Infrastructure based Authentication in VANETs

Brijesh Kumar Chaurasia[1] and Shekhar Verma[2]
[1,2]*Indian Institute of Information Technology, Allahabad, India*
bkchaurasia@iiita.ac.in[1], sverma@iiita.ac.in[2]

Abstract

In a vehicular ad-hoc networks (VANETs), the veracity of a message requires authentication of the source vehicle. In this work, a technique for mutual authentication of a vehicle and road side unit (RSU) that preserves the privacy of the vehicle is proposed. The technique relies on the traffic authorities and assumes a hierarchical structure comprising a central trusted authority (TA) with state level trusted authorities (STA) and city level trusted authorities (CTA). Vehicles and RSU have public - private key pairs and each vehicle- CTA and RSU – CTA share a symmetric key. An RSU can be malicious and a vehicle can be malicious and a vehicle can communicate with a CTA only via an RSU and vice-versa. This requires message exchange in the RSU mediated communication between vehicles and CTAs to be confidential. The process is bandwidth efficient and needs only one request-reply message pair between vehicle and the (RSU- CTA-STA-TA) infrastructure. The time taken is in the order of milliseconds which constitutes only a small portion of the stay time of a vehicle within an RSU region.

Keywords: *Mutual authentication, public-private key, VANETs, Vehicles, Road Side Units.*

1. Introduction

VANETs is a network of vehicles and infrastructure points. In VANETs, infrastructure points are referred as road side units (RSUs). RSUs are placed at certain distance on the road, similar to an access point in traditional wireless ad hoc networks to provide necessary infrastructure support for network setup and communications. The network membership is very volatile with members joining / leaving a neighborhood as they move on the road. Vehicles are equipped with an On Board Unit (OBU) that has an event data recorder (EDR), global positioning system (GPS), forward and backward radar, computing facility, and short range wireless interface [1]. A bandwidth of 75 MHz has been allocated in the 5.850-5.925 GHz band [2]. Each vehicle periodically broadcast information. DSRC identifies five basic classes of applications: public safety application, traffic management, traveler information, freight/cargo transport, and transit. The distance between two RSUs is planned to be are 2-3 km. and a vehicle traveling at 20 ms^{-1} would traverse this distance in about 4-5 minutes. On an average, there are 50-100 vehicles in an RSU area. This requires an authentication message every few milliseconds. The size of authentication messages should be small and the process must consume little time to given enough bandwidth and time for useful communication. In this work, the communication overhead is reduced by employing a single request-reply message exchange between a vehicle and the RSU for authentication. The computation load of the RSU is also reduced by transferring the verification task to the CTA and other authorities. This reduces the authentication overheads.

The rest of the paper is organized as follows. Section 2 describes the related work and problem formulated in section 3. In section 4, the architecture of VANETs is described. The protocol description is given in section 5. The scheme is evaluated through simulation and results are in section 6, section 7 concludes the work.

2. Related work

There are several studies available for authentication mobile networks. In SRAAC protocol [3] anonymous message authentication is done using blinded certificate to achieve the anonymity, revocation and isolation of misbehaving vehicles. SRAAC makes use of a digital signature algorithm called magic Ink-DSS with shared secrets. However, revocation is not done in real time because its certificates (previously stored in their *OBU*) will be valid for some arbitrary time window. The authentication scheme in [4] between vehicles and *RSUs* use pseudonyms and MAC (Message Authentication Code) chain for traceability and privacy. However, this scheme does not address the problem of malicious *RSU*. A highway specific mechanism for access control using the Kerberos model is described in [5]. In this scheme, vehicles use tokens to authenticate from the highways entry points. A privacy preserving authentication protocol in which no central authority can be trusted is given in [6]. The scheme uses a random key-set for anonymously authenticating vehicles. The keys are shared between different random sets to achieve anonymity and further enhanced by using independent keys for authentications at neighboring *RSUs*. The privacy preserving schemes is in [7], [8], [9] use pseudonyms. The pseudonym may be generated by the fixed infrastructure [8] or by the vehicle itself. In [9], vehicle stores anonymous temporary public keys certified by a central authority. To achieve the anonymity vehicle can also switched pseudonym periodically, basis on the nature of the crowed [10]. This scheme also allows traceability along with privacy. In [11], [12], [13] PKI is deployed, where a large number of short-lived anonymous credentials is installed in the OBU that are used as the private key for signing the messages. Verification is through the public key. However, detection of malicious sender is difficult and the security overhead is usually bigger than the useful message contents. The scheme in [14] uses the short certificate based on temporary anonymous certified keys and uses group signature for tracing and revocation. A regional authority distributes certificates and certifies temporary key [15] created by vehicles for authentication. Group based schemes [16], [17], [18], [19] provide anonymity as a receiver cannot distinguish a member from its group. Group based schemes achieve both privacy and authentication. However, group formation, maintenance, revocation need to be further studied [20]. To reduce the size of certificate revocation list and avoid the overheads of PKI, identity based with group signature scheme is proposed. The ID-based cryptosystem simplifies the certificate management process. The ID-based cryptosystem avoids certificate exchange and storage overheads of previous proposed schemes. However, their framework is limited by the strong dependence on the infrastructure for short lived pseudonym generation. This requires large signaling overhead. Timed efficient and Secure Vehicular Communication scheme proposed in [21] needs to perform symmetric MAC operation instead of any asymmetric operation at the verifier vehicle. Verification time is reduced but tight time synchronization between vehicles is needed. An efficient rsu-aided message authentication scheme in vehicular communication networks (RAISE) [22] is responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. The proposed scheme has less computation and communication overhead as compared to PKI-based and the group signature based schemes. However, this scheme is highly dependent on *RSUs*.

3. Problem Definition

In a VANET, vehicles in an RSU region form a neighborhood. The limited communication range of an RSU limits the size of this neighborhood. Since the vehicles move at high speed along strait jacketed lanes in same and opposite directions, members continuously join and leave this neighborhood in batches at regular short intervals. When such a batch of vehicles enters into an RSU region, they need to authenticate themselves and the RSU. All these vehicles request for authentication almost at the same time. This may result in contention delay over the shared wireless channel and queuing delay at the RSU. These necessitate that authentication messages occupy minimum bandwidth and require minimum computational capacity at the RSU. Moreover, the stay time of a vehicle in an RSU region is in the order of minutes. This requires that the authentication time should be very small. This is possible only when there are minimum number of message exchanges between an RSU and vehicles and message size of both request and reply should be small.

In a VANET, RSUs need to be deployed in large numbers. The low cost requirement for RSU manufacturing makes the construction of fake RSUs feasible. Thus RSUs must also be authenticated. Since a vehicle would participate in a VANET only if its privacy is guaranteed; authentication process should preserve the privacy of the vehicle. At the time of authentication, identities of claimant vehicle must be hidden from the RSU. On the other hand, the authority should be able to trace the claimant vehicle or sender of a message by revealing its identity when required. Thus, this privacy must be conditional.

4. VANET Architecture

The VANET architecture for the proposed mutual authentication process is shown in Figure 1. It consists of central trusted authority (TA) at the root, state level trusted authorities (STA), a group of city level trusted authorities (CTA) are under every STA. Under every CTA there are multiple RSUs and vehicles moving on a road. Every vehicle is equipped with an OBU that has an ability to communicate and compute. Since the transmission range of any vehicle is more than the total width of the road, position of a vehicle has no effect on communication. An OBU/RSU is equipped with private key / public key and a shared key which are provided by its immediate higher authority. TA distributes keys and certificate to STAs.

An STA plays the role of key distributor for CTA and similarly CTA distributes the key and short certificates to OBU/RSUs. Each vehicle has tamper proof device to store different keys. A vehicle will receive a short certificate at the time of authentication by CTA via the corresponding RSU for inter-vehicle communication. 3-5 RSUs under a CTA are grouped together such that their ids have a common two bit prefix as group identifier. The groups overlap and an RSU may be a part of more than one group as shown in Figure 2.

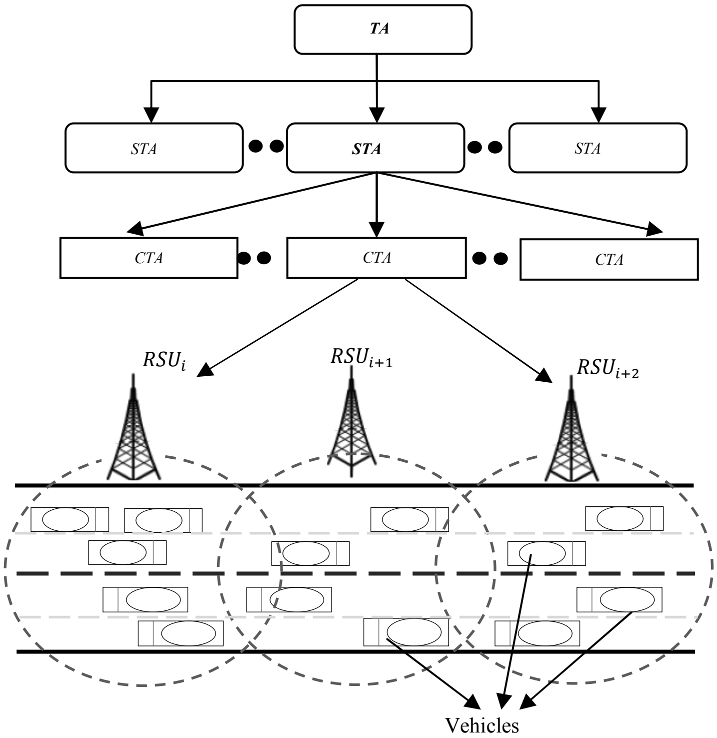

Figure 1. Architecture of VANETs

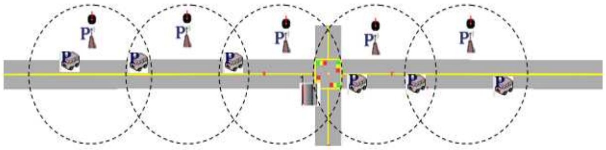

Figure 2. RSUs Grouping

5. Protocol Description

An RSU continuously broadcasts its identity ID_{RSU} and public key in its area. As a vehicle enters the area of a different RSU, it receives RSU broadcast and determines that needs to associate itself and initiate mutual authentication process. The vehicle first encrypts the ID_{RSU}, its ID_v, and current timestamp t_0 using its CTS shared key K_{CTA}. These encrypted bits are again encrypted along with its pseudonym and t_0 by the public key $PK^{+}_{RSU_i}$. This is sent to the RSU. The RSU forwards the encrypted part to the CTA. CTA authenticates the vehicle and the RSU and sends its authentication details report to the RSU by encrypting the authentication information of the RSU with the vehicle shared key and that of the vehicle to the RSU. RSU confirms the authentication of the vehicle and forwards the encrypted part of the report to vehicle for RSU authentication. The CTA also sends a temporary short certificate for inter-vehicle communication. CTA informs about authentication of vehicle to group of $RSUs$ in the transmission range at the same time. This scheme achieve the authentication of vehicle for long time as well as vehicle is also able to mutually authenticate to group of $RSUs$ within transmission range with the help of group public key of RSU. The whole process needs only one request and reply between vehicle and infrastructure. The acronym of variable is given in table I.

The proposed authentication scheme is divided in four phases. The descriptions of phases are as follows:
Phase I: Vehicle sends the request for association and authentication to RSU, phase II: The RSU forwards vehicle's authentication request to CTA, and Phase III: CTA sends the authenticated short certificate to group of RSUs in the transmission range; phase IV: RSU sends the response to vehicle.

Table 1 NOTATION USED FOR THIS ALGORITHM

Notation	Description
v_i	i^{th} Vehicle
TA	Trusted authority (National)
STA	Trusted authority (State)
RSU_i	i^{th} Road Side Infrastructure / Unit
CTA	Trusted authority (City)
PK_e^+	The Public key of any entity in vehicular network. Entity can be a vehicles / RSU_i / CTA etc.
$PK_{RSU_i}^+$	The Public key of i^{th} RSU_i
PK_v^+	The Private key of i^{th} v_i
$PK_{RSU_i}^-$	The Private key of i^{th} RSU_i
PK_v^-	The Private key of i^{th} v_i
PE_{8SU_i}	A public-key encryption function using the i^{th} RSU_i's public key
DE_{RSU_i}	A public-key decryption function using the i^{th} RSU_i's public key
K_{CTA}	The securely pre-shared symmetric key with CTA and vehicle
ID_v	Unique identity of vehicle, issued by CTA
ID_{RSU}	Unique identity of i^{th} road side infrastructure, issued by CTA
Sig_{CTA}	Signature of CTA
CTS	Shared Key

Phase I: $v \rightarrow RSU_i$
Vehicle sends the request for association and authentication to RSU.

Step1. At the time of vehicle enters in the communication range of RSU, it receives RSU ID_{RSU} and $PK_{RSU_i}^+$for sending authentication request.
Step2: Vehicle takes it's identity, and current time stamp t_0.
Step3: Computes a MAC value.

$$ps_0 = h(ID_v, t_0)$$

t_0 is the 4 byte field time stamp for freshness to prevent message by replay attack / Sybil attack.
Step 4: Vehicle sends the authentication request to i^{th} RSU_i .

First, current timestamp, vehicle identity and *RSU* identity are encrypted by the vehicle's private key.
All values is again encrypted by public identity of ID_{RSU}.

$$v_i \rightarrow RSU_i: PE_{SD_{RSU}}\{PE_{K_{CTA}}(ID_v, t_0, ID_{RSU_i}), ps_0, t_0\}$$

Encryption technique is used to provide confidentiality.

Phase II: RSU forwards vehicle's authentication request to CTA.

Step 1: i^{th} RSU_i decrypt received association and authentication request and store ps_0, for the time duration until the CTA does not send the response to the RSU.
Step 2: i^{th} RSU_i will forward the encrypted packet to CTA .

$$RSU_i \rightarrow CTA: \{PE_{K_{CTA}}(ID_v, t_0, ID_{RSU_i})\}$$

Step 3: CTA decrypts the authentication request by its shared key and verifies the vehicle and RSU_i.

Phase III: CTA sends the authentication report and a short certificate to group of $RSUs$ $(RSU_{i..n})$.

Step1: After completion of the authentication process of vehicle and i^{th} RSU_i, CTA will issue the short certificate with time to live (t_1) time stamp to vehicle via i^{th} RSU_i.

$$CTA \rightarrow RSU_i: \{PE_{K_{CTA}}(GID_{RSU}, cert[Sig_{CTA}, t_1])\}$$

The certificate is valid for a time period determined by the approximate duration of stay of a typical vehicle in an *RSU* group moving at normal speed. Thus, different vehicles will be issued certificates with different validity period depending on their estimated stay time with the group.
Step2: At the same time CTA will also inform all the $RSUs$ of the group $RSU_{i..n}$.

$$CTA \rightarrow RSU_{i..n}: PE_{ID_{RSU}}[PE_{K_{CTA}}(GID_{RSU}, cert[Sig_{CTA}, t_1], ID_v), ps_0]$$

Thus, all the $RSUs$ in the vicinity know in advance of the authentication of the requesting vehicle. RSU_i will match the computed MAC value by CTA ps_0. If this is same as previous stored value then vehicle will authenticate to RSU_i.

Phase IV: i^{th} RSU_i sends the authentication report to the vehicle.
Step1: $RSU_i \rightarrow v$:

$$\{PE_{K_{CTA}}(ID_{RSU}, cert[Sig_{CTA}, t_1], ID_v)\}$$

Vehicle receives the authentication certificate and at the same time vehicle will authenticate the group $RSU_{i..n}$.

Re-authentication

Case 1: Same Group

When the vehicle enters the area of $(i+1)^{th}RSU$ of the same group, it sends an association request by encrypting its identity ID_v, $cert[Sig_{CTA}, t_1]$ by $PK^{+}_{RSU_{i+1}}$

$$v_i \rightarrow RSU_{i+1}: PE_{ID_{RSU_{i+1}}}\{PE_{K_{CTA}}(ID_v, t_0, ID_{RSU_{i+1}}), ps_0, t_0\}$$

This authentication is valid for certificate time period t_1 . When the vehicle is in the area of an intersection of RSU, its association request is forwarded to the *CTA*, which extends the time of the certificate.

Case 2: Different Group

In case, the vehicle enters a different group or the certificate expires, the vehicle has to re-authenticate itself through the four phase mutual authentication process.

6. Simulation and Results

6.1. Simulation Setup

In this section, the efficiency of the proposed technique for mutual authentication is verified through simulation using NCTUns [23]. The setup is shown in Figure 3. The other simulation parameters are shown in Table II. The communication delay is estimated by running the simulation experiment for different density of vehicles (5-40) [25] and by varying the speed (10- 30 ms^{-1}) and acceleration (3 ms^{-2}) of the vehicles. The major source for computation delay is the time taken by cryptographic techniques. These were measured using MIRACL [24]. A program containing computation time of standard hash function and encryption/decryption algorithm was run. The computation platform was a desktop (CPU speed - 2.50 GHz, RAM - 2 GB RAM).

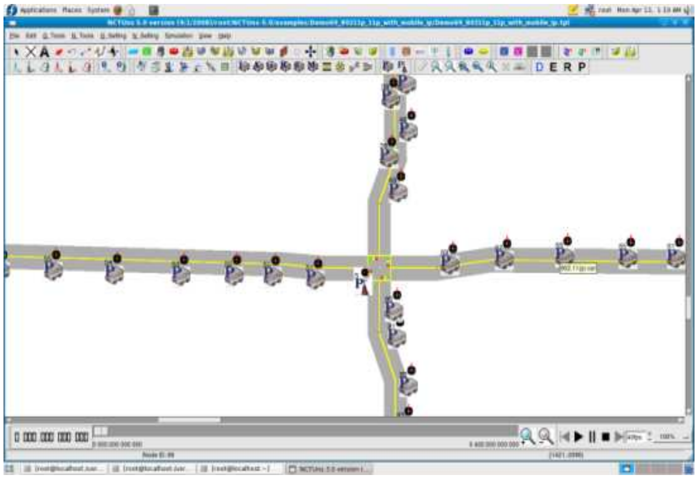

Figure 3. Simulation Setup in NCTUNs

We considered two different packet lengths in authentication scheme. First, when vehicle transmits to RSU (packet structure shown in Figure 4a) and when RSU responds to vehicle (packet structure shown in Figure 4b). Lengths of packets are 108 bytes and 148 bytes respectively.

Type ID	Message ID	Payload	Time Stamp
2 byte	2 byte	100 byte	4 byte

Figure 4a. Packet structure from *OBU* to *RSU*

Type ID	Message ID	Payload	Time Stamp	Signature
2 byte	2 byte	100 byte	4 byte	40 byte

Figure 4b. Packet structure from RSU to OBU

6.2. Results

Data packets were generated at a constant bit rate at *RSU* and the vehicle. Figure 5a and Figure 5b show the average and maximum delay when number of vehicles in the *RSU* region varies from 5-40 [15], [25]. The speed of vehicles was varied between 10- 30 ms^{-1} with acceleration / deceleration = 3 ms^{-2} (Table II).

Table 2 Simulation Parameters

Simulation Parameters	**Values of simulation parameters**
Speed of Vehicles	10-30 ms^{-1}
Acceleration /Deceleration	3 ms^{-2}
Number of Vehicles	5-40
Range of communication	250-300 m
Data rate	6 Mbps
Communication protocol	802.11p

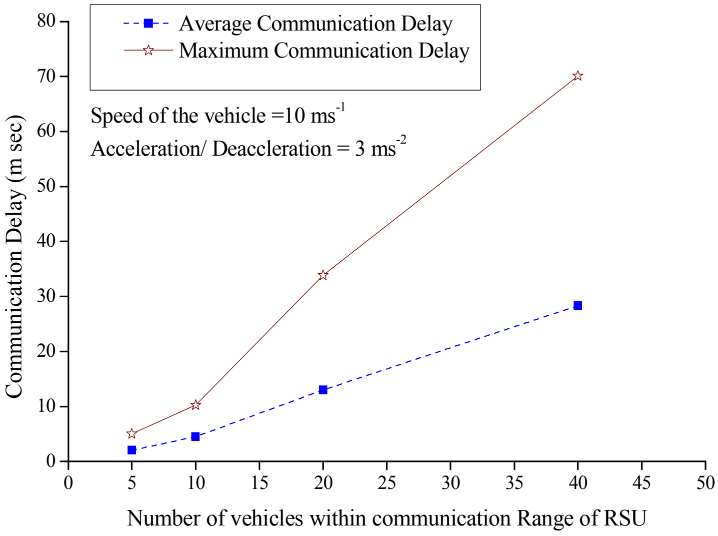

Figure 5a. Average and Maximum communication delay at speed of source vehicle 10ms^{-1}

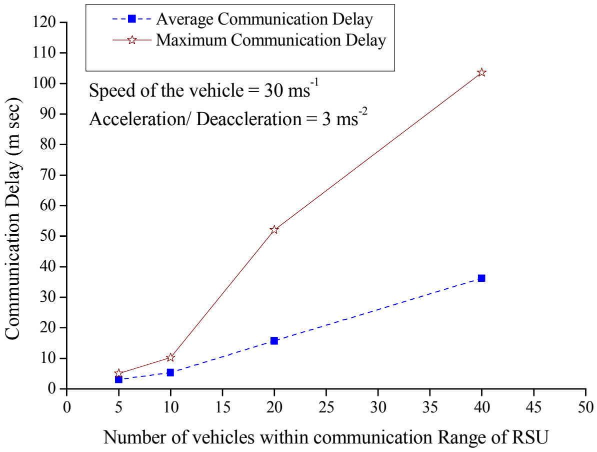

Figure 5b. Average and Maximum communication delay at speed of source vehicle 30ms^{-1}

The usefulness of the authentication technique can be estimated by the average time taken for the process to complete. The authentication process requires a pair of request and reply message. After a vehicle receives the *RSU* broadcast, each step of the process takes time. The total time can be divided into computational delay at the vehicle, *RSU* and *CTA* and the communication delay over the channel. The computational delay in the forward process consists of delay in packet formation at the vehicle, decryption and encryption delay at *RSU*, verification and processing time at the *CTA*. The delay in the reverse process is the packet formation at the *CTA*, decryption and packet formation at *RSU* and finally decryption of the packet at the vehicle. The communication delay is the contention and propagation delay for transmission over the shared wireless channel.

6.2.1. Communication delay: The communication delay in each step was estimated by determining the delay in each step of the process.

Communication delay in phase I, is t_1. Vehicle sends the authentication request packet to the RSU. Maximum value of t_1 is 70.4882 ms. and 104.0115 ms. when vehicles have acceleration / deceleration of 3 ms^{-2} and speed of 10 ms^{-1} and 30 ms^{-1} respectively and vehicle density (5-40). Similarly when RSU communicates with vehicles then communication delay in phase IV is near about to same in phase I.

6.2.2. Computational delay: The computational delay in each step was estimated by determining the delay in each step of the process.

i. t_2 is the computational delay in phase I, Average delay of hash function (SHA-1) after multiple simulations is 0.88 ms. Vehicle encrypts the authentication request two times with public key of RSU and shared key of RSU. After encryption authentication request and its identity with time stamp vehicle sends to the *RSU*. At last, vehicle will decrypt that authentication response received by the *RSU* in phase IV. So computational delay of vehicle t_2 is 5.86 ms.

ii. Computational delay in phase II is t_3. *RSU* also two times decrypt the received authentication request. When request received from vehicle and authentication response from *CTA*. So computational delay at *RSU* t_3 is 3.32 ms.

iii. In phase IV, computation delay is t_4. In this phase, *CTA* will verify the identities of *RSU* and vehicle at the same time. *CTA* also signed that packet, after that forward this authentication request to vehicle through adjacent *RSU*. So computational delay at *CTA* t_4 is 4.30 ms. (signing delay, verifying delay, encryption/decryption delay). Total time taken in authentication process is $T = t_1 + t_2 + t_3 + t_4$.

Total delay for authentication process is T shown in Figure 6a and Figure 6b. In Figure 6a and Figure 6b shown total maximum and average delay of the authentication process when number of vehicles varies 10 to 40 and speeds of vehicle is 10 ms^{-1} , and 30 ms^{-1} respectively with acceleration / deceleration taken as 3 ms^{-2}.

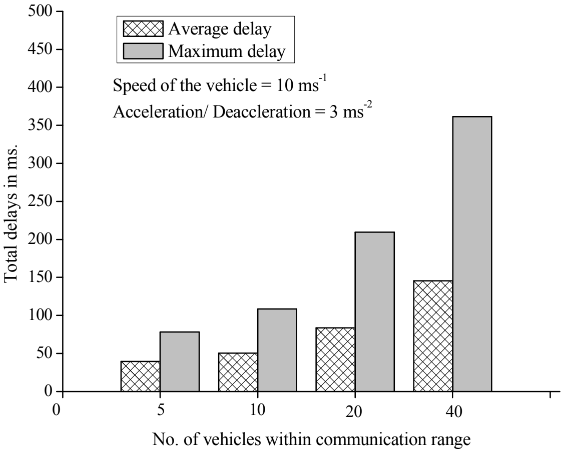

Figure 6a. Average and maximum delay at speed of source vehicle 10ms^{-1}

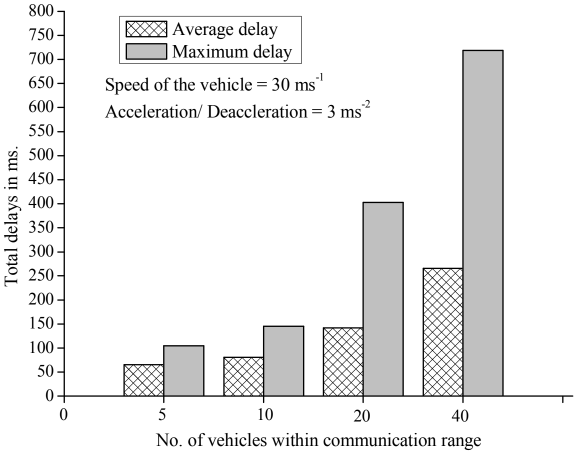

Figure 6b. Average and maximum delay at speed of source vehicle 30ms^{-1}

6.2.3. Certificate Validity: Intuitively, a certificate should be valid for time period greater than the possible stay duration of the slowest vehicle to lessen the communication load due to re-authentication requests over the channel. However, storage of certificates of vehicles that are not in the area would constitute a large memory overhead. If certificates are stored according to the largest possible stay period of a vehicle, then at a given time, the number of certificates would be very large.

A quantitative measure can be obtained as follows. The stay duration of vehicles was estimated in NCTUns for a two lane highway. Vehicles travelling with different speeds (5-20 ms^{-1}) for different vehicle densities ranging from low density (single vehicle), medium density (100 vehicles) and high density (150 vehicles) were considered. The average stay duration was calculated for different conditions and tabulated in Table III.

Table 3 STAY DURATION OF VEHICLES

Speed of Vehicles (m/s)	Time taken For passing Group of RSU (min.)		
	Normal Density	Medium Density	High Density
5	18.7	20.3	25.7
10	10.6	14.9	16.1
20	6.3	9.0	9.8

As can be observed, the minimum stay duration of approximately 6 $minutes$ corresponds to a single vehicle travelling at $20\,ms^{-1}$ and the maximum stay duration is around $26\,minutes$ for slowest vehicle ($5ms^{-1}$) travelling in almost congested road conditions. Very high validity duration (30 $minute$) for lowest stay period (fastest vehicles ~ $20\,ms^{-1}$) in low density traffic state would require storage of almost 750 certificates for around 30 $minutes$ by RSU, whereas it should ideally hold only *150* certificates. This is a large storage overhead. Searching this certificate pool will also take substantial time. At the other extreme, a certificate validity period of 6 $minutes$ for the slowest vehicle in highest traffic density environment would require almost 5 additional re-authentication requests with a huge increase message flow between vehicle, RSU and CTA.

These entail a tradeoff between re-authentication message overhead and certificate storage and search overheads. An optimal certificate validity period should minimize both. This can be achieved by issuing certificates with different validity periods. It can be observed from Table III that the stay period is characterized by the speed (a function of lane) and the traffic density. Hence, certificate validity is assigned in accordance to the initial speed/lane of a vehicle and the general traffic state. For a three RSU group, it would typically range from $10 - 25\,minutes$.

7. Conclusion

In this paper, a mutual authentication technique for RSU and vehicle is proposed. The scheme preserves the privacy of the vehicle. The RSU is used as a mediator for authentication of both the RSU and the requesting vehicle. Since the CTA is responsible for verifying credentials, the load of the RSU is drastically reduced. The technique has only one request reply message exchange. This reduces the bandwidth requirement and the total communication delay in the authentication process. However, many vehicles enter an *RSU* region together and request may cause substantial communication delay. Moreover, all the *RSU* are in continuous communication with a *CTA*, which may constitute a large overhead as a large number of messages flow between *RSUs* and a *CTA*. Authentication of neighboring *RSUs* can reduce this message flow. However this would increase the certificate storage requirements at the *RSUs* inordinately. Message flow and storage can be simultaneously reduced by issuing certificates with different validity periods in accordance to vehicle's speed and current traffic state.

References

[1] V. Casola, J. Luna, A. Mazzeo, M. Medina, M. Rak, and J. Serna, "An Interoperability System for Authentication and Authorization in VANETs," In International Journal of Autonomous and Adaptive Communications Systems , vol. 3, no. 2, 2010, pp. 115 – 135.

[2] D. Jiang, and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," In IEEE Vehicular Technology Conference. VTC Spring-08 , 2008, pp. 2036-2040.

[3] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (sraac)," In the 4th Workshop on Embedded Security in Cars (ESCAR - 06), 2006.

[4] S. H. Kim, B. H. Kim, Y. K. Kim, and D. H. Lee, "Auditable and Privacy-Preserving Authentication in Vehicular Networks," In the Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies , 2008, pp. 19-24.

[5] H. Moustafa, G. Bourdon, and Y. Gourhant, "Providing authentication and access control in vehicular network environment," In SEC. IFIP (Springer) , vol. 201, 2006 ,pp. 62-73.

[6] Y. Xi, K. Sha, W. Shi, and L. Schwiebert, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," In 8th symposium on Autonomous Decentralized Systems, ISADS , pp. 344-351, 2007.

[7] Brijesh Kumar Chaurasia, Dr. Shekhar Verma, and Dr. G. S. Tomar, "Mechanism for Privacy Preservation in VANETs," *In the International Journal of Grid and High Performance Computing (IJGHPC), Special Issue on: Grid computing and Security*, vol. 2, no 2, 2010, 12-22.

[8] F. Dotzer, "Privacy Issues in Vehicular Ad Hoc Networks", *Workshop on Privacy Enhancing Technologies*, Dubrovnik (Cavtat), Croatia, 2005, pp. 197-209.

[9] M. Gerlach and F. Guttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real", In Proceedings of 65th Vehicular Technology Conference VTC2007-Spring, Dublin, Ireland, April 2007, pp. 2521-2525.

[10] B. K. Chaurasia, and S. Verma, "Maximising Anonymity of a Vehicle", International Journal of Autonomous and AdaptiveCommunications Systems (IJAACS), Special Issue on: "Security, Trust, and Privacy in DTN and Vehicular Communications," vol. 3, no. 2, 2010, pp. 198-216.

[11] M. Raya and J. P. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, Special Issue on Security, Ad Hoc and Sensor Networks, vol. 15, no. 1, 2007, pp. 39–68.

[12] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles", IEEE Security & Privacy magazine, vol. 2, no.3, 2004, pp.49–55.

[13] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 2005, pp. 11-21.

[14] A. Studer, Elaine Shi, Fan Bai, and Adrian Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," IEEE SECON 2009, Rom, Italy, 2009, pp. 1-9.

[15] P. Golle, D. Greene and J. Staddon, "Detecting and correcting malicious data in VANETs," In Proceedings of VANET'04, 2004, pp. 29–37.

[16] K. Sampigethaya, M. Li, L. Huang, R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE JSAC, vol. 25, no. 8, Oct. 2007, pp.1569-89.

[17] B. K. Chaurasia, S. Verma, and S. M. Bhasker, "Message broadcast in VANETs using Group Signature", Fourth International Conference on Wireless Communication and Sensor Networks, India, 2008, pp. 131-136.

[18] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," In Proceedings of the Workshop on Vehicular Ad Hoc Networks (VANET), 2007, pp. 19-28.

[19] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," In IEEE 27th conference on computer communication INFOCOM, 2008, pp. 1229-1237.

[20] Mayank Verma and Dijiang Huang, "SeGCom: Secure Group Communication in VANETs" In 6th IEEE Consumer Communications and Networking Conference, CCNC-09, Feb. 2009, pp. 1-5.

[21] X. Lin, X. Sun, X. Wang, C. Zhang, Pin-Han Ho, X. Shen, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving," IEEE Trans. on Wireless Communications, vol. 7, no. 12, 2009, pp. 4987-4998.

[22] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient rsu-aided message authentication scheme in vehicular communication networks", In Proc. IEEE ICC- 08, Beijing, China, May 19-23, 2008.

[23] Available at: http://nsl.csie.nctu.edu.tw/nctuns.html.

[24] Shamus Software Ltd. MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library. Available at: http://indigo.ie/~mscott.

[25] Dedicated Short Range Communications (DSRC), Last accessed: January-05 2011, http://www.leearmstrong.com/DSRC/DSRCHomeset.htm.

Authors

Brijesh Kumar Chaurasia is pursuing Ph.D. from Indian Institute of Information Technology, Allahabad, India in Information Technology. He received his M. Tech. Computer Science from D.A.V.V., Indore, India. His research interest areas are Security in Wireless Ad-hoc Networks and Wireless Sensor Networks. (bkchaurasia.itm@.gmail.com)

Shekhar Verma received his Ph.D. degree from IT, BHU, Varanasi, India in Computer Networks. He is Associate Professor at Indian Institute of Information Technology, Allahabad, India. His research interest areas Computer Networks, Wireless Networks and Communication, Wireless Sensor Networks, Information and Networks Security.