Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 7, July 2015, pg.557 – 566

RESEARCH ARTICLE

Protocol Change Pseudonyms (PCP) for VANETs

Anjana / Student of M.Tech*, **Meenakshi Chawla** / Assistant Professor

Department of CE, MDU -TIT&S, Bhiwani (Haryana) India, Department of CE, TIT&S, Bhiwani(Haryana) India
anjana.alhan@gmail.com *, meenakshi.4441@gmail.com

ABSTRACT- Vehicle Ad-Hoc Network (VANET) is an advance wireless technology in the field of wireless communication, communicate for safety and comfort purpose. Many types of technology and application are being developed for VANET. The security protocols based on periodic change pseudonyms. The illegal traceability of vehicles during their communications avoid the idea and approach is the central authority a new communication in each vehicle asks pseudonym after a time t and in second approach a new communication pseudonym, after t time each vehicle generates itself. To permit at least two vehicles to change their pseudonym in same time interval in our objective. The bandwidth used by considering the vehicle speed in each approach and evaluate by this work. The recommended protocol built on intermediate delivery of the road side unit and the average uses of speed permitted on the road to evaluate lifetime t of the communication's pseudonyms and certificates. The discussion of information is based on asymmetric, symmetric cryptography scheme and it uses hash function. This represented protocol provides authentication, non-repudiation and privacy.

Index Terms: Security, Delivery, Certificate, Privacy, Authentication, Traceability, Equidistant.

I. INTRODUCTION

There are two types of applications in vehicle ad-hoc network (VANET), first one is called security applications and second is qualified as non-safety application. Security application provides real time information about the conditions of road to the drivers. This information can be collision cautionary, auxiliary report, or mobbing information. The qualified as non-safety application is a series of applications that make expedition on road pleasurable such as video gushing, melody, quarter information. As well, VANET offers two fundamental types of communications: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I). Each vehicle is equipped with a wireless communication device called an on-board unit (OBU) and at road side location road-side units (RSU) are installed. The system is coordinated by a trusted third entity called, Central Authority (CA), which could be the department of transportation. Because of the important aspect of the information shared through the network, it is necessary to develop the security protocols to make VANETs applications helpful. Exclusively, sensitive information such by way of identity and location privacy must be preserved through vehicular communications. For this purpose, we propose a security protocol based on periodic change of communication pseudonym. Two different approaches are proposed. In the first approach, each vehicle asks the central authority (CA) a new communication pseudonym after a time t. In the second approach each vehicle generates itself, after a time t, a new communication pseudonym. In each approach, the road side units (RSU) are distributed intermediately so, the RSUs can communicate with each other. The distance between each RSU is their communication range. As a result when a vehicle enters into another RSUs communication range, it will ask for a new pseudonym in first methodology before will generate a new pseudonym and certificate in the second methodology. The time for a vehicle traveling at the average speed to cover the distance between each RSU, is the lifetime (t) of pseudonym and certificate. Our objective is to permit at least two vehicles to change their pseudonym in the same time interval.

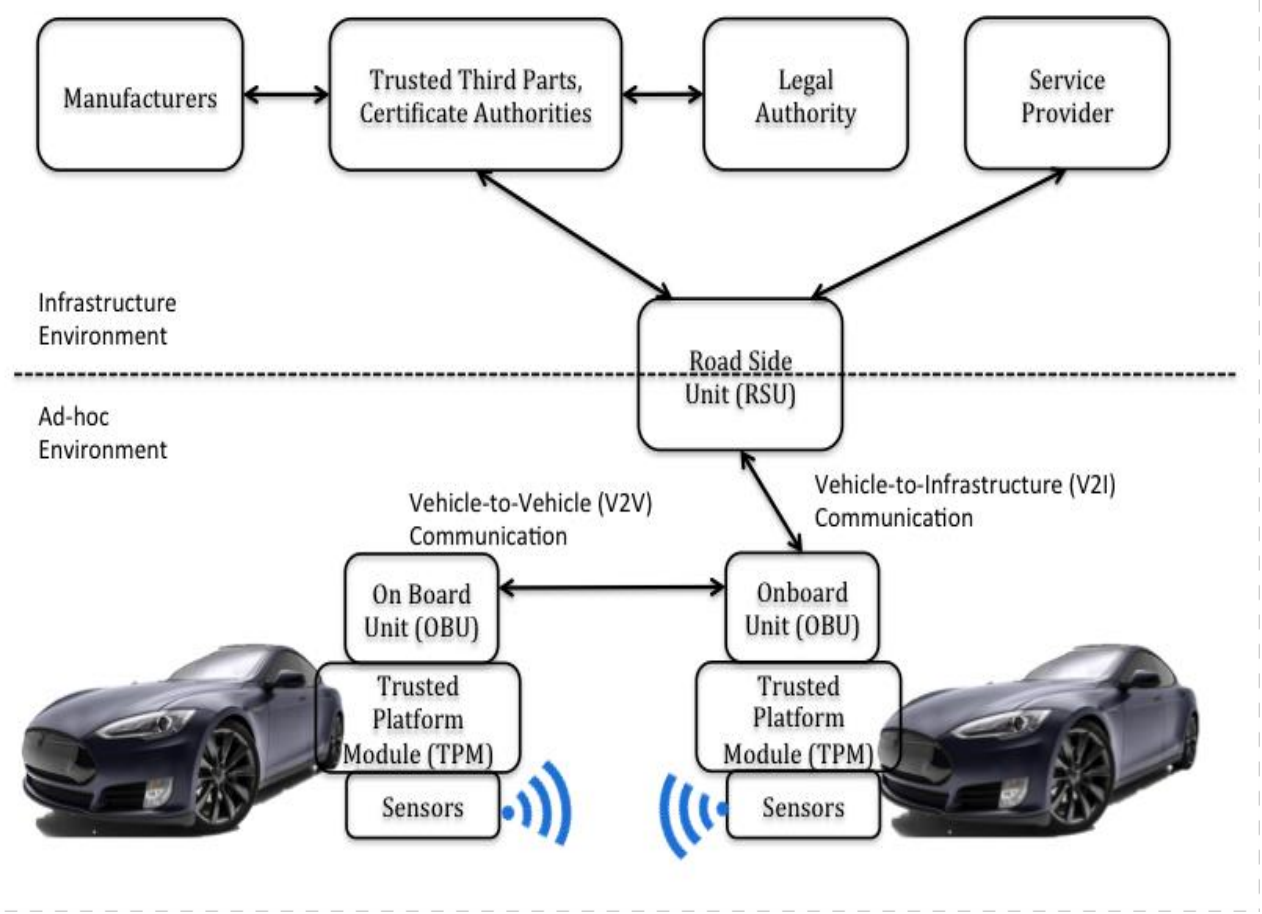

Manufacturers
Trusted Third Parts, Certificate Authorities
Legal Authority
Service Provider
Infrastructure Environment
Road Side Unit (RSU)
Ad-hoc Environment
Vehicle-to-Vehicle (V2V) Communication
Vehicle-to-Infrastructure (V2I) Communication
On Board Unit (OBU)
Onboard Unit (OBU)
Trusted Platform Module (TPM)
Trusted Platform Module (TPM)
Sensors
Sensors

Fig1 Security in VANET

We use the cryptography scheme to secure the information shared through the network. Our aim is to evaluate the bandwidth used, and the bit error rate by considering the vehicles speed in each approach. The remainder of this paper is organized as follows. In section II, we discuss the state of art on the security in VANET networks. In section III, we introduce our model. In section IV, we will present a short security analysis and describe the parameters of simulation for the two approaches, and we will conclude in section V.

II. STATE OF GRAPHIC ARTS

The Young ho Park, KyungHyune Rhee and Chul Sur present a secure and Location Assurance Protocol for Location-Aware Services in VANETs which provides anonymous authentication and avoid illegal movement tracking of vehicles in VANET as well as location assurance. The proposed scheme permits to the vehicle to have confidence that the received information originated from the vehicles that actually passed through the target location area. But if the private key generated by the MA (Master Authority) is not sent to vehicle in a secure way, the attacker can intercept it and use it to threaten the life of drivers, violating confidentiality properties and authentication. The authors propose a novel ID-based authentication framework with adaptive privacy preservation for VANETs. In this framework, the vehicles use pseudonym to communicate and the update of pseudonym depends on vehicles demands. A cooperative message authentication protocol in VANETs is proposed. The idea of this work is to alleviate vehicles computation burden during the authentication stage and reduce the number of safety messages that each vehicle needs to verify. The JaeHyu Kim and JooSeok Song propose a pre-authentication method based on scalable robust authentication protocol (SRAP) to reduce the number of packets transmitted in the key request stage. They also use symmetric key encryption function to decrease calculation time. The authors propose ID-based Safety Message Authentication for Security and Trust in Vehicular Networks. They incorporate an ID-based proxy signature framework with the standard ECDSA for VANETs road-side unit (RSU) originated safety application messages. The proposed protocol is appropriate for authentication and trust management but may suffer of the traceability problem. Because, if an attacker intercepts the message exchanged by two OBUs and if it contains the OBU location, then he could trace a vehicle in the network. The secure and efficient data acquisition method in VANE, the idea of the authors is to allow each vehicle user to communicate individually in the network. The road side unit assigns to each user who is connected a pseudonym per packet to avoid attacks. The authors propose a privacy-preserving trust model that respects the privacy of the users through groups and offers security through trust and reputation. Although the proposed protocol permits to exchange secure messages among vehicles and helps them to assess the reliability of receiving message. It is based on a static group of vehicles assigned offline. This protocol doesn’t provide a better security algorithm because of dynamic

Topology in vehicular network. An efficient pseudonym authentication-based conditional privacy protocol for VANETs is proposed. It allows each vehicle in the network to use pseudonyms to obtain privacy. The vehicles interact with road units to generate their communication pseudonyms. The authors propose a secure and efficient protocol for VANETs. Their scheme ensures both message authentication and privacy preservation. But a vehicle needs to communicate to road side unit before verifying the signature of a message it has received. A distributed key management framework based on group signature to preserve privacy in vehicular ad hoc network is presented. Each group is formed by the vehicles which get keys from the same road side unit. The proposed scheme preserves the privacy and permits to detect compromised road side units and vehicles. A privacy preservation authentication scheme for communication between vehicle and infrastructure in VANETs is proposed. The scheme permits to a vehicle and a road side unit to authenticate each other without returning to the trust authority. Although the proposed scheme satisfies most of the security requirements, it can be used to a communication between vehicles. The authors present a secure and efficient protocol for position based routing in VANETs. The proposed scheme improves the security of position-based protocol. Group-based Source Authentication protocol is proposed to handle the message authentication in VANETs. GSA makes use of group attributes as dynamic group key to protect data transmission in intra-group communication. The results of this implementation can guarantee multicast source authentication and boost the efficiency of authentication for multicast communication in VANETs. An innovative scheme for generating series of-lived secret keys that are shared by all the subscribers of the service is presented. The proposed algorithm is based on a couple of hash-chains generated from the master key. The authors present a security architecture which helps achieve all the security attributes without introducing complex or multi-transaction procedure. This proposed protocol does not require a tamper-proof-device (TPD) which stores the vehicles communication keys. An algorithm to secure vehicular communication based on a probabilistic approach. This scheme helps to determine the trust level of vehicles communication messages and to check the validity of the received messages and to check the validity of the received messages. Security architecture is proposed. This protocol is based on two new concepts: an extend PKI called PKI+ and secure geographical routing. In the proposed scheme, the user acts autonomous after receiving one master key and a master certificate from the CA. The user can create his own certified pseudonyms without interaction with the CA. The authors propose an efficient pseudonym PKI mechanism based on bilinear mapping to improve the performance of the message authentication protocol, and permits certificate tracing and certification revocation. The permit of vehicles to generate themselves their keys for communication but they don't mention the expiration time of the certificate. Authentication and privacy have been studied in various forms to prevent illegal vehicle traceability and protect users' information in the network. But few of these studies have defined a change time of the pseudonyms of communication for vehicles and analyzed the impact of the speed of vehicles on the use of pseudonyms communication. For it, we evaluate in this work, the bandwidth used, and the bit error rate by considering the vehicles speed in the periodic change of the pseudonyms of communication.

III. SYSTEM PROTOTYPICAL

1. Overall idea

Our proposed protocol preserves authentication, nonrepudiation, and privacy. It permits to the vehicles to change their pseudonyms in the same interval time. We have also place the road side unit at the same distance to permit the communication between them and the vehicles.

2. Assumptions

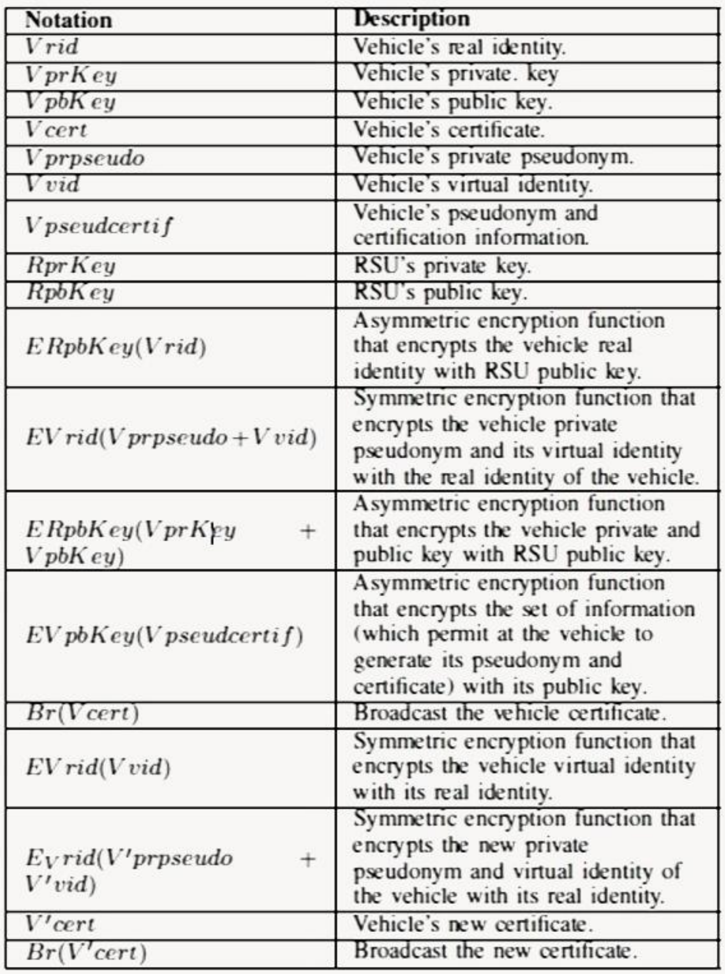
In our proposed protocol, we assume that: in the first approach, each vehicle has an ID which it shares with the Central Authority (CA) to request for the communication pseudonyms. In the second approach, each vehicle is identified by a private/public keys which it uses to get its private pseudonym and its certificate from the CA. The Road side units are trusted and are under the CAs control. The RSUs public key is available to all vehicles and it is certified by the CA. Each RSU broadcasts public pseudonym of the vehicles in its range as soon as it receives them from the CA. The CA is always online and reachable. It knows the RSUs private keys so it can decipher a message encrypted with the RSUs public key. Also the CA certifies the RSUs public key and frequently updates it.

3. Description of the model

1. **Approach**

In this approach, each vehicle is registered at the CA to get its private pseudonym and its virtual identity. The CA, after sending to the vehicle its private pseudonym and its virtual identity, sends the vehicles certificate to the road side unit which broadcasts this certificate. The vehicles certificate contains its virtual identity, public pseudonym and the lifetime of the certificate. The lifetime of the certificate is time for a vehicle traveling at an average speed to cover distance between two road side units. Upon expiry of the certificate, the vehicle sends to the CA its virtual identity. When the CA receives the virtual identity of the vehicle, it sends to this vehicle an update private pseudonym and communicates to the road side unit the vehicles certificate. Then the road side unit will broadcast the certificate. The virtual identity is used to identify the vehicles on the road, while the pseudonym permits them to communicate.

TABLE I.
NOTATIONS USED THROUGHOUT THIS PAPER



Notation	Description
$Vrid$	Vehicle's real identity.
$VprKey$	Vehicle's private. key
$VpbKey$	Vehicle's public key.
$Vcert$	Vehicle's certificate.
$Vprpseudo$	Vehicle's private pseudonym.
$Vvid$	Vehicle's virtual identity.
$Vpseudcertif$	Vehicle's pseudonym and certification information.
$RprKey$	RSU's private key.
$RpbKey$	RSU's public key.
$ERpbKey(Vrid)$	Asymmetric encryption function that encrypts the vehicle real identity with RSU public key.
$EVrid(Vprpseudo + Vvid)$	Symmetric encryption function that encrypts the vehicle private pseudonym and its virtual identity with the real identity of the vehicle.
$ERpbKey(VprKey + VpbKey)$	Asymmetric encryption function that encrypts the vehicle private and public key with RSU public key.
$EVpbKey(Vpseudcertif)$	Asymmetric encryption function that encrypts the set of information (which permit at the vehicle to generate its pseudonym and certificate) with its public key.
$Br(Vcert)$	Broadcast the vehicle certificate.
$EVrid(Vvid)$	Symmetric encryption function that encrypts the vehicle virtual identity with its real identity.
$E_Vrid(V'prpseudo + V'vid)$	Symmetric encryption function that encrypts the new private pseudonym and virtual identity of the vehicle with its real identity.
$V'cert$	Vehicle's new certificate.
$Br(V'cert)$	Broadcast the new certificate.

The design shown in figure 1

Describes the different steps of the approach 1 related step are offered as follows:

1. RSU broadcasts periodically its public key.
2. Vehicle sends to CA ER - pb Key (V rid) message.
3. CA sends to the applicant vehicle EV rid (V PR-pseudo + V vid) message.
4. CA sends to RSU a V cert message.
5. RSU broadcasts V cert message.
6. Vehicle sends EV rid (V vid) message to the CA.
7. CA delivers EV rid (V 0prpseudo + V 0vid) message to the vehicle.
8. CA sends to RSU a V 0cert message.
9. RSU broadcasts V 0cert message

In this approach, the vehicle always communicates with the CA to obtain its private communication pseudonym. We will analyze the bandwidth used between the request and the reception of pseudonym by vehicle in section I approach 2: In the second approach, each vehicle has a private and public key. If the vehicle receives the RSUs public key, it will send to the CA, its private and public keys by encrypting them with RSUs public key. The CA will register the vehicles pair key and will send to the vehicle a set of information by encrypting them with the vehicle public key. This set of information contains data that permits to the vehicle to generate its private pseudonym and certificate. When the vehicle receives this set of information, it will generate its private pseudonym and certificate.

.

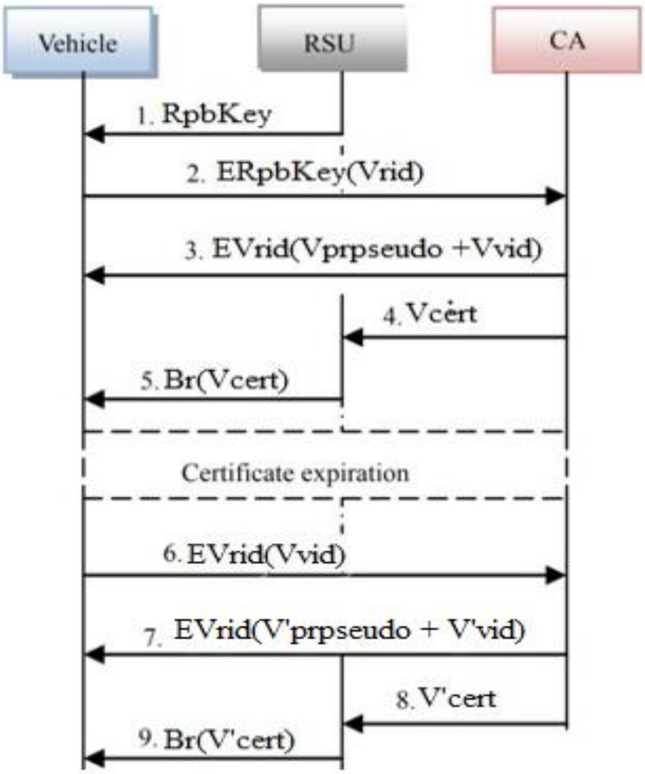


Fig 2 Description of the main steps in approach 1

After that, it will broadcast its certificate. Upon the expiration of the certificate, it will generate a new private pseudonym and certificate that it will broadcast. The vehicles are identified in this approach by the pseudonyms.

Figure 2 describes the different steps of the approach 2. The steps are as follows:
1: RSU broadcasts periodically its public key.
2: Vehicle sends to CA a ER pb Key (V pr Key + V pb Key) message.
3: CA sends to the applicant vehicle a EV pb Key (V pseud-certif) message.
4: Vehicle generates its private pseudonym and certificate.
5: Vehicle broadcasts its certificate.
6: Vehicle updates its private pseudonym and certificate.
7: Vehicle broadcasts the new certificate.

The vehicles, in the second approach are autonomous to update their private pseudonyms and certificates, once they have been authenticated by the CA. As in the first approach, we evaluate in section IV the bandwidth used and the bit error rate for this approach. We will compare the results for each approach. D. Evaluation of the expiration time of certificate and private pseudonym in both approaches, the road side units are distributed equidistantly. Consider d the distance between each road side unit d is also the communication range of each road side unit. V max and V min are respectively the maximum and minimum speed authorized on the road. We suppose, there will be at least two vehicles which will roll at an average speed. Our idea is to permit at least two vehicles to get the pseudonym on road in the same interval time. Denote Vm= (V max +V min)/2. The expiration time of certificate and private pseudonym t, will be the ratio between d and Vm; t = d=Vm. Also, as the communication range of each road side unit is equal road side unit has a communication range equal d, any vehicle, whatever its speed, can communicate at least with one road side unit and could change at least once its pseudonym on the road.

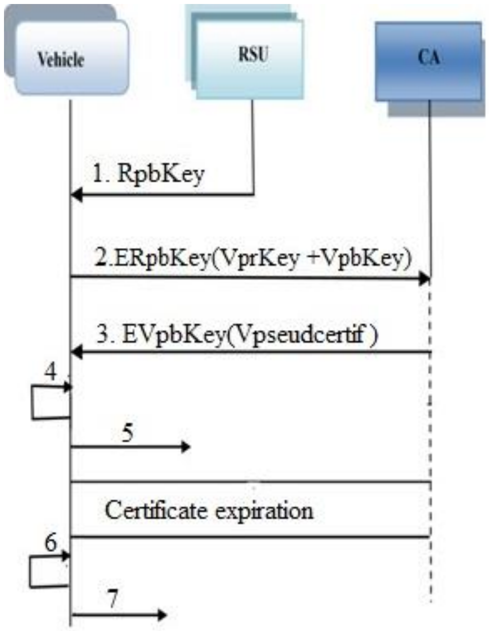


Fig 3 Description of main steps in approach 2

IV. CONSIDERATION

A. Security Analysis:

1. Authentication: In our two approaches, only a vehicle which has certified pseudonyms by the CA, can communicate with the others. This means that all vehicles in the network are registered and trusted by the CA. CA is the one who can decipher a message encrypted with the RSUs public key and all the RSUs are under the CAs control.

2. Non-repudiation: The vehicles communicate with certified pseudonyms received from the CA. In case of dispute, the CA can easily find the real identity of the vehicle because in the first approach, a vehicle requests private pseudonyms with its secret, while in the second approach, the private and public key of vehicle permit to identify it.

3. Privacy: Each vehicle communicates with short lifetime pseudonyms. The pseudonyms are renewed periodically and are not linked. Furthermore the change of pseudonym has done by at least two vehicles. So an attack can't identify precisely which vehicle has changed its pseudonym.

B. Performance analysis

Assessment parameters:

1. Number of vehicles which have gotten the private pseudonym in each approach.
2. Number of vehicles which have changed their pseudonym in each approach.
3. The bandwidth used in each approach according to the vehicle velocity. The scheme is tested by OMNET++ 4.2.2 with veins-2.0 and SUMO-0.15.0. We have run the simulation five times. Network parameters are set as in table 2.

TABLE II
SIMULATION PARAMETERS

Item	Value
Map city	3km x 3km
RSU number	6
Distance b/w RSU	500m
Time simulation	100s
Size of packet	1024 bytes
Number of vehicles in every approach	200
Speed interval on road	10m/s – 20m
Changing pseudonym and certificate	15 s
Bit rate	12mbps
Analogue models	Path loss models Obstacle shadowing Two ray interference model
MAC protocol	802.11p
RSU communication rang	500m
Vehicle communication rang	250
Thermal noise (8021.1)	-90dBm

1. The number of vehicles which have gotten the private pseudonym in each approach. In both approaches, 40% of vehicles didn't get their privates pseudonyms. 60% of them have gotten their private pseudonym in different time. We suppose, in the first approach, a vehicle receives its private pseudonym if its certificate has been broadcasted. The results are presented in figure 3.

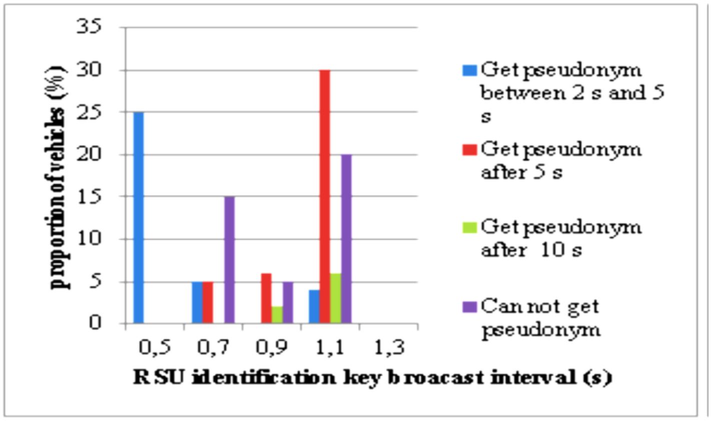


Fig. 4 Private pseudonym distribution phase

2. Number of vehicles which have changed their pseudonym in each approach. The aim of our study is to evaluate the change of pseudonyms vehicles. As described previously in subsection D, the expiration time of certificate and private pseudonym t = 300=9:5. t = 31:5 s. But we have considered in our simulations that the vehicles will begin to change their pseudonyms every 30 s. This will allow them to have new pseudonyms before expiration of the current ones. During the first period for change the communication pseudonym, 80% of vehicles which have been authenticated in the second approach have changed their pseudonyms while 75% of vehicles have received a new pseudonym in the first approach. We remark that the number of vehicles in first approach decreases until 50%, in time; while proportion of vehicles in the second approach is above 50%. This is due to0 loss of packets. The result is presented in figure 4 below.

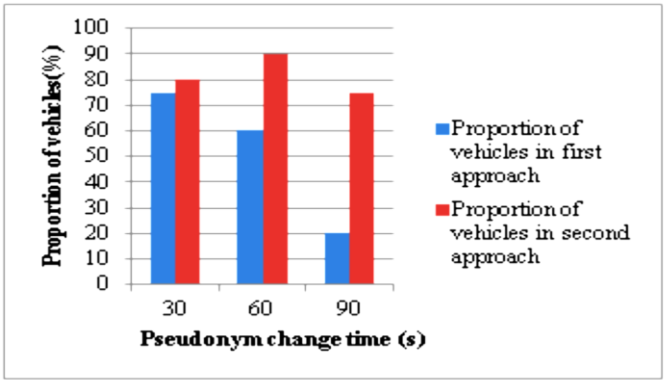


Fig. 5 Change of pseudonym in each approach

3. The bandwidth used in each approach according to the vehicle velocity. In this section the average velocity of vehicles. In figure 5, the bandwidth used by vehicles in first approach is increasing quickly depending on the velocity. While in the second approach, the consumption of bandwidth is less significant depending on the speed. The used of bandwidth in first approach is more important than the second approach. This is the fact in the first approach; a vehicle needs to communicate always with the central authority to get its private pseudonym.

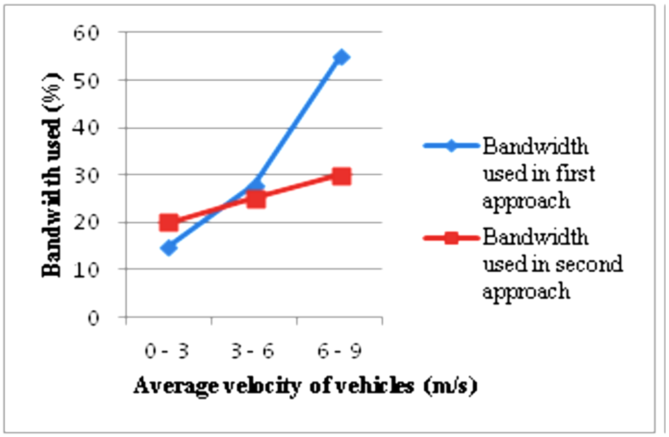


Fig. 6 Bandwidth consumption in each approach based on average velocity

V. CONCLUSION

The accessible in this paper a protocol change pseudonyms for VANETs, using urban environment for simulation. The bandwidth used and the update of pseudonyms have been considered in each approach. Our future work we will evaluate the bit error rate and take in to operation of our protocol in highway scenario. After then we will propose a dissemination routing protocol to fit best our method.

REFERENCES

[1] Subir Biswas, Jelena Misic and Vojislav Misic, ID-based Safety Message Authentication for Security and Trust in Vehicular Networks, 31st International Conference on Distributed Computing System Workshops, pp.323-331, 2011.

[2] Youngho Park and Kyung-Hyune Rhee, Chul Sur, A Secure and Location Assurance Protocol for Location-Aware Services in VANETs, 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.456-461, 2011

[3] Yong Hao, Tingting Han and Yu Cheng, A Cooperative Message Authentication Protocol in VANETs, Global Communication Conference (GLOBECOM), IEEE, pp. 5562-5566, 2012.

[4] JaeHyu Kim and JooSeok Song, A Pre-authentication Method for Secure Communications in Vehicular Ad Hoc Networks, 8th International Conference on Wireless Communication, Networking and Mobile Computing (WiCom), pp. 1-6, 2012.

[5] Ayman Tajeddine, Ayman Kayssi and Ali Chehab, A Privacy-Preserving Trust Model for VANETs, 10th IEEE International Conference on Computer and Information Technologie (CIT 2010), pp.832-837.

[6] Dijiang Huang, Satyajayant Misra, Mayank Verma and Guoliang Xue, PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs Intelligent Transportation Systems, IEEE Transaction on Volume 12, pp. 736- 746, 2011.

[7] Yong Hao, Yu Cheng, Chi Zhou and Wei Song, A Distributed Key Management Framework with Cooperative Message Authentication in VANETs, IEEE journal vol 29, pp. 616-629, 2011.

[8] Ming-Chin Chuang and Jeng-Farn Lee, PPAS: A Privacy Preservation Authentication Scheme for Vehicleto- Infrastructure Communication Networks, Consumer Electronic, Communicatins and Networks (CECNet), International Conference, pp. 1509-1512, 2011.

[9] Jie Hou, Lei Han, Jiqiang Liu and Jia Zhao, Secure and Efficient Protocol for Position-based Routing in VANETs, Intelligent Control Automatic Detection and High-End Equipment, (ICADE), IEEE International Conference, pp. 142-148, 2012.

[10] Kaouther Abrougui and Azzedine Boukerche, Secure Service Discovery Protocol for Intelligent Transport Systems: Proof of Correctness, 1st NSERC DIVA WORKSHOP, Developing the next Generation Intelligent Vehicular Network and Applications, pp.51-57, September 9, 2011-Ottawa-Canada.

[11] http://www.omnetpp.org/

[12] http://sumo.sourceforge.net/