MULTI-HOP CLUSTERING WITH CONDITIONAL PRIVACY PRESERVATION FOR VANETS

[1]M.Ramakrishna, [2]P.Vijayasree, [3]V.Siva Jyothi, [4]A.Revathi
[1]Associate professor, [2]FinalB.Tech, [3]Final B.Tech, [4]Final B.Tech
[1]Electronics and Communication Engineering,
[1]Andhra Loyola Institute of Engineering and Technology, Vijayawada,Andhra Pradesh

***Abstract: In* Vehicular Ad hoc Networks, authentication is a crucial security service for both inter-vehicle and vehicle-roadside communications. On the other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy, as well as to be capable of being investigated for accidents or liabilities from non- repudiation. In this paper, we investigate the authentication issues with privacy preservation and non-repudiation in VANETs. We propose a security framework for providing Authentication with Conditional Privacy-preservation and Non- repudiation for VANETs. In ACPN, we introduce the public-key cryptography to the pseudonym generation, which ensures legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicles' real IDs. The self generated PKC-based pseudonyms are also used as identifiers instead of vehicle IDs for the privacy-preserving authentication, while the update of the pseudonyms depends on vehicular demands. Typical performance evaluation has been conducted using efficient IBS and IBOOS schemes. We show that the proposed ACPN is feasible and adequate to be used efficiently in the VANET environment.**

IndexTerms: VANET, IBS, IBOOS,security, Trust Authority.

I. INTRODUCTION

It is designed in order to provide a security Framework for Authentication with Conditional Privacy-preservation and Non-repudiation for VANETs. In Vehicular Ad hoc Networks, authentication is a crucial security service for both inter-vehicle and vehicle-roadside communications and vehicles have to be protected from the misuse of their private data and the attacks on their privacy, as well as to be capable of being investigated for accidents or liabilities from non-repudiation. Many related studies have been reported on security and privacy issues in VANETs. For instance, the message from an OBU has to be authenticated and integrity-checked before it can be relied on. Because, an attacker can alter the safety message from a vehicle or even impersonate a vehicle to transmit afake safety message. Thus, an anonymous communications protocol is needed. While being anonymous, a vehicle's real identity should be able to be revealed by a trust authority when necessary. For example, a driver who sent out fake messages causing an accident should not be able to escape by using an anonymous identity. Therefore, the anonymous identity in vehicular communications should be conditional, such that a trust authority can find a way to obtain a vehicle's real identity.

Fig.1:Traffic Monitoring

It is commonly named as conditional privacy. This model consists of a trust authority, roadside units along the roads and on-board units embedded in vehicles. RSU is trustable and usually equipped with not only high-storage capacity but strong computational capability as well. Author assumed that TA is always online, trusted and will never be compromised. The responsibility of TA is to publish digital certificates for RSUs and vehicles. RSUs are distributed in the roadside and have higher computation power than OBUs. It uses a conventional public key infrastructure for initial handshaking. Each vehicle has a conventional public key and a private key, and public key is not revealing the vehicle's real identity with the pseudonym certificate. The working procedure is given in the following figures with Initial handshaking process, Message signing, Batch verification, and Group key generation and verification.

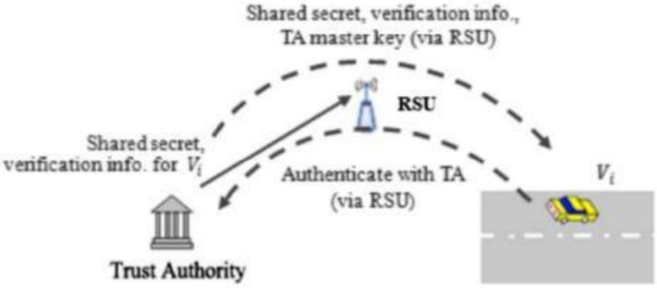


Fig. 2. Initial handshaking.

.

II.RELATED WORK

In [1] paper, author presents a position-based routing scheme called Connectivity-Aware Routing (CAR) designed specifically for inter-vehicle communication in a city and/or highway environment. A new Connectivity-Aware Routing protocol for VANETs is proposed. The CAR protocol is based on PGB and AGF to provide a scalable low overhead routing algorithm for intervehiclecommunication both in the city and on the highway but the design of CAR does not naturally allow for the inclusion of location errors in the analysis. In [2] paper, author presents Ad-hoc On Demand Distance Vector Routing a novel algorithm for the operation of such ad-hoc networks. Each Mobile Host operates as a specialized router, and routes are obtained as needed (i.e., on-demand) with little or no reliance on periodic advertisements. AODV is an on demand routing protocol in which routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is less. The HELLO messages supporting the routes maintenance are range-limited, so they do not cause unnecessary overhead in the network but the intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. The VANET has witnessed several endeavors toward the development of suitable routing solutions. Multi-hop information dissemination in VANETs is constrained by the high mobility of vehicles and the frequent disconnections. In [3] project, we propose a hop greedy routing scheme that yields a routing path with the minimum number of intermediate intersection nodes while taking connectivity into consideration. Moreover, we introduce anchor nodes that play a key role in providing connectivity status around an intersection. Apart from this, by tracking the movement of source as well as destination, the anchor nodes enable a packet to be forwarded in the changed direction. Vehicular communication networks, which are also, referred to as VANETs, inherently provide us a perfect way to collect dynamic traffic information and sense various physical quantities related to traffic distribution. Such functionalities simply turn a VANET into a Vehicular Sensor Network. Many challenging security and privacy issues in VANETs have been identified. To ensure both identity authentication and message integrity in VSNs, one appealing solution is to sign each message with a digital signature technique before the message is sent. However, conventional signature schemes that verify the received messages one after the other may fail to satisfy the stringent time requirement of the vehicular communication applications. In order to tackle the above mentioned problems and make VSNs suitable for the intelligent traffic systems, this paper introduces an efficient batch signature verification scheme for the communications between vehicles and RSUs. Author's scheme has the following unparalleled features: 1) multiple signatures can beverified at the same time instead of one after the other as that in the previously reported approaches. Therefore, the signature verification speed can be significantly improved such that the computational workload of the RSUs can be alleviated; 2) By generating distinct pseudo identities and the corresponding private keys for signing each message with a tamper-proof device, privacy regarding user identity and location of the vehicles can be protected; 3) The identities of the vehicles can be uniquely revealed by the trusted authorities under exceptional cases.

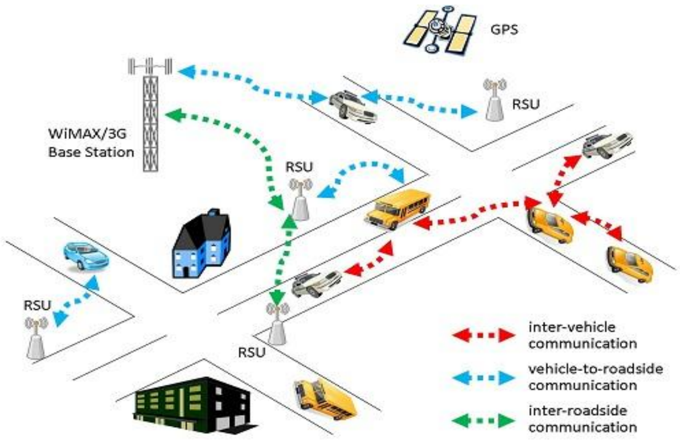

GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig.Types of vehicle communication

III.PROPOSED TECHNIQUE

The main aim of this paper is to provide the bulk verification to reduce the delay in message authentication. We are mainly focusing on the city side vehicular communication. To make communication, vehicle must register with the RTA. RSU is one of the main sources for secured communication. To make long enough communication RSU should be present in the network. In our project, we have made the following assumptions. 1) Each vehicle equipped with damper proof WiFi communication device. 2) V-V communication range is ~150m and V-R-V communication range is ~300m. 3) Each vehicle has enough memory to store the key information's. 4) In network necessary counts of RSU's available.

a)Module Description:

The project is divided into the following modules:

- ○ Network Design
- ○ RTA registration
- ○ RSU Registration
- ○ V-V communication

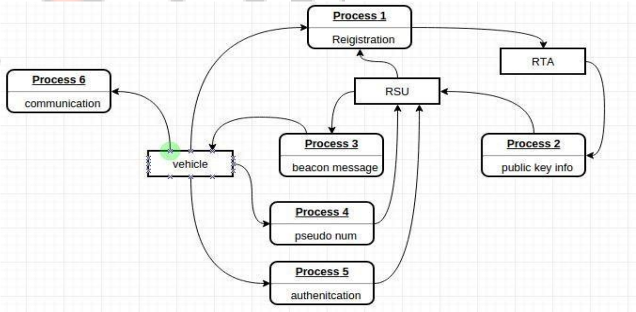


Fig.3 Data flow of proposed model

i. Network Design:

A VANET basically consists of three networkcomponents: road side units, vehicles (users) and aregional trustedauthority. In this project we assume the vehicles in an urban vehicular communications structure mainly travel on roads, and do not frequently stop at certain places. The RSUs are always reliable to cover the wireless vehicular communications of the whole region, while vehicles are vulnerable to being compromised by attackers but can change their pseudonyms as IDs on demand for the privacy preservation. The wireless communication in this structure of VANETs can be classified mainly into the following three types, the vehicle-to-roadside communication, and the roadside to- vehicle communication, and the vehicle-to-vehicle communication. Other communications are through secure wired channels, such as inter-RSU communication and RSU-to- RTA communication. The transmission range of an RSU is assumed to be much longer than that of vehicles. All vehicles use symmetric radio channels. An RTA generates cryptographic domain parameters for the RSUs and vehicles in its region, and delivers these keys to them over securechannels. It manages a list of vehicles of which the participations have been revoked, updates the list periodically, and advertises the list to the network to isolate the compromised vehicles. If a vehicle transmits false messages for malicious purposes on the road, the RTA is responsible for tracing and identifying the source of the messages to resolve any dispute. An RTA serves in one region, e.g., a city, a province or a country. An ID pool of RSUs in a region is preloaded in each vehicle, in which the number of RSUs is usually fixed that does notchange frequently.

Network Model summary is given below.

- RTA (Trust Authority Can generate the key's and act as admin) .
- RTA broadcasts Random pubic key via Registered RSU's .
- RSU controller (Region RSU controller) .
- Used to share info b/w V-V or V-RTA

  Vehicles.
- Legitimated vehicles and attacker vehicles.

ii.RTA Registration

The cryptographic key pairs are generated by the RTA periodically, and the public keys are transmitted to every RSU in its service region through secure channels. Each key is broadcast to all vehicles by the RSU, while the corresponding private key isknown only to the RTA. The RTA computes a master key s and public parameters for the private key generator (PKG), and gives to all vehicles. The vehicle registration is required before a vehicle starts off to hit the road in a region. If the vehicle is newly manufactured, it can be registered to the RTA at the car dealer via a secure network infrastructure. If a vehicle is driven into a new region, it can be registered to the RTA at the entry- exit administration or the border immigration office via the secure network infrastructure. Through the vehicle registration of each vehicle, the RTA registers the vehicle ID and profile.

iii. RSU Registration:

The PKC-based pseudonym of a vehicle is generated instead of the real-world ID in the authentication process. Since the RTA is periodically broadcasting the current public key via RSUs for the PKC in the pseudonym generation, the vehicle can use it for the PKC-based pseudonym generation, when it wants to update its current pseudonym or generate a new pseudonym.

The summary of RSU base registration is given below:

- Vehicle has to generate the Pseudonym by using Time, Home region, Current RSU, Modified vehicle id.RSU has to broadcast the own information's periodically, which contains the Time, own public key, RSU id, Digital Sign.
- Vehicle joins into the RSU with newly generated Pseudonym .
- RSU verifies the Pseudonym from the vehicles if it correct then RSU will reports to RTA.

iv.V-V Communication:

Authentication in VANETs can be divided into three categories, namely vehicle-to-roadsideauthentication, to- vehicle authentication and vehicle-to- to-roadside authentication, roadside to- vehicle authentication and vehicle-to-vehicle authentication. In the proposed ACPN, RSUs are broadcasting their information periodically, and all the operations at RTAs and RSUs are tamper-proof and being performed trustfully. The proposed ACPN operates adaptively, whenever a vehicle wants to newly authenticate itself to others, or update its current pseudonym.

The summary of vehicle communication is given below:

- Each vehicle can verify the neighbour vehicle is correct or wrong by using the offline signature verification.
- If vehicle verified correctly then the vehicle can make communication.
- If a vehicle is not having any clear info about neighbour vehicle then it will verify with RTA.

IV.RESULTS

Fig.4.1. Vehicle Registration: On terminal when we enter ./6.tcl the following window is appeared.

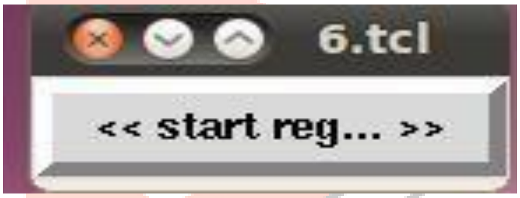
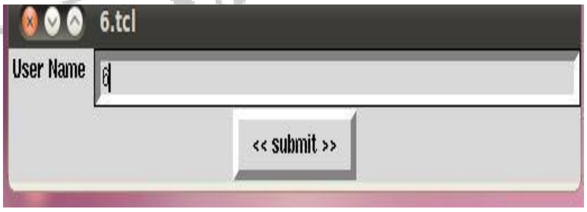


Figure 4.1: Start Registration window

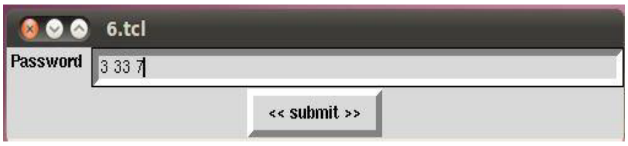
Fig 4.2. On clicking start reg.. the following screen is displayed.



User Name 6

Figure 4.2: Enter User Name window

In the above screen enter the username i.e. vehicle name (example 6). After entering click on submit. Fig 4.3. When clicked on submit the following window is displayed.

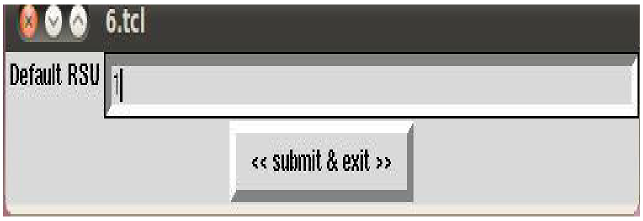


Password 3 33 7

Figure 4.3: Enter Password window

Enter the password as (3 33 7). First field (3) represents the publickey, third field (7) represents the private key and second

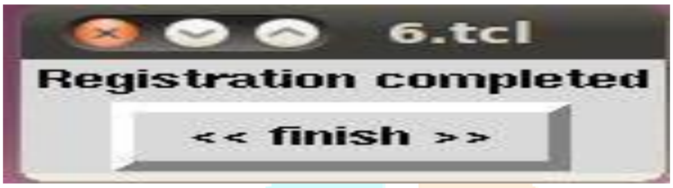
field (33) isthe n value calculated according to RSA algorithm. After entering the password click on submit.
Fig 4.4. Once submit is clicked the following window is displayed.


6.tcl

Default RSU 1

Figure 4.4: Enter Default RSU

The default RSU is set to 1 and then click on submit & exit.
Fig.4.5. On Clicking submit& exit the following window is displayed.


6.tcl

Registration completed

Figure 4.5: Registration finished

Click on finish. The registration of vehicle 6 is done. After Completion of registration of vehicles the next step is to create the system Architecture i.e. display the RTA, RSU and all the vehicles that are registered as shown in Fig4.6. System Architecture.

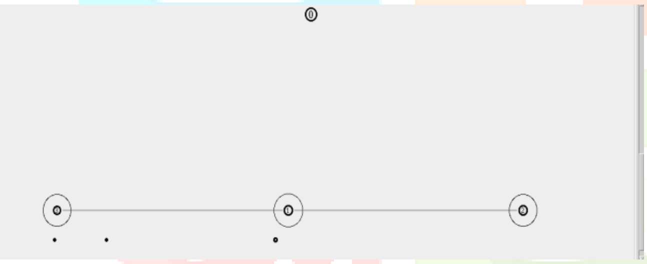


Figure 4.6: System Architecture

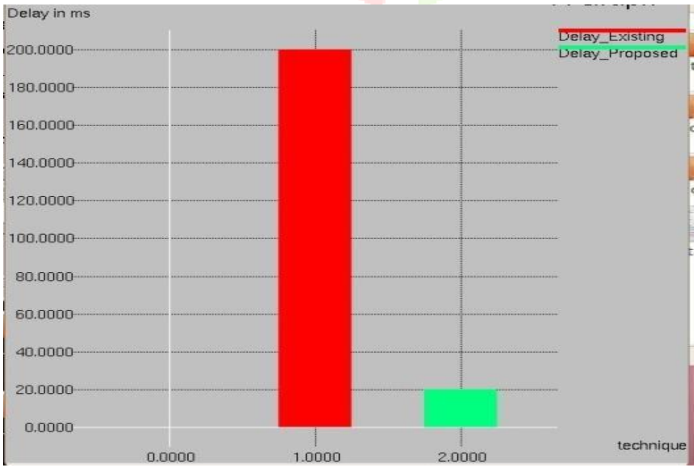


Figure 4.7 Delay Graph

- The Delay in the proposed system is low, compared to existing system.

V. Conclusion

The efficient for VANETs has been proposed, which utilizes the IBS and IBOOS schemes for the authentication, the pseudonym-based scheme for the privacy preservation, and the PKC-based scheme for the pseudonym generation. ACPN achieves the desired authentication, privacy preservation, non- repudiation and other security objectives for UVC in VANETs. Another important characteristic of ACPN is its reusability, i.e., it can also be utilized with other new schemes for security and performance improvements. In our project, we considered only security system, but in vehicles safety solution is also one of the main factors. So in the future work we need to concentrate on the safety alert system so as to provide safety for the vehicles.

References

[1]. S.Zeadally, R.Hunt. "Vehicular adhoc networks (VANETS): status, results, and Challenges," Telecomm. Syst, vol. 50, no. 4, pp. 217–241, 2012.
[2]. F.Li and Y.Wang, "Routing in vehicular ad hoc networks: A survey," IEEE Veh. Technol. Mag., vol. 2, no. 2, pp. 12–22, 2007.
[3]. M. Raya and J. Pierre, "Securing vehicular ad hoc networks," Jour. Comput. Secur., vol. 15, no.
1, pp. 39–68, 2007.
[4]. X.Lin, X.Sun, X.Wang., "TSVC: timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, 2008.
[5]. R. Lu, X. Lin, H. Zhu et al., "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," IEEE INFOCOM, pp. 1229–1237, 2008.
[6]. Y. Sun, R. Lu, X. Lin et al., "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589–3603, 2010.
[7]. P.Kamat, A.Baliga, and W.Trappe, "An identity-based security framework For VANETs," in *Proc. VANET*, pp. 94–95, 2006.
[8]. P.Kamat, A.Baliga, and W.Trappe, "Secure, pseudonymous, and auditable communication in vehicular ad hoc networks," Secur. Commun.Netw., vol. 1, no. 3, pp. 233–244, 2008.
[9]. X.Lin, X.Sun, P.-H.Ho, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," IEEE Trans. Veh. Technol., vol.
56, no. 6, pp. 3442–3456, 2007.
[10]. J.Sun, C. Zhang, Y.Zhang., "An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, 2010.
[11]. S. Even, O. Goldreich, and S. Micali, "On- Line/Off-Line Digital Signatures," in Proc. CRYPTO, pp. 263–275.
[12]. C. Zhang, R. Lu, X. Lin., "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," in Proc. IEEE INFOCOM, pp. 246–250, 2008.