Enhanced Privacy Preservation and Non-Repudiation for VANET'S

Sibil Joseph[1] and Rajagopal. R[2]

[1]PG Scholar, Department of Electronics and communication, K.C.G College of Technology, Chennai, India
[1]sibilmj73@gmail.com
[2] Asst. Professor, Department of Electronics and communication, K.C.G College of Technology, Chennai, India
[2]rajagopal@kcgcollege.com

ABSTRACT

Vehicular ad hoc network (VANET) is a technology which make use of moving vehicle for communication. The user authentication is major security service for access control in both inter-vehicle and vehicle-roadside communication. Moreover privet data of the vehicles need to be protected and non-repudiation access to authorized people to track the vehicle in the network. The proposed system Enhanced privacy preservation and repudiation for VANETs using public-key cryptography (PKC) for pseudonym generation, which ensures authorized third parties to achieve the non-repudiation of vehicles by using vehicles' real IDs. The self-generated PKC based pseudonyms are authentication instead of vehicle real IDs for the privacy-preserving authentication, depending on vehicular demands update of the pseudonyms will occur. The system uses ID-based signature (IBS) scheme authentication between road side unit (RSU) and vehicle. The ID-based online/offline signature (IBOOS) scheme for the authentication between vehicle and vehicle to road side units (RSU) authentication. The proposed system efficiently enhance the security in the VANET environment.

Keywords — Vehicular Communication, ID-Based Signature, ID-Based Online/Offline, Public-Key Cryptography, Roadside Unit, Regional Trusted Authority.

1. INTRODUCTION

Vehicle ad hoc network (VANET) is a technology which make use of moving vehicles as nodes in a network to establish a mobile network for communication among vehicles, road side units (RSUs) and regional trusted authorities (RTAs). A VANET is a sub group of mobile ad hoc network (MANET). Which make every vehicle in the network into a wireless router or node, and make approximately 300 meters range to connect with each other. VANET having IEEE standard of 802.p and have a frequency range of 5.9 GHZ. Vehicles are equipped with intelligent transportation systems (ITS) which are capable of longer transmission ranges, having storage capacities, and rechargeable power source. A Vehicular Ad hoc Networks is a special type which are different other Mobile Ad hoc Networks, which make use of vehicles for network nodes. The main difference other network is that mobile routers are created by network of vehicles like cars or trucks. Several different applications are emerging which utilize vehicular communications. For example, safety applications for driver for driving, information services to inform drivers about the traffic and business services using internet and other multimedia application. Most of the government and privet organization of different countries are working and updating technology to provide new applications for VANETs. VANET provide communication between vehicle which is having coverage area of 300m and The road side unit (RSU) which act as a base station to provide a vast coverage to VANET technology. The main focus of VANETs is to increase road safety and safe driving by the use of wireless communications. For achieve these goals vehicles acts as like sensors network and inform other vehicle about abnormal condition in roads and environmental conditions like accident, traffic jams, rain and snowfall. Vehicular networks resemble ad hoc networks properties because of their rapidly

updating and changing topology, so that VANETs require secure routing protocols.

2. CHALLENGES IN IMPLEMENTATION

VANETs is used for various safety applications, and non-safety applications, such as accident warnings, road navigation and traffic information. In VANETs, The user authentication is major security service for access control in both inter-vehicle and vehicle-roadside communication [13]. Moreover privet data of the vehicles need to be protected and non-repudiation access to authorized people to track the vehicle in the network. I.e., safety applications require a well-structured authentication, because most of the information transferred are safety related messages and it contain life-critical information. Therefore in this paper, along with the development of the VANET technology based on advancing smart vehicles, and other undiscovered potential threats on security, we are solving the issues of authentication with privacy preservation and non-repudiation in VANETs. There is a number of research work related to the authentication issue in VANETs [18], by using symmetric key cryptography or asymmetric key cryptography managements [1]. In the proposed system we are using asymmetric key based cryptography for message authentication [4], [5]. The drawback of using symmetric key management is that we are having only one key for encryption and decryption which allow the inducer can easily crack the system and the vehicles have to authenticate each other through a trust authorities, which is difficult for large-scale vehicular communications in VANETs and less security. The asymmetric key system is mostly used in VANET because we are using separate keys used for encryption and decryption i.e. public key and privet key. Asymmetric key cryptography based authentication are classified into two classes: public key infrastructure (PKI) based authentication and identity (ID) based authentication. Although many PKI based authentication frameworks are available but they are not so powerful in privacy preservation and a certificate revocation lists (CRLs) is maintained by every vehicle which make communication overhead and memory space [4]. Authentication frameworks using the ID-based signature (IBS) schemes based on the ID-based cryptography (IBC) have been proposed to reduce the communication overheads, in which the certificate management process has been simplified by using the digital signature schemes. We note that, the IBS schemes can be adopted to the authentication service for VANETs, in which each vehicular identity is used as a public key for signing/verifying messages in communication. Using ID-based online/offline signature (IBOOS) is an attractive solution for authentication in VANETs, for alleviating the computation overhead of the IBS process. An IBOOS scheme increases efficiency of the pairing process by separating the signing process into an offline phase and an online phase, in which the verification is comparatively more efficient than that of IBS [9], [10]. In this paper, different from the existing work, we propose an authentication framework by utilizing the IBS scheme in the V2R communication, and together with the IBOOS scheme in the V2V communication for better performance. In IBOOS for VANETs, the offline phase can be executed initially at RSUs or vehicles, while the online phase is to be executed in vehicles during the V2V communication. In VANETs, usually vehicles' drivers (users) do not want their private information such as vehicle names, positions, moving routes, and user information to be revealed, in order to protect themselves against any illegal tracing and/or user profiling. That is, the anonymity of vehicular identities should be supported for the privacy preservation in VANETs. Achieving anonymity by using vehicle pseudonyms is a superior solution for the privacy preservation, which intimately links a real-world identity (ID) to the corresponding pseudonyms. In VANETs, the pseudonym of a vehicle may be generated by the fixed RSUs or the vehicle itself, even can be downloaded from a trusted link from the RTA periodically. On the other hand, when traffic accidents or certain crimes occur, the vehicle anonymity should be conditionally retrievable, and the identity information should be revealed to legal authorities to establish the liability of accidents or crimes, which is so-called conditional privacy or conditional anonymity. The non-repudiation service in VANETs prevents a vehicle from denying previous commitments or actions. For example, vehicles causing accidents should be reliably identified, or a vehicle cannot deny services received. Therefore, the privacy preservation with non-repudiation service is required for VANETs, against the abuse of anonymous authentication techniques by malicious vehicles to achieve malicious goals or escape from liabilities. The pseudonymous authentication used in vehicular communications can provide the privacy

preservation with an effective tracing mechanism, which is used only by the trusted authorities (e.g., the certification authority (CA)) to reveal the real identity of malicious vehicles. Many existing system shows the issues of privacy preservation and non-repudiation for VANETs [10], [13], [14], [21], [22], various methods of using anonymous credentials are different in each proposal, which render these issues more important and more complex to be handled in VANETs.

3. NEED FOR VANET'S

In this paper, we consider security improvement in VANET to make effective communication for the Regional Trusted Authority (RTA), the fixed RSUs at the road side, and the mobile vehicle equipped navigation system. The RTA is a registration and certification center for RSUs. Only the TA have the real identity of the vehicle. RSUs work as intermediaries between vehicle and RTA in a secure channel. They are responsible for filtering fake messages from malicious vehicles and reporting vehicle's certificate information to RTA. Vehicles regularly broadcast traffic-related status information to help drivers. A secure privacy-preserving protocol are needed in VANET to satisfy the following requirements [3], [5].

1. V2R Mutual Authentication: To defend prevent and protect against maliciously-behaved vehicle, it is important to archive mutual authentication between RSU and vehicle before the information exchange.

2. V2V Mutual Authentication: In the absence or non-coverage area of RSUs, vehicles should be able to authenticate each other and discover and communicate each other vehicle to disseminate safety message to each vehicle using an ad hoc vehicular networks.

3. Anonymous authentication: Authentication should be verified without revealing their identities.

4. Unlink ability: The attacker should not be able to link the relation between packets issued by a vehicle even by eavesdropping transmitted message in an open wireless channel.

5. Vehicle ID traceability: Vehicle in the VANET network should be able trace by authorized authority like cops and other registered authority's,

6. Efficiency: The authentication process should be efficient, when there is a large number of vehicles which are passing through the RSU we need secure link which connect all the vehicle in the network before it leave the communication range of RSU.

Attacks on authentication [4], [6]: There are two kinds of attacks related to authentication in VANETs and are given as follows:

1) Masquerade attack: The attacker pretends to be another entity. The masquerade attack will steals the communication information and privet data of other vehicle. As a consequence, the malicious vehicle will send false messages and make system failure.

2) Sybil attack: In VANET vehicle will be the attacker, so malicious vehicle use different identities at the same time and attack the network system.

Attacks on privacy: Attacks on privacy over VANETs are related to illegally gathering of sensitive information about. As there is a relation between a vehicle and its driver, the exposure of a vehicle's secret/ sensitive information could affect its driver's privacy:

1) Identity revealing attack: Getting the owner's identity of the vehicle malicious vehicle will put its privacy at risk. Vehicle's owner is also its driver, so it can get personal data about that person or the vehicle.

2) Location tracking attack: The location of a vehicle in a given moment. It allows the attacker to build the vehicle's profile and, therefore, tracking its driver.

Attacks on non-repudiation: In VANETs, the non-repudiation is related to the fact that a vehicle cannot deny a specific message if it has sent that message. Conventionally, by producing a signature for the message in VANETs, the vehicle cannot later deny the sent messages. The attack on the message non-repudiation is explained as follows [13]:

1) Repudiation attack: Repudiation refers to a denial of service or communication in VANET for some part or all part of communication. For example, the malicious vehicle denial information to RTA.

4. SYSTEM DESIGN

Vehicular ad hoc networks have derived from mobile ad hoc networks (MANETs) and Ad hoc network composed of vehicle which is Equipped with wireless communication devices, positioning system and digital maps. VANET having

IEEE standard of 802.11p. System is having a short range radio technology like WLAN.

Vehicle ad hoc network (VANET) is a technology make use of moving vehicles as nodes in a network to form a mobile network to provide communication between vehicles, road side units and regional trusted authorities. RTA which serves as a server for entire communication. In this proposed system we are using public key cryptography where we have set of key for encryption and decryption making the system highly secure.

There three main blocks in VANET environment as shown in Fig-1. They are

1. Vehicle
2. Road Side Unit (RSU)
3. Regional Trusted Authority (RTA)

Vehicle are used for the communication which make VANET communication, vehicle having a communication coverage of 30 meter, using vehicle communication it will pass information like braking, vehicle turn indication, traffic information, road accident, weather report and so on.

Rode side unit (RSU) which act as a base station having a large coverage like mobile tower, WiMAX and so on make an increase in communication rage where Vehicle ad hoc coverage is not there. Data received through vehicle is passed to RSU to inform emergency information to authorized authority like accident, robbery, and traffic information's.

Regional Treated Authority (RTA) is used in VANET which serve as a server having all the details about the vehicle, both public encryption key and privet decryption key are stored in RTA memory and the history of location and current position of vehicle and this RTA help the authorized authority like cope to find the location of specific vehicle.

The vehicle is registered in regional trusted authority when it enters into VANET. Vehicle have its own ID and it is registered on RTA, we are using ID based Public Key Cryptography (IDPKI) for key exchange between vehicle and road side unit. In ID based cryptography identity of vehicle is preserved by using some random ID for communication with vehicle, RSU and RTA, this will prevent an inducer to track the vehicle and get the information about the private data of the vehicle. We are using a pair of key which are different for encryption of message and decryption of message which making the system highly secure. Using PKC each vehicle creates its own private and public key and it is known to RTA.RTA pass the public key of the vehicles to RSU and it transfer to vehicles in network.

Communication between roadside units to vehicle is done using ID Based Cryptography (IBC), where the real name or identity of the vehicle is replaced by some ID so it avoids tracing of vehicle by their name or identity, using vehicular ID key transfer and data communication is maintained. Communication between vehicle to vehicle and vehicle to roadside is done using ID Based online and offline Cryptography (IBOOC).Where Online cryptography is used in communication between vehicles i.e., the network should be always active, it need to transfer information like accident, traffic alert and other information to vehicles and Offline cryptography is used in communication between vehicles and roadside unit i.e., when vehicle is registered in network can communicate in offline network. The IBOOC make faster communication between vehicle and RSU with less overhead. System model is shown in Fig-1

Using IBC and IBOOC, private data of vehicles are preserved because we are exchanging only ID of the vehicle and trusted third party can trace the information about the vehicle by communicating with regional trusted authority.

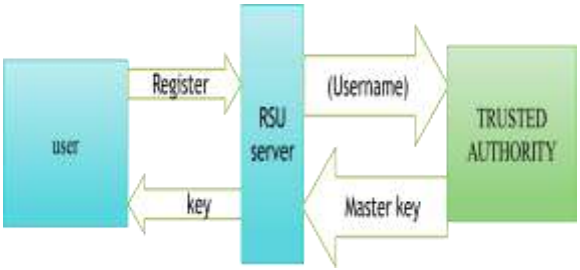

Fig-1: System model

Program module have four parameters they are as followers

1. Creating the VANET environment
2. Route discovery
   2.1 Route request
   2.2 Route reply
3. Registration process in the RSU
4. Vehicular communication using RSU

4.1. Creating the VANET Environment

We providing vehicle which is having sensors and RSU's for the certain coverage area of the vehicles which act as base

station. TA (Trusted Authority) which act as a server and will have all the information of the vehicle in the coverage area and provide authentication to the user. Model shown in Figure 3.3.

4.2. Route Discovery

Rout discovery is a routing process to find route to destination. In VANET route finding which is initiated by the source vehicle to provide route to the destination node, if the source vehicle has no route to the destination vehicle, then source vehicle find route discovery process by on-demand routing. After generating RREQ, node check with the neighbor node route table for route to destination, if route is available the RREQ packet is forwarded to that vehicle. If no closer neighbor are available then RREQ packet is flooded to all neighbor. On receiving RREQ the destination vehicle produces a route reply (RREP) for three cases as below.

1. If the RREQ packet is a having higher sequence number or first to be received from a source vehicle.
2. If the RREQ packet having higher source sequence number than the RREQ packet which it is received before by the destination vehicle.
3. If the RREQ packet is having the same source sequence number which it received before, but it have a better route to the destination.

4.3. Registration Process in the RSU

All the users i.e. the vehicle in the VANET will register their details in the RSU. After registration the RSU will provide one initial packet key to the user. Using this initial packet key, the user will get information about the other nearby vehicles from the RTA. Model shown in Figure 3.4

4.4. Vehicular communication using RSU

In this module, we are providing routing protocol to make communication between vehicle and RSU. The service between RSU should be service oriented so that it should be service oriented by making use of internet facility. .

5. SYSTEM ALGORITHM

In the proposed system pseudonym generation is done using PKC, the IBS is used for communication and authentication between vehicles and RSUs, and the IBOOS scheme for the authentication and communication between vehicles and RSU. These schemes are applied in the proposed system. The conventional IBS and IBOOS schemes are not specifically designed for VANETs. In this section, we are giving a basic background of the PKC scheme, IBS scheme and the IBOOS scheme used for VANETs.

5.1. Public Key Cryptography

PKC is an asymmetric key algorithms, where we have different key for encryption and decryption of message [18]. Many public key based system for VANET'S Diffie–Hellman are available for pseudonym generation, like RSA [1], deffi-helman, SHA-1 and SHA-2 [11], [14]. In the proposed system for VANETs, each vehicle v have a pair of cryptographic keys, i.e., encrypted public key pk_v and a decrypted private key sk_v. The RTA generate pair of cryptographic key periodically, and RTA pass public key to vehicle through RSU in a secure channel. Public key pk_v of all vehicle are broadcast by the RSU, and private key sk_v is known only to the RTA. Vehicle communicate each other using public key pk_v and decrypt the message using privet key of the vehicle sk_v.

5.2. IBS Scheme

ID-based signature scheme [17] for VANETs is based on four steps they are setup, key generation, signature signing and verification.

Setup: The RTA generate a master key K and public message PM for the private key generator (PKG), and gives PM to all vehicles.

Extraction: Using vehicle ID, vehicle generates a private key $DSEK_{ID}$ associated with the ID of the vehicle using the master key M.

Verification: Based on the ID, M and DSIG, the receiving vehicle will verify the authentication, if DSIG is valid one else connection is dropped.

5.3. IBOOS Scheme

ID-based online/offline signature scheme [15] is used for communication between vehicle and vehicle to road side unit. IBOOS for VANETs consists of five steps they are, key extraction, offline signing, online signing and verification:

Setup: Process is same as that in the IBS scheme.

Extraction: The RTA generates a private key $DSEK_{ID}$ associated with the ID of the vehicle using the master key M.

Offline signing: Offline signature is used for communicating between vehicle and roadside unit, Vehicle can transfer the road information to road side unit such that it can inform other vehicle where vehicle to vehicle communication do not exist. Using $DSEK_{ID}$ and public message, the RTA generates an offline signature $DSIG^{offline}$ for each vehicle.

Online signing: Online signature is used for communicating between vehicles because it should be always active to transfer road information periodically to other vehicle in the network Using offline signature $DSIG^{offline}$ and a message M, the sending vehicle generates an online signature $DSIG^{online}$, of M.

Verification: using ID, M and $DSIG^{online}$, the receiving vehicle accept the connection if $DSIG^{online}$ is valid and reject connection if not valid.

5.4. Pseudonym Generation

For privacy preservation, user defined ID based PKC-based pseudonym instead of the real-world ID for authentication process. RTA periodically broadcasting the current public key via RSUs to vehicle for pseudonym generation, the vehicle can use PKC-based pseudonym generated by RTA for communication and can update its current pseudonym key or generate a new pseudonym. Vehicle can create self-generated PKC pseudonym as follows:

$$PSG_V \stackrel{def}{=} \text{Time} \parallel E_{pv}(ID_v \parallel HL \parallel RSU \quad \ldots\ldots\ldots (1)$$

Where Time is the current time at pseudonym is generation. PSG_V is the encrypted value generated by vehicle using vehicle's real ID, by exploiting PKC's public key pk_c Obtained from the RSU. HL denotes represent vehicle's home location. RSU denotes the ID of the current RSU in coverage.

6. AUTHENTICATION PROCESS

Authentication in VANETs can be divided into three they are vehicle-roadside authentication, roadside-vehicle authentication and in between vehicle authentication. In the proposed system, RSUs are broadcasting their information periodically to vehicle and and in between RSU, and all the operations at RTAs and RSUs is trustful.

6.1. Authentication for V2R and R2V

The authentication process for V2R and R2V is carried three steps. We take an example in Fig-2 for illustrate of authentication between e RSU and vehicles.

Step 1: The RSU which act as base station and it transfer information to vehicle and different RSU is broadcasting its information periodically, vehicle in the transmission range of RSU can get the information. V2R and R2V authentication. $\{ID_r, T, pk_c, adv, new, SIG_r\ (ID_r \parallel T)\}$ Where ID_r is the ID of the current active RSU, T is the time stamp. pk_c is the public key broadcast by RTA., and new is the freshness of message. $SIG_r\ (ID_r \parallel T)$ is the IBS process used for R2V authentication using RSU id , which is generated from the RSU's ID ID_r and the time stamp T.

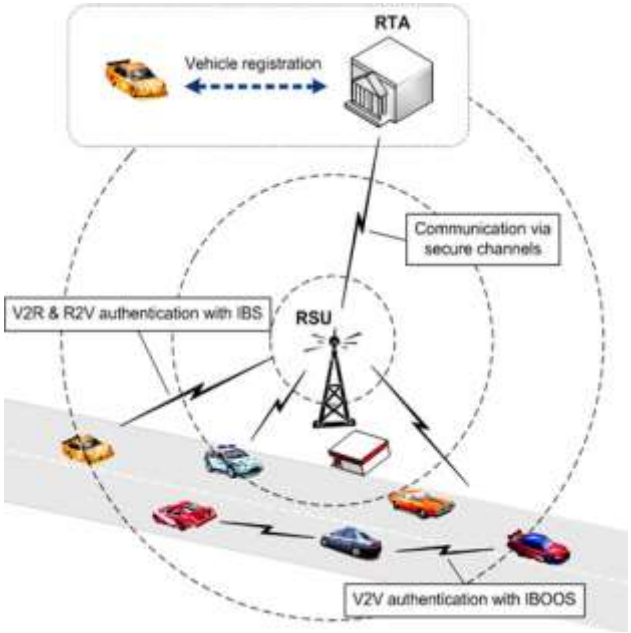

Fig-2: Vanet Architecture

Step 2: A vehicle replies a message to the corresponding RSU for any of the following two cases, for V2R authentication using IBS scheme, a vehicle need to update its pseudonym or need for a newly generated one and the second case when vehicle receives a new RSU ID from a RSU message. Fig-2. An illustration of the operations for VANETs. The vehicle send new pseudonym as a message to the RSU message $\{ID_r, NPS_v, T, join, DSIG_r\ (NPS_v \parallel T)\}$ where ID_r is the destination id of RSU, NPS_v is the new pseudonym which is generated, join is the request message for joining, and $DSIG_r$

$(NPS_v \parallel T)$ is the digital signature generated from the vehicle's pseudonym NPS_v and T is the time stamp.

Step 3: When receiving the join request message the RSU verify the message and if authenticated it accept the message else reject it. After accepting the message the RSU send the pseudonym NPS_v to RTA and it will update. Then the RSU generates the offline signatures $DSIG_v^{offline}(NPS_v)$ from the pseudonym NPS_v for the vehicle. Afterwords the RSU will send an allocation message to all the vehicle in coverage area, IBS is used for authentication of R2V. The allocation message consist of RSU ID and it is in the form $(NPS_v/DSIG_v^{offline}/(NPS_v)/ID_r)$, where digital signature of RSU is $DSIG_v^{offline}/(NPS_v)/ID_r)$ Here ID_r denotes the current RSU. All the vehicles in the coverage area of current RSU's will receive the message, and accept the message it if the signature verification is valid else it will drop the message.

6.2. V2V Authentication

The V2V authentication is used for secure vehicle communication. Vehicle need to get information from other vehicle, which is achieved only when authentication is successful.V2V authentication is done using IBOOS it first compute online signature $DSIG^{online}$ using the offline signature $DSIG^{offline}$. The receiver vehicles use online signature for the V2V communication and authentication. When a vehicle need to communicate with each other in communication range it first compute online signature $DSIG_v^{online}(DSIG_v^{offline}(NPS_v) \parallel T)$ from the offline signature $SIG_v^{offline}(PS_v) \parallel T$ and the time stamp t. Then, it can broadcast the authentication message as $\{NPS_v, T, new, DSIG_v^{online}(DSIG_v^{offline}(NPS_v) \parallel T)\}$ on receiving the authentication message from the sender vehicle, the vehicles verify the online signature with the stored details of the corresponding vehicle.

6.3. Authentication between RSU and V2V

The authentication between RSU and V2V occur a vehicle receive authentication message from other vehicle whose authentication details is not in the memory of the receiver vehicle , then it will enquire the RSU for authentication parameter which consists of three steps:

Step 1. Let vehicle A wand to authenticate with the nearby vehicles, then vehicle A broadcasts the authentication message with its online signature $DSIG_A^{online}$ of the form $\{NPS_A, T, new, DSIG_A^{online}(DSIG_A^{offline} \parallel T)\}$.

Step 2. When receiving authentication message from vehicle A, vehicle B checks the authentication information in B's memory. If the information does not exist in vehicle B's memory then vehicle B transmits a enquiry message to its current RSU for authentication parameter, where message includes authentication details of vehicle of A in the form $NPS_A/DSIG_A^{offline}(NPS_A)ID_r)$.

Step 3: On receiving the enquiry message RSU check with authentication details of the vehicle in its memory or check it with RTA. Then the current RSU send the result back to vehicle B with $DSIG_{Ar}$ and if it is not authenticated it will inform that it is a malicious vehicle.

6.4. Authentication between RSU

When a vehicle enters a new region, it first register with RTA so that new RSU can get the information about the old RSU and communication is reestablished. After finishing registration procedure with above V2R, R2V and V2V authentication.

7. RESULT

The proposed system use using network stimulator 2 (ns2) for stimulation using a nam window and Xgraph. Enhanced privacy preservation and non-repudiation for VANETS is based on ID Based Scheme (IBS) and ID Based Online Offline Scheme (IBOOS) provide better security and privacy preservation in compared with the existing systems.. Storage requirement of IBS and IBOOS is of 4.2 M bytes, so the system is storage efficient. System output includes

Create VANET environment: VANET environment consist of 11 mobile nodes i.e. the vehicle, four Road Side Unit (RSU) and a Regional Trusted Authority (RTA). Model output is shown in Fig-3. in nam window.

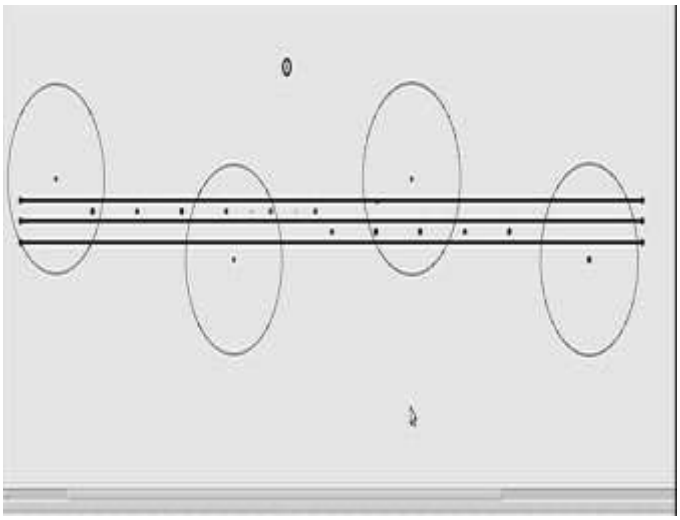

Fig-3: Create VANET Environment

Vehicle registration with RSU: Registration of vehicle with RSU is the first step to make communication with RSU, which need a user ID, region where the vehicle is currently located, current RSU which is serving the vehicle and vehicle password as shown in Fig-4. The ID and password should be authenticated with Regional Trusted Authority (RTA). The registration starting with RSU, which require certain parameter about the vehicle, current region and RSU. For registration with RSU we should produce the user ID, current region where we are located, and the password.

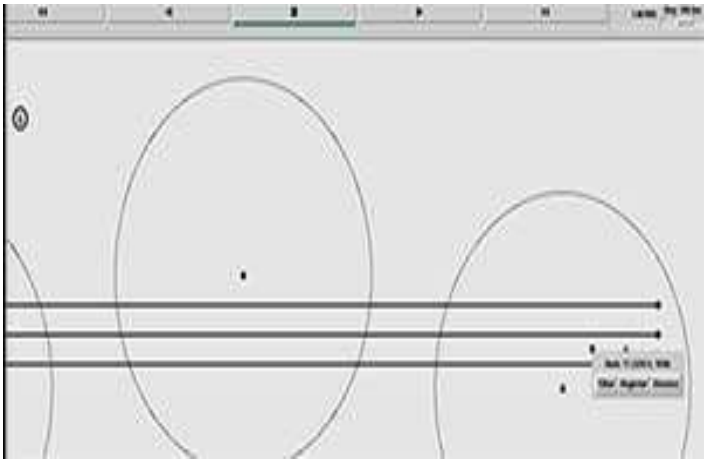

Fig-4: Vehicle Registration with RSU

RSU pass the information to RTA: Road Side Unit (RSU) receive the registration information form vehicle and it is passed to Regional Trusted Authority (RTA) and it will verify the data with the information about the vehicle in RTA and pass the authentication detail to RSU. RTA will authenticate the data and if it succeeds data transmission between RSU and vehicle will start as shown in Fig-5 else the RTA will inform that the particular vehicle is a malicious node shown in Fig-6.

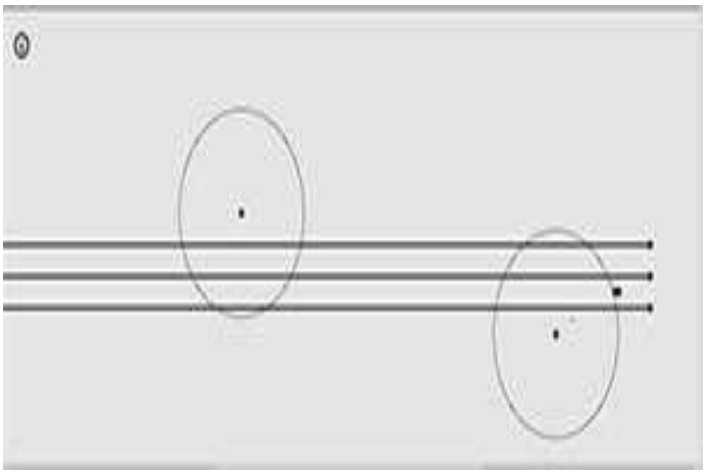

Fig-5: Authentication Verified

7.1. Delay Calculation

The proposed system using IBS and IBOOS having higher security than the existing system but it increases the delay time in transition of packet as shown in Fig-7, Delay increased due to the enhancement in the security area. Further enhancement can be implemented to reduce delay.

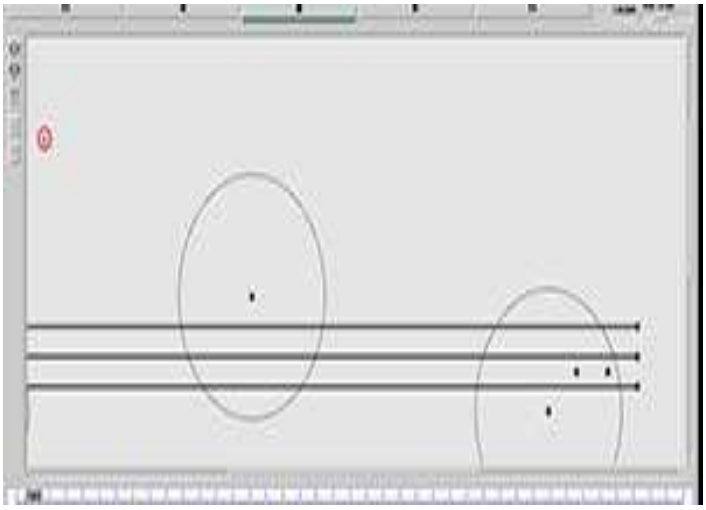

Fig-6: Detection of Malicious Vehicle

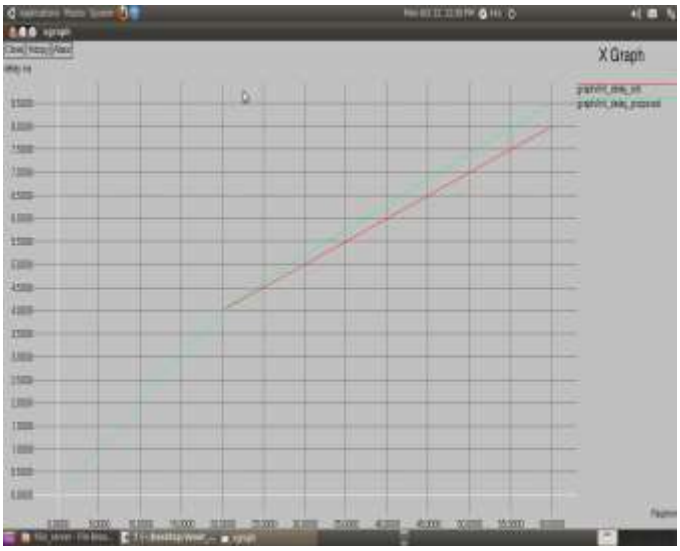

Fig-7: Delay Calculation

8. CONCLUSIONS

In this paper, enhanced privacy-preservation and non-repudiation for VANETs which utilizes the IBS and IBOOS for privacy preservation and authentication and public key cryptography for pseudonym generation. From the analysis the system achieves the desired privacy preservation, non-repudiation and security for VANET environment. Analysis and performance evaluation show that, the proposed system is feasible and adequate for VANET environment for efficient privacy-preserving authentication with non-repudiation. Future work can be done to enhance security by using a new Hybrid cryptographic approach that ensures higher security than the existing system and We illustrate a new handover scheme can be implemented for RSU that provide higher coverage and interoperability between different network that is particularly suitable for VANETs.

REFERENCES

[1] Anjali Patil, and Rajeshwari Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices" International Journal of scientific & technology research volume 2, issue 8, August.2013.

[2] Daojing He, Sammy Chan, Mohsen Guizani, Haomiao Yang, and Boyang Zhou, "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks" IEEE Transactions on Parallel and Distributed Systems, VOL. 26, NO. 4, April.2015.

[3] H. Dok et al, "Privacy Issues of Vehicular Ad-Hoc Networks," Int'l J. Future Generation Comm. and Networking, vol. 3, no. 1, pp. 17-32.

[4] H. Lu, J. Li, and M. Guizani "A Novel ID-Based Authentication Framework with Adaptive Privacy Preservation for VANETs," Proc. Comm. and Applications Conf. (ComComAp), pp. 345-350, March.2012.

[5] Huang Lu, Jie Li, and Guizani "A novel ID-based authentication framework with adaptive privacy preservation for VANETs" International Journal on Communication and Application (345 – 350), volume 23-No .31, June.2012.

[6] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks" IEEE Transactions On Vehicular Technology, Vol. 60, No. 1 August.2011.

[7] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey" IEEE Communication Surveys & Tutorials, VOL. 17, NO. 1, First Quarter 2015.

[8] J. Sun et al, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, February.2010.

[9] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" IEEE Transactions on Vehicular Technology, VOL. 62, NO. 2, February. 2013.

[10] Lo-Yao Yeh and Yu-Cheng Lin, "A Proxy-Based Authentication and Billing Scheme With Incentive-Aware Multihop Forwarding for Vehicular Networks" IEEE Transactions On Intelligent Transportation Systems, Vol. 15, No. 4, May.2014

[11] M. Alimohammadi, and A. A. Pouyan (2014) "Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET" International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February.2014.

[12] Mansoor Ebrahim, Shujaat Khan, and Umer Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis" International Journal of Computer Applications (0975 – 8887), Volume 61– No.20, January.2013.

[13] Mina Rahbari1 and Mohammad Ali Jabreil Jamali, "Efficient Detection Of Sybil Attack Based On Cryptography In VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, April.2011.

[14] Shanmuga Priya.S , and Erana Veerappa Dinesh.S, "A Novel Approach for Data Acquisition and Handover Scheme in VANET" Shanmuga Priya.S et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5.

[15] Song Guo, Senior Member, IEEE, Deze Zeng, Member, IEEE, and Yang Xiang, Senior Member, IEEE, "Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 11, December.2014

[16] SuKyoung Lee, Member, IEEE, Kotikalapudi Sriram, Fellow, IEEE, Kyungsoo Kim, Yoon Hyuk Kim, and Nada Golmie, Member, IEEE, "Vertical Handoff Decision Algorithms for Providing Optimized Performance in Heterogeneous Wireless Networks" IEEE Transactions On Vehicular Technology, Vol. 58, No. 2, March.2009.

[17] Xiaodong Lin, Xiaoting Sun, Xiaoyu Wang, Chenxi Zhang, Pin-Han Ho, and Xuemin Shen, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving" IEEE Transactions On Wireless Communications, VOL. 7, NO. 12, December.2008.

[18] Xiaoyan Zhu, Shunrong Jiang,and Hui Li, "Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks" IEEE Transactions on Vehicular Technology, vol.63, no. 2, February.2014

[19] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificate less Public Keys" IEEE Transactions On Dependable and Secure Computing, VOL. 3, NO. 4, December.2006.

[20] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen, and Jinshu Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications" IEEE Transactions on Vehicular Technology, vol. 23, no. 4, February.2010

