INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 6 ISSUE 1 – JUNE 2015 - ISSN: 2349 - 9303

A New Secure Message Transferring in Taxi Service of Vehicular Ad Hoc Network

Dr.R.Radhakrishnan
Principal
Vidhya Mandhir Institute of Technology

Prof.K.T.Mikel Raj
Assistant Professor
Vidhya Mandhir Institute of Technology

Mr.E.Kamalavathi
Assistant Professor
Dr.Mahalingam College of Engineering and Technology

Abstract: Taxi service is an important point to point transportation in many cities. One of the major issue have to do with is safety of both the passengers and the taxi drivers. To tackle this problem and to address the certain requirements, we propos e a new message transferring scheme for the taxi service. It is based on the theoretical account of the VANET (vehicular Ad-hoc network). Vehicular networks have attracted wide attentions in recent years for their promises. Most of the transmissions in a VANET are via the DSRC wireless interface. For safety purpose the taxi's OBU uses the pseudo identities instead of real identity for all ongoing transmissions so that a passenger's travelling route cannot be traced by a third party easily. For communications protocols, our results provide lower message overhead and higher success rate than previous ones. We describe that our schemes are effective in terms of processing delay and message overhead. In detail, our navigation scheme extends to shorter travelling time while our secure taxi service scheme only introduces marginal passenger waiting delay and message overhead.

Keywords: DSRC (Dedicated Short Range Communication), OBU (On-Board Unit), VANET(Vehicular Ad Hoc Network), Success Rate, Message Overhead and Waiting delay.

I. INTRODUCTION

There are incidents of a driver with false identity robbing the passengers or a passenger robbing the taxi driver from time to time. So our VANET based Taxi Service scheme has three newly introduced security measures to reduce the risk of taxi crimes which ensures the safety of the passengers and the drivers. In this paper, we utilize the framework of vehicular network (VANET) to provide a secure and privacy based taxi service. As VANETs are still under development in many countries, interesting and useful applications are essential to promote current drivers to migrate to such a new system.

(1)Driver-based authentication: In the VANET community almost all the previous works assume a vehicle-based authentication [1,2]. That is, a tamper-proof device is installed on a vehicle. Since a taxi may be driven by different drivers at different times, this is not applicable to the taxi industry. Before providing any service each taxi driver needs to enter their real identity and password that is assigned by a trusted authority (TA) such as the Transportation department and the password can be updated later on.Driver needs to authenticate themselves before accepting any service request or before sending out any message. So that only registered drivers can send messages to the system or provide the service. The one who does not have a valid identity and password cannot provide any service and also the denial-of-service attack (DOS attack) cannot be launched to the system.

(2)On-journey protection: We propose an on-journey protection mechanism to protect the safety of both the passengers and the driver throughout the journey. It has to Periodically upload its signed GPS location to a nearby RSU, once a taxi driver has picked up a Passenger. The nearby road side unit (RSU) would have well-known fixed location signs the message as well since it may be easy for an attacker to alter the GPS receiver [3]. Mainly important to note that this approach is much more secure than requiring cell tower to sign the message in 3G-based or 4G based tracking schemes [4] because the coverage of an RSU is much smaller than that of a cell tower. Hence the location of a vehicle detected can be much more accurate. If the taxi driver is a bad guy who does not upload, else upload an incorrect GPS location or turn off the device, or if the passenger is a bad guy who forces the driver to detour, the server can broadcast the license plate number of the concerned taxi to the whole network so that other taxis can help locate it.

(3)Driver and passenger privacy preservation: One potential risk in our scheme is that by eavesdropping multiple messages sent, attacker may be able to trace a certain taxi‟s travelling route and it does not matters whether it is carrying a passenger or not. Privacy leakage caused by our scheme should be no worse than the current situation hence it encourages the taxi service operators to adopt our scheme. Two situations are seen over here: one is taxi is carrying a passenger and the other is taxi is not carrying a passenger. In case the taxi is carrying a passenger if the passenger is famous person in the city, the passenger may not want their travelling route to be traced. The driver may not want their travelling route to be traced, in case the taxi is not carrying a passenger, driver may be using the taxi for private purpose. (E.g. going to a night club with some friends). Instead of real identity pseudo identities are used in all messages sent to prevent all these from happening. The real identity of the driver can be recovered only by the server.

The rest of this paper is organized as follows: Section 2 describes the related work, the system mode landdifferent requirements used in our scheme. Schemes that are related to our research work have been explained detail in section 4.

Then we discuss the detailed analysis and the evaluation of our schemes in section 5 and 6. Finally we conclude the paper and present some future research directions in section 7.

II. MATERIALS AND METHODS

A. Related Work

In [1] for vehicle-to-RSU communications, the IBV protocol was proposed. However these works has some limitations. First this IBV protocol heavily relies on a tamper proof device installed in each vehicle, which preloads the system-wide secret key. The whole system will be compromised, once one of these devices is cracked. In [2] more recent work, for vehicle-to-vehicle communications, the RAISE protocol was proposed. The RSU has to verify the signature one after another, since no batch verification can be done. On the other hand, hash value of 128 bytes needs to be broadcasted to notify other vehicles whether a message from a certain vehicle is valid. There can be tens up to thousands of signatures within a short period of time, thus the notification messages induce a heavy message overhead.

In terms of integrity-checking and authentication, digital signature in conventional public key infrastructure (PKI) [4] is a well-accepted choice. However, requiring a vehicle to verify the signatures of other vehicles by itself as in works like [3] induces two problems as mentioned in [2]. First, the computation power of an OBU is not strong enough to handle all verifications in a short time, especially in places where the traffic density is high. To achieve both message authentication and anonymity, Raya and Hubaux in [5] proposed that each vehicle should be pre-loaded with a large number of anonymous public and private key pairs and the corresponding public key certificates. Freudiger et al. in [6] addressed the problem of achieving location privacy in VANETs with randomly changing identifiers. Sun et.al in [9] introduced a group signature scheme to sign each message. Some recent works [10-12] also propose to achieve the goal by using group signature schemes. That is, each vehicle in the system is assigned a group private key. Most recently in our prior work [15], we propose two Secure and Privacy Enhancing Communications Schemes for vehicular sensor networks.

B. System Model

It is assumed that a vehicular network to be comprising of on-board units (OBUs) set up on vehicles and road-side units (RSUs) along the roads. There is a trusted authority (TA) which holds the real identities of vehicles. Over the wireless channel using (DSRC) dedicated short range communication protocol the OBUs and the RSUs communicate with each other. The trusted server communicates using a secure fixed network (e.g. the internet). We consider that taxis and the (road side units) RSUs along the roads in the vehicular network consisting of (OBUs) on-board units installed on them. We further assume the following:

1. Secure fixed network (e.g. Internet) access the communication between RSUs and the trusted server.

2. The OBU on a taxi is confiscated with a smart card reader so that a taxi driver can connect his/her smart card (which represents his/her identity) into it.

3. For accepting taxi booking requests and for scheduling taxis in response to requests the trusted server is always online. Redundant and synchronized servers are installed to avoid being a single point of failure.

C. Proposed System

Inthis section we propose a scheme for providing secure taxi service using the framework of the VANET in details. Basically the proposed scheme has 7steps.

1. Preparation: TA prepares all system parameters and keys.

2. OBU starts up: When a taxi driver starts providing any service this module is triggered. For performing the cryptographic operations, the taxi driver starts up the OBU on their vehicle.

3. Broadcasting of passenger service request: Passenger‟s taxi service requests are broadcasted and the information are displayed on taxi‟s OBU in this module.

4. Acceptance of passenger service request: In this module, with proper authentication taxi driver accepts any passenger‟s taxi service request.

5. Driver verification and service conformation: The trusted server verifies the identity of a driver in this module and then confirms the provision of service.

6. Generation of On-journey heart beat message: Once a taxi driver has picked up a passenger, this module is triggered. Secure heartbeat messages about their current location are generated and uploaded to the trusted server

7. Report generation for witnessing: This module is triggered only when the trusted server wants to locate a taxi. A driver who identifies the taxi concerned generates a witness report and then sends it to the trusted server.

In this paper for security purpose, the process of encryption and decryption are used. Throughout this paper, the process of encryption and decryption, signing and computing hash values are followed as:

1. Encrypting plaintext MSG with the public key PU to obtain the cipher text C as C= ENCPU(MSG)

2. Decrypting the cipher text C with the private key PK to obtain the plain text A = DECPK(C)

3. Signing the message MSG with the private key PK to obtain the signature α as α=SIGPK(MSG)

4. Compute the hash value H of the message MSG as H = h(MSG)

Next, we describe all the above mentioned stepsindetail one by one. Vehicular communication systems comprise a number of interacting models that we classify broadly as follows:

1) Preparation

In our proposed scheme we consider that there is a trusted authority (TA) which hosts the trusted server. The following three initial tasks are performed by the TA:

(1.) Each taxi driver Di assigns a real identity DRIDi and initial secret key DSECKi during the network deployment or taxi driver first registration. DRIDi and DSECKi are securely kept by Di so that they cannot be easily known to anyone. Through a secure web interface DSECKi can be updated by Di at any time.

(2.) Each taxis on board unit (OBU) which contains the taxis License plate number LPj, it is assigned during the network Deployment or taxis first registration. This license plate number cannot be modified by anyone. We consider that this license plate number is burned into the OBU hardware, hence it cannot be modified by anyone easily.

(3.) Each RSUs Rk assigns an identity RRIDk during the network deployment or during the placement of new RSU Rk. And also we assume that Rk‟s location RLock is fixed and known in advance.

On the other side, three pairs of public and private keys are generated by the trusted authority TA:

Firstly public key SPU and the private key SPK for the trusted server is generated. SPU is preloaded into all the OBU.Secondly public key DPUi and the private key DPKi for the taxi driver is generated. Here DPUi and the Di‟s DSECKi forms this pair of public and private keys. Thus, DPUki will be updated by the system immediately when DSECKi is updated by Di. Thirdly each RSUs Rk forms the pair of public and the private keys as RPUk and RPKk.The further assumptions are made as follows , we assume that the trusted server has a dynamic database to store the tuples<DRIDi,DPUi,h(DSECKi)>and <RRIDk,RLock,RPUk> for the drivers and the RSUs, respectively. Here h(.) represents the one way hash function such as SHA-1.List of notations used in the proposed scheme is given below.

Notations	Descriptions
TS	Trusted authority which hosts the trusted server
Di	Taxi driver number i
Tj	Taxi number j
Rk	Road side unit number k
DRIDi	Real identity of taxi driver Di
DSECKi	Password or secret key/private key of the taxi driver Di.
RRIDk	Identity of RSU Rk
RLock	Location of RSU Rk
LPj	License plate number of taxi
SPU	Public key of trusted server
SPK	Private key of trusted server
RPUk	Public key of road side unit
RPKk	Private key of road side unit
DPUi	Public key of the taxi driver Di
Curr_Loci	Current location of taxi driver Di
ENCx(MSG)	Encryption of plaintext/message using key x
DECx(C)	Decryption of cipher text C using key x
SIGx(MSG)	Signature on message M using key x

2) On-board unit starts up

The real identity DRIDi and the secret key DSECKi of the taxi driver should be entered into the taxi‟s OBU, whenever the taxi driver starts providing any service. Using the trusted servers public key SPU ,the OBU computes the hash value of the secret keyh(DSECKi) and encrypts the DRIDi and h(DSECKi) and the encrypted message is formed as ENCSPU (DRIDll h(DSECKi)). Next, for the verification purpose this encrypted message is send to the server.

The encrypted message is decrypted by the server using the server‟s private key SPK. It checks whether DRIDi and h (DSECKi), conforms with the records in its local database. If it is conformed it replies to the message ENCDSECKi (ID_SECK_OK).Using the stored secret key DSECKi, the OBU decrypts the message upon receiving the servers reply. It is observed in two cases: one is the servers reply is positive, on the other hand server reply is negative. If the server reply is positive, it starts its function normally, and the message is decrypted. Otherwise it does not perform any function and the system hangs, it is negative in this case. It waits until another real identity and the password are given as input and verified by the server.

3) Broadcasting the service request by the passenger

To accept a taxi service requests from passenger we assume that trusted server provides a secure web service or phone interface. Each request message will be in the form <Pickup_Loc,Dest,Pickup_Time> where pickup _Loc represents the exact location to pick up the passenger, Destrepresents desired destination of the passenger (it may be the GPS representation or the represented by the landmark nearby) Pickup_time represents the time that the passenger needs the taxi.In most of the cases, passenger needs the taxi immediately (i.e. current booking is defined in most cases), in such cases Pick_up time is generally set to the current time. The trusted server prepares the message as <Taxi_Service_Request,Dest, Pickup_Time,SIGSPK(h (Taxi_Service_request||Dest||Pickup_Time))> where || represents simple concatenation. Then this message is the broadcasted. Actually the server informs all the road side units to broadcast this message. Note that here Pickup_Loc is not included in the broadcast message to ensure that only an authenticated taxi driver is going to pick up the passenger. This is because an unauthenticated taxi driver who eavesdrops the broadcast message does not know where to pick up the passenger.Each OBU displays the request information including Dest and Pickup Time, upon receiving the broadcasted request message onto a screen. Note that it displays request information only when the taxi driver is on hire.

4) Service request acceptance

A Taxi driver who is willing to pick up a passenger, if carrying no passenger first Verifies the trusted server‟s signature SIGSPK(h(Taxi_service_request||Dest||pickup_Time)) using its public key SPU. The taxi driver authenticates himself using the OBU, if the signature is valid.Instead of generating the real identity, the OBU generates the Pseudo identity i.e. DPID as ENCSPU (DRIDi||r) r is a per session random nonce. A random nonce is used to avoid replay attacks which involve using an expired response to gain privileges. The server provides the client with a nonce (Number used ONCE) which the client is forced to use to hash its response, the server then hashes the response it expects with the nonce it provided and if the hash of the client matches the hash of the server then the server can verify that the request is valid and fresh. This is all it verifies; *valid and fresh*. It computes the request acceptance message RAi =

<DPIDi,Lpj,ENCSPU(curr_Loci),SIGDSECKi{h(DPIDi||LPj||curr_Loci)}> in such a form, after retrieving the taxi‟s license plate number LPj, where curr_Loci represents the taxi‟s current location. The OBU sends this message to a nearby RSU, say Rk. Rk attaches its identity RRIDk to ensure that the taxi driver does not send a fake curr_Loci and its signature on RAi before forwarding it to the trusted server. The message forwards to the trusted server becomes <RRIDk,RAi,SIGRPKk(RAi)>.

5) Driver verification and service conformation

The trusted server may receive more than one request acceptance message in return, due to the broadcasting nature of the request message. After decrypting to get their current location the trusted server estimates which taxi can arrive the Pickup_Loc in the shortest time. Based on its real time road conditions reported by taxi drivers and by analysing its local map server finds the shortest paths from the taxi‟s current locations to Pickup_loc. When the taxi driver is chosen, without loss of any generality, the trusted server first reveals the real identity DRIDi by computing DECSPK (DRIDi). Using the drivers Di public key DPUi, then it verifies the signature SIGDSECKi {h(DRIDi||LPj||curr_Loci)}. Using the roadside units public key RPUk, next it verifies the Rk‟s signature SIGRPKk(RAi). To see whether they are in proximity of each other the trusted server compares the Rk‟s location RLock and curr_Loci. Suppose in another case, if DRIDi is not a valid identity, if any of the signature is invalid or if curr_Loci is far from RLock, then the server simply drops the acceptance message. Else the service is confirmed by the server by performing two simple tasks. First it sends the LPj to the passenger who made the service request so that the passenger can get onto the correct taxi when it is arrived. Secondly, it sends <DPIDi,ENCDPUi (pickup_loc||suggested_route), SIGSPKk (h(pickup_loc||suggested_route))> to the driver Di. Note that DPIDi is included so that Di‟s OBU knows that the message is intended for it.

Also note that Pickup_Loc is encrypted using the public key of the Di so that any other unauthenticated driver cannot get the correct pickup location by eavesdropping the message. The trusted server also includes a suggested route for Di to bring the passenger to the desired destination in the confirmation message. This suggested route is the shortest delay path computed based on the server‟s local map and road conditions reported by taxi drivers. The trusted server stores the details of the request together with taxi driver assigned into its local database for later usage.

Finally to ensure that the pickup location and the suggested route are not modified by anyone, drivers Di‟s OBU verifies the trusted server‟s signature. Note that there is also another situation, sometimes driver may not receive the server‟s confirmation message properly may be due to packet loss, due to that taxi driver does not pick up the passenger. To avoid such a situation, after sending out the confirmation message, the trusted server waits for the preset amount of time for the taxi drivers first heart beat message. It is detailed in the following sub-section. If the server still does not receive any heart beat message from the taxi driver after the preset time. The server concludes that the request is not fulfilled, and will look for another taxi driver to provide the service.

6) On-journey heartbeat message Generation

To protect both the taxi driver and the passenger, our scheme requires the taxi‟s OBU to periodically upload its current GPS location to the trusted server via RSUs nearby. This helps to ensure that the taxi travelling is on the right track towards the passenger‟s desired destination.Once the taxi driver Di picks up a passenger, the OBU on his/her taxi periodically sends the trusted server a heartbeat message. The OBU generates the pseudo identity DPIDi = ENCSPU(DRIDi||r) where r is a per session random nonce as before. Then it computes the heartbeat message as HBi = <DPIDi,ENCSPK(Curr_Loci),SIGDPWDi (h(Curr Loci))> and sends it to a nearby RSU Rk.

To ensure that the taxi driver does not send a fake Curr_Loci, Rk attaches its identity RRIDk and its signature on HBi before forwarding it to the trusted server. That is, the message it forwards to the trusted server becomes <RRIDk,HBi,SIGRPKk (HBi)>.Upon receiving this forwarded heartbeat message, the trusted server first reveals Di‟s real identity DRIDi by computing DECSSK(DPIDi) as before. Then it verifies the signature SIGDPWDi (h(Curr Loci)) in HBi using Di‟s public key DPKi. Next it verifies Rk‟s signature SIGRSKk (HBi) using RPKk. Finally, the trusted server compares RLock and Curr_Loci to see whether they are in proximity of each other. If after a preset period, the taxi driver Di does not send out heartbeat messages or if the reported location does not match the corresponding RSU‟s location or if any of the signatures is invalid, the server initiates a cooperative tracking process.

7) Cooperative tracking and witness report generation

In the cooperative tracking process, the trusted server computes the searching message <Search,LPj, SIGSPK(h(Search||LPj))> and asks all RSUs to broadcast it. Assume that the taxi driver Dw witnesses the license plate LPj while he/she is driving. Dw computes the witness report WRw =<DPIDw;LPj;Curr_Locw,SIGDPWDw (LPj;CurrLocw)> where DPIDw = ENCSPK(DRIDw||r), r is a per session random nonce and DPWDw is the password of Dw. The OBU on his/her taxi then transmits the message to a nearby RSU Rw. Similarly to the above, Rw attaches its identity RRIDw and its signature on WRw before forwarding it to the trusted server. That is, the message it forwards to the trusted server becomes <RRIDw,WRw,SIGRPKw (WRw)>

Upon receiving the witness report message, the trusted server first reveals Dw‟s real identity DRIDw by computing DECSPK(DPIDw). Then it verifies the signature SIGDPWDw (WRw) using Dw‟s public key DPKw and verifies Rw‟‟ signature SIGRSKw (WRw) using RPKw. Finally it compares RLocw and Curr_Locw to see whether they are in proximity of each other. If they are far, apart or if any of the signatures is invalid, the trusted server simply drops the witness report.

Mainly DSRC protocol plays a vital role in transferring of all these messages from one communication channel to the other, which is based on the framework of the VANET.

D.DSRCProtocol

The DSRC technology is selected as the communication method for VANET because the properties of the DSRC technology given in table 1. Operates in a licensed frequency band, Geared for safety applications, Low latency and high speed communication, Secure communication, Immunity to extreme weather conditions, High tolerance for message loss, Supports both V2I and V2V communication, Supports high vehicle speed conditions. The specifications of the DSRC Protocol are given below as Table 2.

Specifications	DSRC802.11p(Wave)
Range	Up to 1 km
Data Rate	Up to 27 Mbps
Spectrum/GHZ	5.9 (USA), 5.8(Japan,Europe)
License	Dedticated Spectrum(USA)
Access Mechanishm	Contension Based
Limitations	Short medium Range
Advantage	Low deployment costs, Distributed

Safety, mobility and environment friendliness are three main issues in improving the transportation industry. To put this into perspective, in 2008 there were 37,000 fatalities through vehicle accidents, 4.2 billion hours lost stuck in traffic and 2.8 billion gallons of fuel wasted .The Intelligent Transportation systems (ITS) program of the U.S. Department of transportation (USDOT) aims to solve these issues by integration of intelligent vehicles and intelligent infrastructure.

The goal of IntelliDrive, a major initiative of the ITS, is to provide connectivity between vehicles, infrastructure and passenger wireless devices to ensure safety, mobility and environmental benefits. The Wireless communication designed for these automotive connectivity purposes is the dedicated short-range communication (DSRC). It is a 75 MHz of spectrum in the 5.9 GHz band assigned for automotive use by U.S. Federal Communication Commission in order to increase traffic safety and efficiency.

In its five year ITS strategic plan, the USDOT is committing to the use of Wireless technology such as DSRC for active safety in both vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) application .The DSRC communication is designed as the best available choice for its low latency, high speed and high tolerance for message loss [4]. Fig 4.1 describes the specifications about DSRC.

E. Attack Model and Vulnerabilities

Presumed that participating OBUs are not secure, and communication channel are not trustworthy. Malicious performance and major attacks of an adversary can be anticipated soon. Different vulnerability in VANET environment are listed below.

Forging of the message: A challenger may try to devise a message by changing the original contents of a reasonable message from a legitimate OBU. It may also attempt to create a valid signature on the altered message payload.

Repudiation and Compromise of OBU: To obtain its secret credentials which are used for generating valid signatures a challenger may compromise an OBU. Also, a node which is compromised may advisedly send fake and harmful messages, and then further refuse its contribution in signing any such messages. Refusal of accountability of such kind from an challenger is called repudiation attack.

Reiterating and Tunneling of the Messages: From a particular traffic area, an assailant may gather and store a signed emergency message and attempt to deliver it at a later time when the original message is invalid. Similarly, an assailant may conspire with another assailant from some other different area. When the message content is irrelevant for the given circulation a conspiring assailant may tunnel the legitimate emergency messages from a specific traffic area to a different area. This needless replaying of legitimate messages would arrive at confusion among the VANET manipulators in the newfangled area.

Signature Linking: Signature linking refers to a condition when an assailant or an eavesdropper successfully discerns an anon. entity within a group by linking some of its signatures. From a particular OBU, back to back periodical messages might contain similar information in the message payload. Based on the received contents a challenger may try to use two or more successive signed messages from a node to identify the signer. For vehicular authentications in a group signature-based approach, each vehicle belongs to a group which allows „group-anonymous message signature [13].

The user-anonymity of the VANET is compromised, if the proportion of the amount of OBUs and the amount of groups in a particular scenario is not high enough.In order to extenuate the awaited attacks and vulnerabilities in VANETs, ECDSA algorithm is introduced based on the attack model and awaited susceptibilities on an anon. The authentication scheme for VANET is given below.

Elliptic Curve DSA (ECDSA): This subdivision draws the processes for generating and verifying signatures using the ECDSA.

Domain parameter generation: The domain parametric quantity for ECDSA consist of a appropriately chosen elliptic curve E defined over a finite field Zp of characteristic q, and a base point R ∈Ep(x, y) with order n.

1. Choose a random integer „i" such that $1 \leq i \leq n - 1$.
2. Compute K = iG.
3. A"s public key is K; A"s private key is i.

ECDSA signature generation: To sign a message m, an entity A with domain parametric quantity (q, Ep(x, y), R, n) and associated key pair (i, K) does the following:

1. Choose an integer x such that $1 \leq x \leq n - 1$.
2. Calculate xQ = (a1, b1).
3. Calculate r = a1 (mod n). If r = 0 then go to step 1.
4. Calculate x−1(mod n).
5. Calculate SHA-1(m) and convert this string to an integer H(m)
6. Calculate d = x−1(H(m) + ar) (mod n). If s = 0, then go to step 1.
7. A"s signature for the message m is (r, d).

ECDSA signature verification: To assert A"s signature (r, s) on m, B obtains an authentic copy of A"s domain parameter (q, Ep(x, y), R, n) and associated public key K. B then coiffes the complying:

1. Verify that r and d are integers in the interval[1, n − 1].
2. Calculate SHA-1(m) and win over this string to an integer H(m).
3. Calculate c = d−1(mod n).
4. Calculate u1 = H(m)c (mod n) and u2 = rc (mod n).
5. Calculate X = (x2, y2) = u1R + u2K.
6. If X = O , then deny the signature. Otherwise, Calculate v = x2 (mod n).
7. Take the signature if and only if v = r.

Proof for signature verification: If a signature (r, d) on a message m was certainly afforded by A, then d = i−1(H(m) + ar)(mod n). Rearranging gives

iR = d−1(H(m) + ar)R (mod n)
= d−1H(m)R + d−1raR (mod n)
= H(m)cR + rcK (mod n)
= u1R + u2K (mod n).

Thus u1R + u2K = (u1 + u2l)R = iR, and so v = r as required.

III. RESULTS AND DISCUSSION

In this section, we evaluate our scheme in terms of the following metrics using a network simulation program:

(1) The additional delay of the average waiting time for passengers due to the security measures;

(2) The amount of data transmitted in the system.

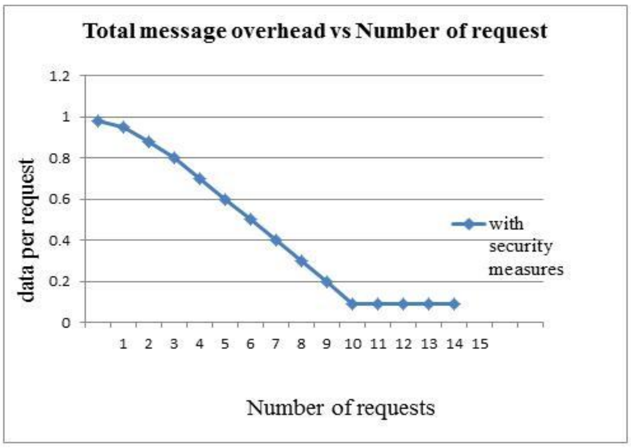
Different sizes of message components are given as Table 3.

Message component	Size (bytes)
DRIDi	20
DPWDi	128
RRIDk	20
RLock	30
LPj	8
SPK	128
SSK	128
DPKi	128
RPKk	128
RSKk	128
Time	30
Random number	10

A. Simulation models

To investigate our authentication and verification scheme we used a WAVE-based simulator with MAC priorities using the network simulator ns-2.34. This is the first simulator to implement VANET‟s periodic message broadcast with MAC-layer‟s ECDSA access categories, to the best of our knowledge. We consider a simple urban vehicular traffic scenario in a 1000m x 100m bidirectional road with 2 lanes in each direction.

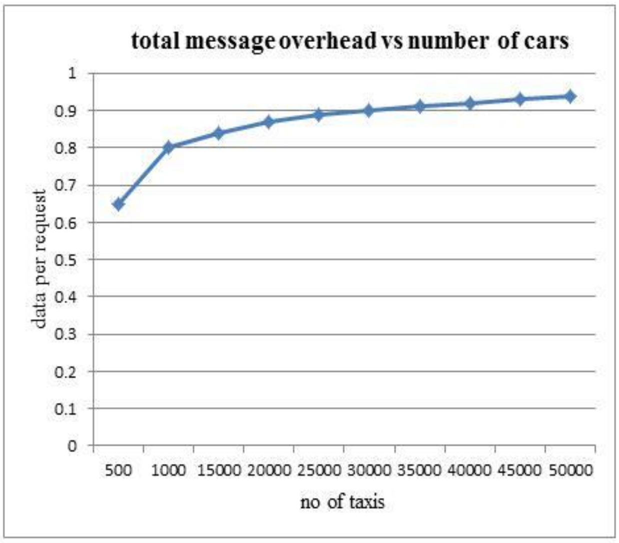
Vehicles‟ speed vary following a Gausian distribution with mean of 50 km/hr and standard deviation of 6 km/hr. OBUs are mounted with moving vehicles on road while different number of RSU is setup at the roadside. We allow the RSU and OBUs to broadcast a WSMP packet every 300 ms for simulating OBU‟s safety messages and RSU‟s encrypted messages, respectively.

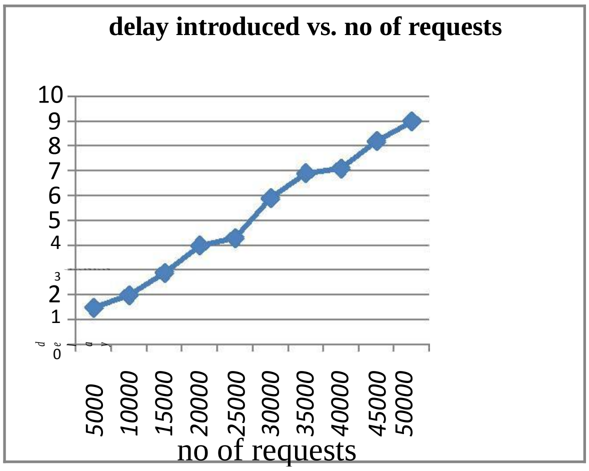


RSU broadcasts its periodical messages over the highest access category while equal number of OBUs disseminates their periodic messages over each access category. Times of the initial message disseminates for individual OBUs and the RSU have been picked out from a uniform distribution over 300 ms period. The ECDSA mechanism is implemented over IEEE Std 802.11p MAC and PHY which is provided by ns-2.34‟s IEEE 802.11Ext package given in [17].

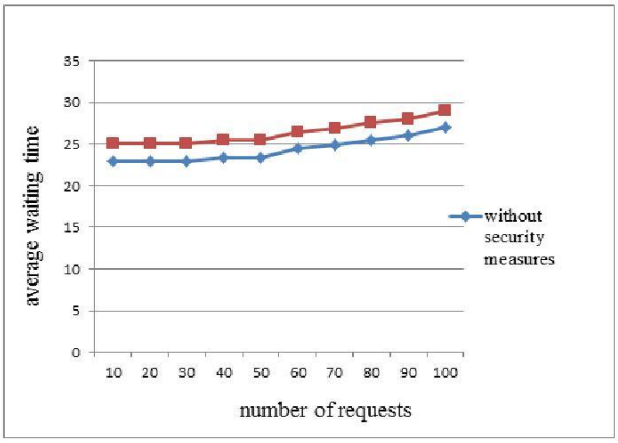
The number of requests and the number of taxis are considered as input parameters to the simulation. From Figure1 We can see that the delay increases as the number of requests increases. This is due to the fact that with more requests, RSUs need to sign more locations (from both service acceptance and heartbeat messages).

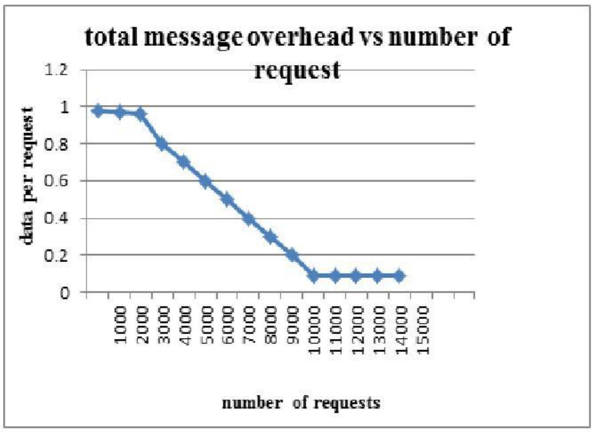
Thus a message needs to wait a bit longer at an RSU for location signing.Interestingly, the data per request decreases when there are more requests as in Figure 2. This is because when the number of requests is small, the number of replies per request is higher as there are more empty taxis and more taxis will reply for each request. Thus, the amount of data transmitted per request is more.





On the contrary, when the number of requests is large, the number of available taxis is lower and so there are fewer replies to each request. Figure 3 shows the average waiting time a passenger experiences under the situations with and without our scheme. With more requests, a passenger needs to wait for a longer time in general. This makes sense since the generation and the verification of signatures by both the trusted server and the taxis‟ OBUs take a certain amount of time.Due to the security measures, more data needs to be transmitted per request. The total amount of data to be transmitted per request is shown in Figure 4. Interestingly the data per request decreases when there are more requests. This is because when the number of requests is small, the number of replies per request is higher as there are more empty taxis and more taxis will reply for each request. Thus, the amount of data transmitted per request is more. On the contrary, when the number of requests is large, the number of available taxis is lower and so there are fewer replies to each request.The corresponding amount of data required to be transmitted per request is shown in Figure 5. With more taxis, there are more data needs to be transmitted per request due to the fact that more acceptance messages will be sent to the trusted server for a single request.





IV. CONCLUSION

We proposed a scheme to provide a secure taxi service. We introduced several new security features to reduce the risk of taxi crimes and to preserve the privacy of taxi passengers.Current proposals mostly focus on entity based authorization. Frame-work of vehicular ad hoc network (VANET) is utilized to provide a secure and privacy based taxi service. V2V communication is not focused. If this exists, it will reduce the delay even with the security measures. For simulating this in the NS-2 platform a new clustering based concept with the routing protocol has been addressed in the future work.Using the analysis and results obtained in this work, we have come to the certainty that existing network solutions cannot be readily applied to VANETs, given the radically different nature of this new type of networks. A good example is that of authentication mechanisms, where digital signatures showed to be the most suitable approach despite high overhead. In this work we have investigated the feasibility of V2R communications. In the future work jointly V2V communication jointly with several attacks has been explained.

REFERENCES

[1] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, “An Efficient Identitybased Batch Verification Scheme for Vehicular Sensor Networks,” in *Proceedings of the IEEE INFOCOM ’08*, Apr. 2008, pp. 816 – 824.

[2] C. Zhang, X. Lin, R. Lu, and P. H. Ho, “RAISE: An Efficient RSUaided Message Authentication Scheme in Vehicular Communication Networks,” in *Proceedings of the IEEE ICC ’08*, May 2008, pp. 1451 – 1457.

[3] P. P. Tsang and S. W. Smith, “PPAA: Peer-to-Peer Anonymous Authentication,” in *Proceedings of ACNS ’08*, 2008, pp. 55 – 74.

[4] R. Housley, W. Ford, W. Polk, and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” *IETF RFC2459*, 1999.

[5] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (1), 2007 39–68.

[6] J. Freudiger, M. Raya, M. Feleghhazi, Mix zones for location privacy in vehicular networks, in Processings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS‟07), Vancouver, Canada, August 14, 2007.

[7] H. Wen, P.H. Ho, G. Gong, A novel framework for message authentication in vehicular communication network, in: Proceedings of the IEEE GLOBECOM‟09, December 2009,pp. 1–6.

[8] A. Wasef, X. Shen, MAAC: message authentication acceleration protocol for vehicular ad hoc networks, in: Proceedings of the IEEE GLOBECOM‟09, December 2009, pp. 1–6.

[9] X. Sun, X. Lin, P.-H. Ho, Secure vehicular communications based on group signature and ID-based signature scheme, in: Proceedings of International Conference on Communications (ICC‟07), Scotland, June, 2007.

[10] B.K. Chaurasia, S. Verma, S.M. Bhasker, Message broadcast in VANETs using group signature, in: Proceedings of the IEEE WCSN‟09, December 2008, pp. 131–136.

[11] Y. Hao, Y. Cheng, K. Ren, Distributed key management with protection against RSU compromise in group signature based VANETs, in: Proceedings of the IEEE GLOBECOM‟08, December 2008, pp. 1–5.

[12] A. Studer, E. Shi, F. Bai, A. Perrig, TACKing together efficient authentication, revocation, and privacy in VANETs, in: Proceedings of the IEEE SECON‟09, June 2009, pp. 1–9

[13] A. Wasef, X. Shen, PPGCV: privacy preserving group communications protocol for vehicular ad hoc networks, in: IEEE Proceedings of the ICC‟08, May 2008, pp. 1458–1463.

[14] M. Verma, D. Huang, SeGCom: secure group communication in VANETs, in: IEEE Proceedings of the CCNC‟09, January 2009, pp. 1–5

[15] T.W. Chim, S.M. Yiu, L.C.K. Hui, V.O.K Li, SPECS: Secure and Privacy Enhancing Communications for VANET, 2009, manuscript.

[16] T.W. Chim, S.M. Yiu, L.C.K. Hui, V.O.K Li, DRS: Dynamic, Reliable and Secure Group Communications Schemes for Vehicular Sensor Networks, 2009, HKU Technical Report No. TR-2009-06.

[17] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, Overhaul of IEEE 802.11 Modeling and Simulation in ns-2, in Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems, ser. MSWiM ‟07. New York, NY, USA: ACM, 2007, pp. 159–168.