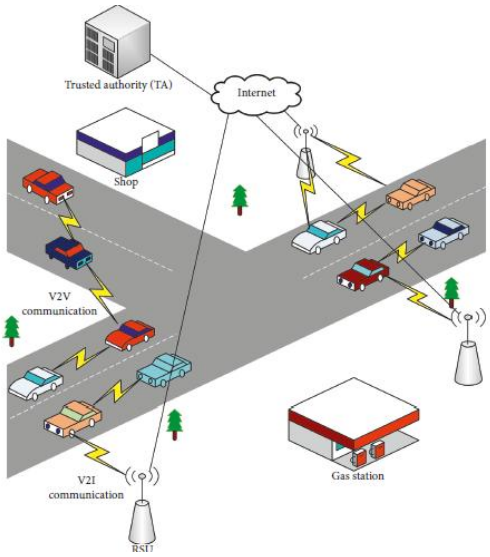

Fig. 1. VANET System Model[3].

V2V communication and V2I communications are used for VANET. Vehicle to vehicle information is share with V2V communication. And related to safety information is share in V2I communication with the help of RSU unit.

II. CHARECTERISTICS OF VANET

The main characteristics of VANET are as follows:

A. Mobility:

VANET having good mobility comparative to MANET. Due to high mobility it plays and important role in protocol. In VANET speed of network is so fast and communication time is less. In mobility management handover is main term. Handover is a procedure in media communications and portable correspondences in which an associated call or an information session is exchanged from one cell site (base station) to another without disconnecting the session. Handovers are a center component in arranging and sending cell systems. It enables clients to make information sessions or associate telephone approaches the move. This procedure keeps the calls and information sessions associated regardless of whether a client moves starting with one cell site then onto the next. In customary cell systems, handovers are for the most part occasion activated. The base station controls the client terminals to execute the estimation and report the deliberate system status data to the serving base station. Nonetheless, in our proposed system cutting based 5G frameworks, portability related occasions should be reclassified. For example, handovers may happen in various

cutting situations. Adaptable handover components and versatile handover edges ought to be abused to help portability the executives in administration tai-lured situations. Figure 2 shows handover management system.

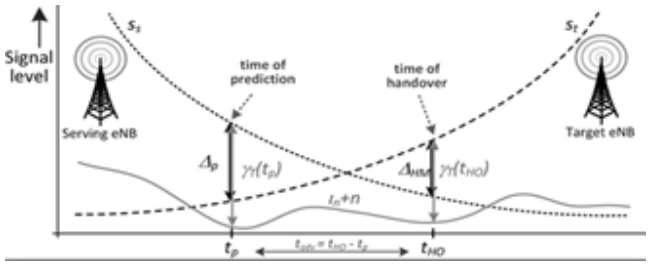

Fig. 2. Handover Management System .

B. *Saftey:*

VANETs can increase the driver safety, provide the passenger comfort, and also provide the traffic flow. A big benefit of VANET is it communicate directly with each other.

C. *Power Management:*

There is better power management in VANETs as compared to MANETs; thus, in VANET battery life is long so power is provide through OBU.

D. *Network:*

Network is maximum in VANET when there is more traffic on road, and when traffic is less then network also reduced. And more applications like security, confidentiality, and authentication.

III. LITURATURE REVIEW

This section describe a previous survey of the existing schemes and techniques in vehicular networks. The system in [5] discuss a brief review of the handoff process for VANET over LTE-A wireless networks. In paper [6] mobility management for VANET is surveyed. Authors [7] designed

a live emergency and warning alerts for VANET though android application. In [8] author describe about an outline of the vertical handover choice procedure with a grouping of the diverse existing vertical handover choice methodologies. By studying this papers, a new research options can be enhanced by understanding the gaps in previous systems.

IV. BACKGROUND DETAILS

The existing communication models of VANET can be divided as follows.

- Roadside Unit (RSU) Model.
- Vehicle to Vehicle (V2V) Model

A. *Roadside Unit (RSU) Model:*

Existing work on VANET was started with Roadside Unit (RSU) model [19]. In this model a tower (RSU) is fixed at the road sides as shown in the Fig. 3. From which message can be transmitted through a single tower. To exchanging the information Dedicated

Short Rage Communication (DSRC) is applicable. Vehicle which passes from existing tower are connected with that tower and the data can be delivered to the RSU. Each vehicle can send the messages to the RSU and the RSU will route the message to the right destination

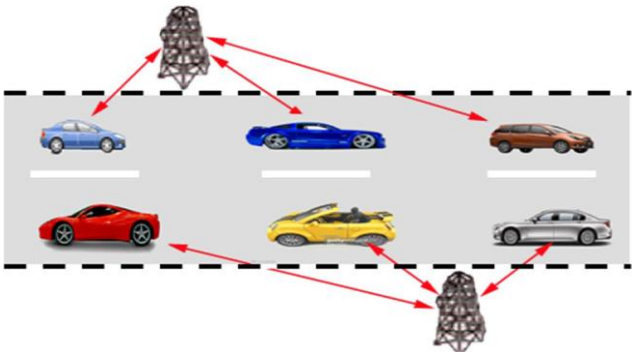

Fig. 3. Roadside Unit (RSU) Model .

B. *Vehicle to Vehicle (V2V) Model:*

The second existing model is Vehicle to Vehicle (V2V) model. V2V model is consuming less time as compared to the RSU model for sending the signal. For sending and transmitting the signal V2V model is work with a different unit which is On Board Unit (OBU). This OBU directly connect with the router and send the message to destination.

V. PROPOSED SYSTEM DESCRIPTION

Most proposed solutions for privacy preservation in VANETs did not include a tracking mechanism to prevent inside attacks such as fake message and spoofing attacks. In proposed system we are using visual studio for visualization handover process, and also using VANET network for implementing handover management process [10]- [12]. In proposed system we are using four wheeler and it work as a node for handover process. While handover process security is also important factor to secure the network ,so we are added privacy and security to the users, for adding security to network we are using RSA algorithm, in RSA algorithm every user has his own public and private key without public and private key user cannot communicate with each user. So here we use the some security to some vehicles by using RSA algorithm. In VANET mechanism i.e. pseudonym generation is use and some privacy scheme is use in RSA algorithm. Were such are not use pseudonym for privacy preservation [9] .this scheme a based on ID based cryptography. So after keeping some points while developing in this project Security goals Privacy: the information of driver like (driver name, license plate, speed, position etc.) must be update against any illegal access. Non repudiation: if any message cannot send and received then it is important to send a warning message in this way if a vehicle we can avoid the some loss of data [16]. Following figure 3 shows that how data is transmitted.

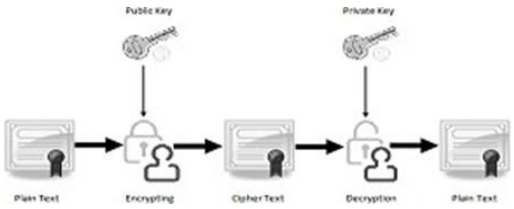

Fig. 4. Data transmission process

Data transmission process done by using RSA algorithm [11]. When a transmitter wants to send the data to receiver, the message in the form of plaintext is encrypted by using public key and converted to the cipher text form. After that this cipher text is transmitted over communication medium. Receiver receives that cipher text and it decrypted using private key and receiver gets the original data.

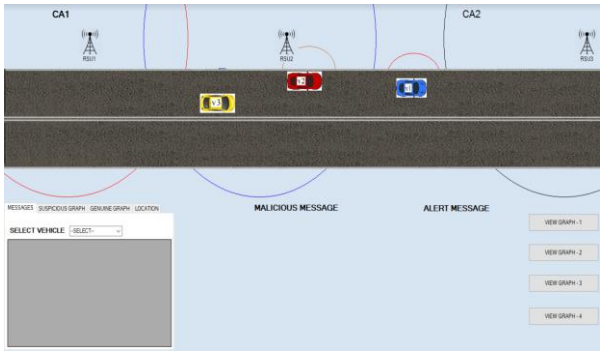

Fig. 5. Proposed system design

The proposed framework provides handovers scheme for efficient data transmission. The proposed model considered RSU as central data control authority for providing information about signal strength to vehicles. Above figure [4] shows the operation of proposed system, here RSU is road side unit considered as the central data authority for providing information about signal strength to vehicles . When a vehicle means node wants to communicate with other node RSU, it uses public and private key for data transmission. When the vehicle moves from one cell to another cell handover process occurs. In this handover process some data will be loss due to signal strength .if the vehicle is closed to RSU then the signal strength of the user is high and when the its away from RSU signal strength of the user is less that means when user is away from the RSU data loss is occurs.

A. Attacks on Authentication

Considering security in VANETs, its square measure various assaults that compromise the V2R, R2V and V2V interchanges out and concerning. Here, we tend to examine these assaults especially on validation, protection conservation and on repudiation, and clarify however they are activated and therefore the potential outcomes. Assaults on the

Validation: There square measure 2 types of assaults known with confirmation in VANETs and square measure given as pursues [1]. 1 Pantomime assault: The aggressor professes to be associate different component. The impersonation assault is per60 formed by taking different conveyance substances qualifications for validation. As associate outcome, a number of admonitions sent to a selected component would be sent to associate unsought one. 2 Sybil assault: The aggressor utilizes distinctive personalities within the in the meantime. On these ines, e.g., a solitary aggressor might imagine vehicles to report the presence of a fake bottleneck in hour snarl-up. Assaults on the security: Attacks on protection over VANETs square measure known with illicitly collection touchy information concerning vehicles (e.g., listening in).As there's an association between a vehicle and its driver, the presentation of a vehicles mystery/touchy information might influence 13 its driver protection [12]. 1 Character uncovering assault: obtaining the proprietors temperament of a given vehicle might place its security at risk. Typically, a vehicles man of a airs is in addition its driver, thus it might set up obtaining individual info this individual.

2 Area following assault: the realm of a vehicle in a very given minute, or the way pursued amid a timeframe is taken into account as about to home info. It allows the highest to manufacture the vehicles prole and, on these lines, following its driver. Assaults on the non-denial: In VANETs, the non-revocation is known with a reality that a vehicle cannot deny a selected message within the event that it's sent that message routinely, by delivering a mark for the message in VANETs, the vehicle cannot later deny the sent messages. The assault on the message nonrepudiation is processed as pursues [2]. 4. Revocation assault: Repudiation alludes to a rejection of support all told or half of interchanges in VANETs. As an example, a slim minded driver might deny directive associate task on an open-end credit get, or vindictive vehicles might mishandle unknown authentication systems to accomplish malevolent objectives or break from their liabilities.

VI. RESULT

A. Delay

Delay is defined as the difference between the expected time of arrival of a message and the actual time. Figure provide an analysis of the occurrence of the packet loss during the handover procedure. However as the amount of data in the network increases it affects the delay in data transmission too

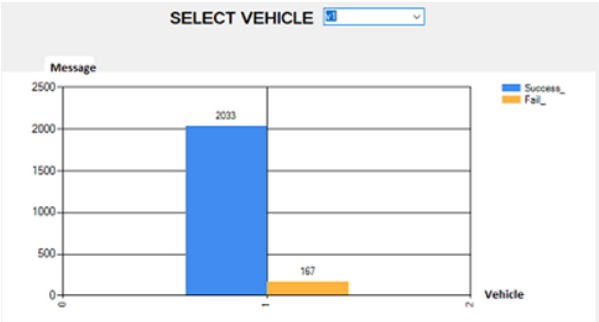

Fig. 6. Message for vehicle 1

Above figure shows graph of vehicle 1s message sent and failed in process of transmission .total 2038 messages are sent successfully and 167 messages are failed during transmission

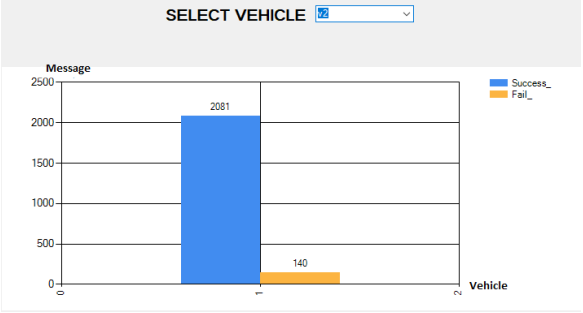

Fig. 7. Message for vehicle 2

Above figure 7 shows graph of vehicle 2s message sent and failed in process of transmission. Total 2081 messages are sent successfully and 140 messages are failed during transmission.

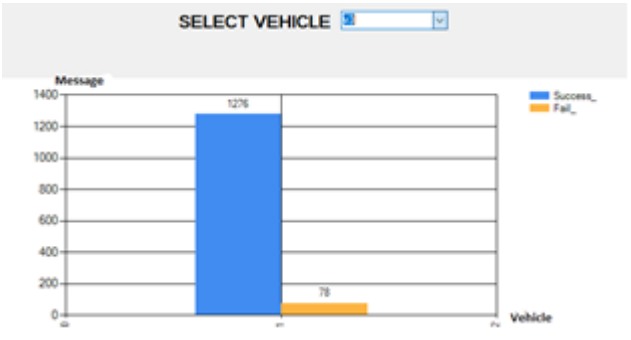

Fig. 8. Graph of vehicle 3

Above figure shows graph of vehicle 3s message sent and failed in process of transmission. Total 1278 messages are sent successfully and 78 messages are failed during transmission

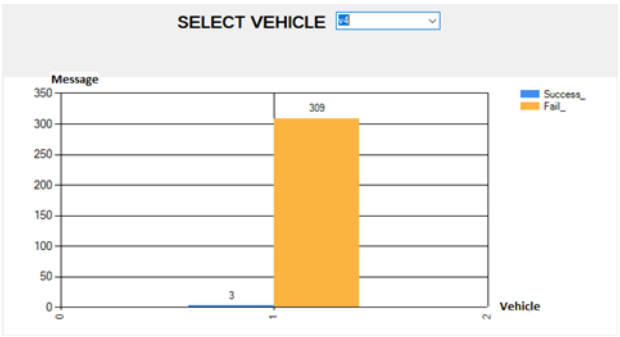

Fig. 9. Graph of vehicle 4

Above figure shows graph of vehicle 4s message sent and failed in process of transmission. All the messages of vehicle 4 are failed because vehicle 4 is malicious node.

The process of transferring a mobile user from one base station to the other known as handover. Following fig.10 describes about handover process. In which BS1 and BS2 are two base stations and handover is takes place between them. As figure10.

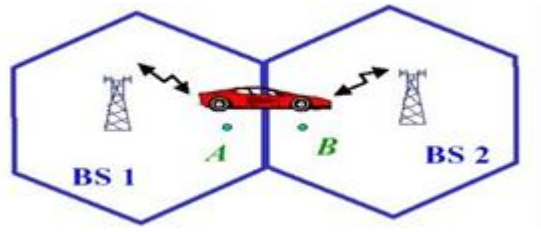

Fig. 10. Handover process

Shows RSS increases when it is closer to RSU. It will increase linearly and then reaches to highest value when it comes in maximum range of RSU.

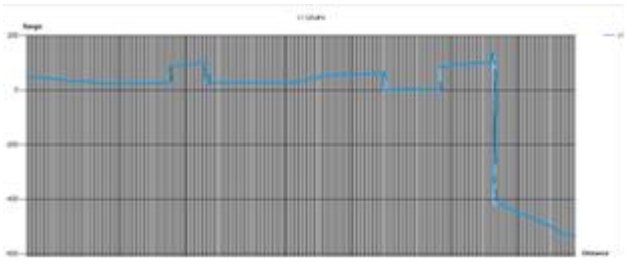

Fig. 11. Handover for vehicle 1

Above graph 11 shows signal strength of vehicle 1. In which distance covered by the vehicle 1 with respect to the range of RSU. It will increase linearly and then reaches to highest value when it comes in maximum range of RSU. When the node is close to RSU i.e. road side unit then strength of the signal is more and when node is far from RSU strength of signal is less. In a graph, it shows that when node moves from one cell to another cell signal strength drops to zero for some times and it again increases when it comes in range of road side unit.

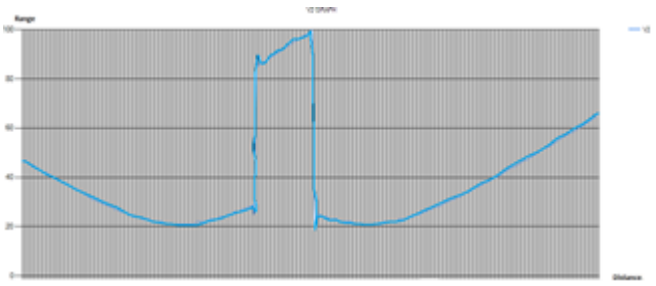

Fig. 12. Handover for vehicle 2

Above graph 12 shows signal strength of vehicle 2, when the node is close to RSU i.e. road side unit then strength of the signal is more and when node is far from RSU strength of signal is less. In a graph, it shows that when node moves from one cell to another cell signal strength drops to zero for some times and it again increases when it comes in range of road side unit. Graph13 shows signal strength of vehicle 3, When the node is close to RSU i.e road side unit then strength of the signal is more and when node is far from RSU strength of signal is less. In a graph, it shows that when node moves from one cell to another cell signal strength drops to zero for some times and it again increases when it comes in range of road side unit.

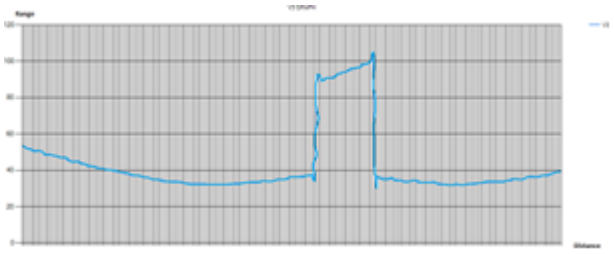

Fig. 13. Handover for vehicle 3

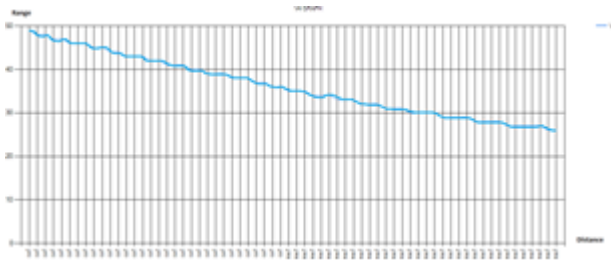

Fig. 14. Handover for vehicle 4

Above graph14 shows signal strength of vehicle 4, When the node is close to RSU i.e. road side unit then strength of the signal is more and when node is far from RSU strength of signal is less. In a graph, it shows that when node moves from one cell to another cell signal strength drops to zero for some times and it again increases when it comes in range of road side unit.

VII. CONCLUSION

The proposed framework provides handovers management scheme for efficient data transmission. Handover is occurred in MBS, FAP and D2D. The algorithm rst preprocesses target selection based on SINR and Rate threshold. Only networks meeting the SINR and Rate threshold can enter into the management logic decision phase. Then, management logic ranks the available networks in terms of QoS. The proposed model considered RSU as central data control authority for providing information about signal strength to vehicles. The obtained simulations results show that the proposed scheme.

REFERENCE

[1] Chitra A. Parmar, Sunil P. Khachane, "Enhanced Conditional Privacy Preservation In VANETs," International Journal of Engineering Re-search and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 13, Issue 2 (February 2017), PP.25-29.

[2] Pallavi Sapkale et al., "Handover Decision Algorithm for Next Generation", Proceedings of International Conference on Wireless Communication, ICWiCOM 2019, 978-981-15-1002-1, Pages 269-277.

[3] Muhammad Sameer Sheikh et al., "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey", Hindawi Wireless Communications and Mobile Computing Volume 2020, Article ID 5129620, 25 pages, https://doi.org/10.1155/2020/5129620

[4] Bilal Haider et al.," A Survey on Mobility Management Techniques in VANETs", 2016 IEEE International Conference on Computer and Information Technology.

[5] Salihin, S.S.; Nissirat, L.A.; Noor, R.M.; Ahmedy, I. Handover schemes for vehicular ad-hoc networks over long term evolution advanced: A survey. In Proceedings of the 2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA), Kuching, Malaysia,

[6] Yibo Yang, Hongling Li, Qiong Huang, "Mobility Management in VANET" 978-1-4673-5699-2 /13/$31.00 ©2013 IEEE.

[7] M. Milton Joe1 ,"Live Emergency and Warning Alerts Through Android Application for Vehicular Ad Hoc Network Communication (Android VANET)." © Springer Science+Business Media, LLC, part of Springer Nature 2020.

[8] P. Chan et al, "Portability the executives joining handover rationale for a heterogeneous IP condition", Vol. 3, No.2,February 2014.

[9] 15–17 August 2018; pp. 1–7.WHO, Global Status Report on Road Safety 2015, WHO,

[10] Geneva, Switzerland, 2018, http://www.who.int/violence_

[11] injury_prevention/road_safety_status/2015/en

[12] [3]R. Pushpavani K. Thamizhmaran and T. Ravichandran, "Fast Handover Algorithm for Mobility Management in VANETs," International Journal of Advanced Research in Computer Science,Volume 8, No. 3,ISSN No. 0976-5697, March April 2017

[13] Adel A. Ahmed and Ahmad A. Alzahrani, "A comprehensive survey on handover management for vehicular ad hoc network based on 5G mobile networks technology,"Wiley,DOI: 10.1002/ett.3546.6 November 2018

[14] Pallavi Sapkale and Uttam Kolekar, "Mobility Management for 5G Mo- bile Networks," International Journal of Computer Applications.ISBN: 973-93-80899-49-7 DOI: 10.5120/ijca2018918093,November 26, 2018

[15] [6]O AlFarraj, A Tolba, S Alkhalaf, A AlZubi, "Neighbor predictive adaptive handoff algorithm for improving mobility management in VANETs," Computer Networks, 2019 - Elsevier.

[16] [7]K Shankar, M Ilayaraja, KS Kumar, Mobility and QoS analysis in VANET using NMP with SALP optimization models, Emerging Tech- nologies for Connected Internet of Vehicles and Intelligent Transporta- tion System Networks 2020 - Springer.

[17] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, An identity-based security system for user privacy in vehicular ad hoc networks, IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, September 2010.

[18] Jie Li, Huang Lu and Mohsen Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," IEEE transactions on parallel and distributed systems, vol. 26, no. 4, pp. 938-948, April 2015.

[19] Shivaldova, V., Paier, A., Smely, D., & Mecklenbra´uker, C. F. (2012). On roadside unit antenna measurements for vehicle to infrastructure communications. In: 23d IEEE International symposium on personal, indoor and mobile communications (PIMRC).