Infrastructure Aided Privacy Preserving-Authentication in VANETs

Brijesh Kumar Chaurasia[1], Shekhar Verma[1], and G.S. Tomar[2]

[1] Indian Institute of Information Technology, Allahabad, India
{bkchaurasia,sverma}@iiita.ac.in
[2] Malwa Institute of Technology and Management, Gwalior, India
gstomar@ieee.org

Abstract. The paper presents a privacy preserving authentication protocol for vehicles in a VANET. The authentication process involves authentication of the vehicle and the corresponding RSU by a fixed infrastructure (CTA). Every RSU has a public key infrastructure and continuously broadcasts public key. The vehicle encrypts its identity, RSU Id and timestamp using its symmetric key. The encrypted bits along with the pseudonym of vehicle and timestamp are again encrypted by the public key of RSU and send to the RSU. RSU forwards the encrypted part to the CTA. CTA sends its verification to the RSU. The verification of the vehicle is encrypted by the vehicle symmetric key and sends along with authentication of the vehicle to the RSU. The encrypted portion is forwarded to the vehicle which confirms the authentication of the RSU after decryption. The CTA also sends a temporary short certificate to the vehicle for vehicle to vehicle communication. The whole process needs only one request and reply between different entities. Simulation results indicate the time taken ($\sim 223\ ms$) for the whole process is small and 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 are moving on the road exchanging information. 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 and vehicles use dedicated short range communications (DSRC) protocol for communication [2]. According to DSRC, each vehicle periodically broadcast information. DSRC classifies the five basic classes of applications; public safety application, traffic management, traveler information, freight/cargo transport, and transit. Messages class can be divided in two categories; safety and non-safety categories. The entails that (a vehicle) the source of message be authenticated beforehand joining the networks. Since

T.-h. Kim et al. (Eds.): FGIT 2010, LNCS 6485, pp. 74–84, 2010.

message can cause / prevent life endangering situations, the variety of a message must be ascertained before an action is taken. In life threatening situations, the time for message authentication is almost negligible. Moreover, a malicious vehicle can broadcast with different identities. In vehicular network, DSRC [2], recommends the range of communication of vehicle is 500 meters and 1000 meters for road side infrastructure, a vehicle sends each message within 100-300 milliseconds time interval. However, if 50-200 vehicles present in the communication of road side infrastructure then network is high density network and in this case receiver vehicle will needs to verify near about 500-2000 messages per second. So main issue of authentication protocol is low communication overhead and fast verification.

At the time of authentication, identities of claimant vehicle must be hidden from a verifier vehicle and 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, such as liability investigation etc. So privacy must be preserve and privacy should be conditional.

Privacy preserving authentication can be achieved by using pseudonyms that are intimately linked to the original identity [1]. The pseudonym may be generated by the fixed infrastructure [3], [4] or by the vehicle itself [5]. They may be presorted [1] or downloaded from a trusted site periodically [6], [7]. During communication, the pseudonyms are switched periodically [8], or when required [9], in a crowd or a maximizing zone [10].For entity authentication public key infrastructure (PKI) [11], [12], [13] is deployed, where a large number of short-lived anonymous credentials is installed in the OBU. One of them is randomly selected used as the private key for digitally signing the messages. Verification is through the public key. However, detection of malicious sender is difficult. The CA has to exhaustively search a very large credential database to find the identity the compromised vehicle. Moreover, the security overhead is usually bigger than the useful message contents. Authentication can be done between two parties through exchange of certificates. This scheme [14] uses the short certificate based on temporary anonymous certified keys (TACKs) and uses group signature for tracing and revocation. A regional authority distributes certificates and certifies temporary key created by vehicles for authentication. Vehicles download CRLs certification revocation list to find for revoked entities [15]. 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, which also renders the signaling overhead overwhelming. Timed efficient and Secure Vehicular Communication (TSVC) scheme [21] is also proposed for authentication. This scheme needs to perform symmetric MAC operation instead of any asymmetric operation at the verifier vehicle. Verification time is reduced but required tight time synchronization between vehicles. RAISE [22] is a RSU-aided scheme, responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. Where the message authentication code (MAC) can be used for inter vehicles authentication under the aid of

a RSUs. 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 depend upon road side infrastructure, communication will be effected due network jammed because VANET is highly densely deployed and frequently disconnected network.

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

2 Problem Definition

A malicious vehicle can be an outsider or may be previously good vehicle. This malicious vehicle may inject false messages with different identities with dire consequences. This necessitates that messages and vehicles both are to be authenticated. Message authentication process needs to be repeated for each new message. Vehicle authentication should be done at the time of message sending to the verifier. At the time of communication, mutual authentication should be done for vehicle and RSU. This authentication must preserve the privacy of the vehicle. However, this privacy must be conditional. The true identity of a vehicle must be revealed if required by law. Finally, since the lifetime of a vehicle with an RSU is small, the authentication time should be almost negligible.

3 Architecture of VANETs

The architecture of a VANET is shown in Figure 1. It consists of national trusted authority ($\boldsymbol{TA}$), under this authority there are state level trusted authorities ($\boldsymbol{STA}$), city level trusted authorities ($\boldsymbol{CTA}$) are under in $\boldsymbol{STA}$. In every $\boldsymbol{CTA}$ there are many road side infrastructures ($\boldsymbol{RSUs}$) and there are vehicles moving on a road with an $\boldsymbol{RSU}$, they lateral motion is very restricted and the motion is unidirectional except at the junctions. A vehicle moving in a particular direction can move at different speeds and also pause. Vehicles can take velocity as variable or profile based etc & these vehicles may overtake one another. Since the transmission range of any vehicle is more than the total width of the road, this lateral motion has no effect on communications and can therefore be neglected. An $\boldsymbol{OBU}$ /$\boldsymbol{RSU}$ is equipped with private key / public key which will provided by it's adjacent higher authority like $\boldsymbol{TA}$ distributes the keys and certificate to state level authorities. $\boldsymbol{STA}$ will play the role of key distributors to $\boldsymbol{CTA}$ and similarly $\boldsymbol{CTA}$ distributes the key and short certificates to road side infrastructures and vehicles. Each vehicle has equipped with storage area named as Tamper Proof Devices (TPD) to store different keys and for prevention and detection of tampering. A vehicle store many pseudonyms along with public / private key and short certificate which will be received at the time of authentication by $\boldsymbol{CTA}$ via the corresponding $\boldsymbol{RSU}$. When vehicle will come within the transmission range of a $\boldsymbol{RSU}$ it receives its public identity. All vehicles have used pseudonyms to preserve the privacy for vehicle during the broadcast. City level trusted authority ($\boldsymbol{CTA}$) plays the role as a key distributor. All vehicles register with $\boldsymbol{CTA}$ via any RSU or such as

police station, government office, petrol pumps, and service stations etc. It is given one secret key for signing the messages, one shared secret key for communication between vehicles to city level trusted authority via ***RSU***. The vehicle will receive a short certificate by ***CTA*** via any ***RSU*** during authentication process. This short certificate can be used to authenticate claimant vehicle to verifier entity of network when infrastructure is absent.

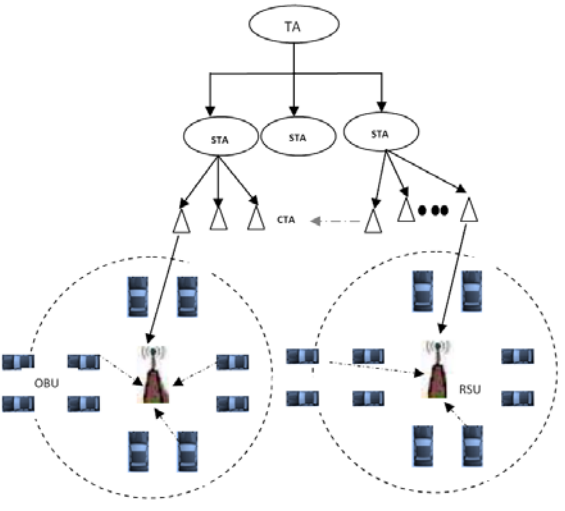

Fig. 1. Architecture of VANETs

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 or RSU_i 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_{RSU_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

4 Protocol Description

The proposed authentication scheme is divided in four phases. The first three phases achieves the authentication with privacy using hashing and pseudonyms. Confidentiality is achieved by encryption of public identities and is in the fourth phase traceability and revocation is achieved by the simple cooperative scheme wherever infrastructure is absent or present. The proposed authentication scheme is 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 vehicle via i^{th} RSU_i ; phase IV: Revocation.

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 selects a pseudonym from its storage pool, 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, timestamp, vehicle identity and RSU identity are encrypted by the vehicle's shared key. Second, all values is again encrypted by public identity of RSU.

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

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 .

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

Phase III: CTA sends the authenticated short certificate to vehicle via i^{th} RSU_i .
Step1: CTA decrypts the authentication request by its shared key and verifies the vehicle and RSU_i.
Step2: 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.

$$CTA \rightarrow RSU_i: PE_{ID_{RSU}}[PE_{K_{CTA}}(ID_{RSU}, cert[Sig_{CTA}, t_1], ID_v)\ ps_0]$$

RSU_i will match the MAC value obtained from CTA from it's previously stored MAC valued if this is same then vehicle authenticates to RSU_i.
The certificate is valid for a time period determined by the approximate duration of stay of a typical vehicle in an RSU.

Step3: i^{th} RSU_i sends the authentication report to the vehicle. $RSU_i \rightarrow v$:

$$RSU_i \rightarrow v:\left[PE_{K_{CTA}}(ID_{RSU}, cert[Sig_{CTA}, t_1], ID_v)\right]$$

Vehicle receives the authentication certificate and at the same time vehicle will authenticate the RSU.

Phase IV: Revocation
Vehicle found some conditions regarding RSU that are such as:
(i) RSU_i is malicious, (ii) RSU_i is switched off, (iii) Large congestion in the network- RSU_i is overloaded, hence delay occurred, and (iv) CTA founds RSU_i is malicious at the time of authentication process.

(i) If any vehicle found the identity of i^{th} RSU_i was not valid then vehicle can inform the CTA connected by next RSU_{i+1} or connected by next other trusted infrastructure. So that CTA will verify the authenticity of that RSU_i. If finds RSU_i is malicious then broadcast the alert messages about RSU_i.
(ii) This condition is very rare in VANETs. If vehicle found i^{th} RSU_i is switched off then vehicle will report to next adjacent RSU_{i+1}. This will verify, if found true then broadcast the i^{th} RSU condition and to inform the CTA.
(iii) In this condition vehicle will be send association & authentication request again and again and wait some more time for authentication, otherwise resend association & authentication request to the next RSU_{i+1}. Vehicle will use the old certificate until didn't get new certificate.
(iv) If CTA founds that RSU_i is malicious then it will send information to vehicle and inform the other network entities or broadcast alert messages regarding false identity of RSU_i and also will take action to remove from the VANETs. CTA will listed this malicious RSU_i in revocation list, which stored in CTA. The revocation list can be seen at time to time by the connected from any type of infrastructure in VANETs such as next RSU_{i+1}, police station, government office , service stations and petrol pump etc. So this scheme is also able detect the false identity of network entities.

5 Simulation and Result Setup

5.1 Setup

In this section, simulation is conducted to verify the efficiency of the proposed secure protocol for inter vehicular communication applications with NCTUns [23]. For cryptographic delay we install MIRACL [24] and its library. So for these cryptographic delays we run a program that contains computational time of all standard hash function and encryption / decryption algorithms. The hardware/processor/clock of the system over which we install MIRACL is given in Figure 2.

Intel (R) Core (TM) @ Quad CPU
1.99 GB RAM
Q9300 @ 2.50 GHz

Fig. 2. CPU configuration over which we install MIRACL

We consider two types of different length of packets for authentication scheme. First when vehicle communicates to road side infrastructure then structure is as shown in figure 3a and when road side infrastructure responds to vehicle then structure is as shown in figure 3b. Lengths of packets are 108 bytes and 148 bytes respectably.

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

Fig. 3a. Packet structure from RSU to OBU

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

Fig. 3b. Packet structure from OBU to RSU

In the simulation, speed of vehicle are (10-30 ms^{-1}), while communication range of VANET is 250-300 meters. Vehicle stays within transmission range of the *RSU* for a very short duration of time (approx. 10-20 sec.). In the proposed scheme there will be two types of delays one is communication delay and another is computational delay. For communication delay we have simulated in NCTUNs because in VANET environment communication protocol 802.11(p) is used. We have simulated number of vehicles 10, 20, 40 in fixed transmission range (300 m).

5.2 Setup

Data packets are generated at a constant bit rate at *RSU* as well as on OBU. Figure 4a and figure 4b, shows the average and maximum delay when number of vehicles varies from 5-40. Speed of vehicles are assumed here 10- 30 ms^{-1} and acceleration / deceleration = 3 ms^{-2}.

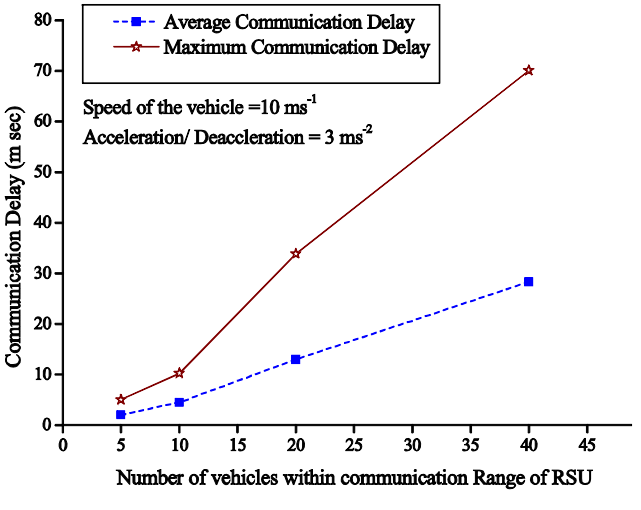

Fig. 4a. Average and Maximum communication delay at speed of source vehicle 10ms^{-1}

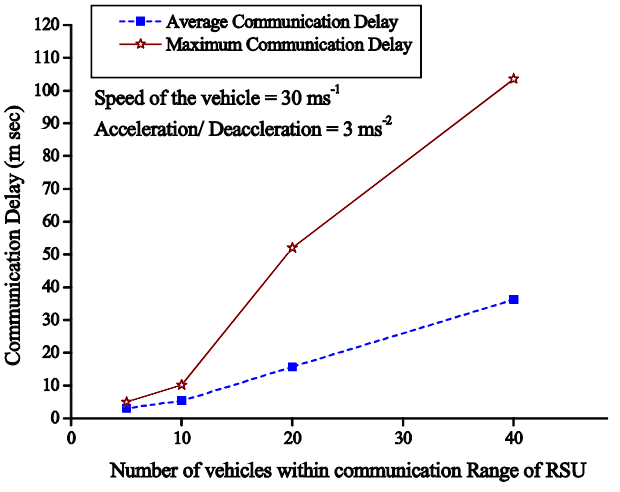

Fig. 4b. Average and Maximum communication delay at speed of source vehicle 30ms^{-1}

Computational Delay

For calculating delay of the authentication phase we analyze each step of the phase. Here we start with first step.

i. The delay when vehicle takes identity from RSU. t_2 is the time when vehicle send the request for authentication to RSU and RSU will send the public identity to vehicle $t_2 = t_0 + t_1$.

t_0 is the time when packet send by vehicle to RSU is 0.4081 ms.

t_1 is the communication delay of received packet from RSU when vehicles (around 40) are within the communication range of the RSU. Time t_1 is the maximum communication delay around 70ms and (~104) ms when vehicles having acceleration / deceleration of 3 ms^{-2} and speed of 10 ms^{-1} and 30 ms^{-1} respectively.

ii. t_3 is the delay when vehicle compute the hash function and encrypt the packet. Average delay of hash function (SHA-1) after multiple simulations is (~0.88) ms and similarly encryption or decryption delay t_4 is (~1.66) ms.

The delay of hash and encryption of the packet is $t_5 = t_3 + t_4$.

iii. Signing delay of the CTA is t_6 = (~1.33) ms. Verification delay t_7 is dependent on the computational delay of accessing the identity of claimant from its database and decryption delay t_4 .

Delay when RSU send the authentication request to CTA and CTA send the response to RSU along with the computational delay which is taken as 10 ms maximum.

Total time taken in authentication process is $T = t_2 + t_5 + t_7$.

Total maximum delay for authentication is T shown in figure 5. In figure 5a and figure 5b 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}.

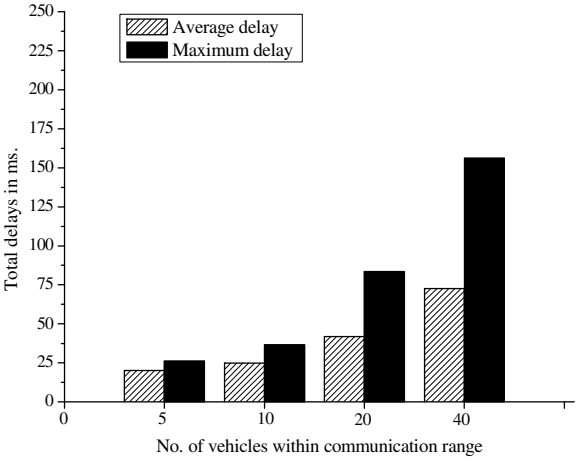

Fig. 5a. Average and maximum delay at speed of source vehicle 10ms^{-1}

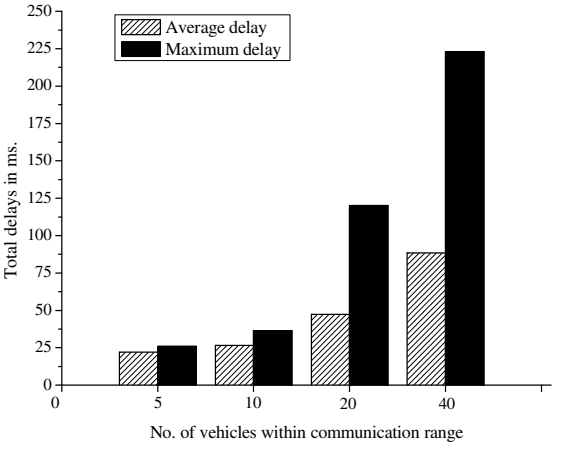

Fig. 5b. Average and maximum delay at speed of source vehicle 30ms^{-1}

6 Conclusion

In this paper, we provide a solution for privacy and mutual authentication process. We use the pseudonym based scheme for privacy preservation and mutual authentication.

The RSU was used as a mediator for authentication for both the RSU, itself, and requesting vehicle. Since the CTA is responsible for checking the credentials, the work of the RSU is drastically reduced. However, this requires all the RSU to be in continuous communication with a city level trusted authority, which may constitute a large overhead. This also solved the problem of malicious RSU along with the number of message exchange between different entities.

References

1. Dotzer, F.: Privacy Issues in Vehicular Ad Hoc Networks. In: Workshop on Privacy Enhancing Technologies, Dubrovnik, Cavtat, Croatia, pp. 197–209 (2005)
2. Dedicated Short Range Communications (DSRC), http://www.leearmstrong.com/Dsrc/DSRCHomeset.htm
3. Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., Raya, M.: Architecture for Secure and Private Vehicular Communications. In: International Conference on ITS Telecommunications (ITST 2007), Sophia Antipolis, France, pp. 1–6 (2007)
4. Gerlach, M., Guttler, F.: Privacy in VANETs using Changing Pseudonyms - Ideal and Real (Poster Presentation). In: Proceedings of 65th Vehicular Technology Conference VTC 2007.Spring, Dublin, Ireland (2007)
5. Armknecht, F., Festag, A., Westhoff, D., Zang, K.: Cross-layer privacy enhancement and non-repudiation in vehicular communication. In: Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks, WMAN 2007 (March 2007)
6. Raya, M., Hubaux, J.-P.: The Security of VANETs. In: VANET 2005, Cologne, Germany, pp. 93–94 (2005)
7. Ma, Z., Kargl, F., Weber, M.: Pseudonym-On-Demand: A New Pseudonym Refill Strategy for Vehicular Communications. In: Proc. IEEE 68th Vehicular Technology Conference, pp. 1–5 (2008)
8. Gruteser, M., Grunwald, D.: Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. Paper presented in the Proceedings of ACM WMASH, pp. 46–55 (2003)
9. Chaurasia, B.-K., Verma, S., Tomar, G.-S., Abraham, A.: Optimizing Pseudonym Updation in Vehicular Ad-hoc Networks. In: Gavrilova, M.L., Tan, C.J.K., Moreno, E.D. (eds.) Transactions on Computational Science IV. LNCS, vol. 5430, pp. 136–148. Springer, Heidelberg (2009)
10. Chaurasia, B.-K., Verma, S.: Maximising Anonymity of a Vehicle. Inderscience, International Journal of Autonomous and Adaptive Communications Systems (IJAACS), Special Issue on: Security, Trust, and Privacy in DTN and Vehicular Communications 3(2), 198–216 (2010)
11. Raya, M., Hubaux, J.-P.: Securing Vehicular Ad Hoc Networks. Journal of Computer Security, Special Issue on Security, Ad Hoc and Sensor Networks 15(1), 39–68 (2007)
12. Hubaux, J.-P., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Security & Privacy magazine 2(3), 49–55 (2004)
13. Raya, M., Hubaux, J.-P.: The security of vehicular ad hoc networks. In: Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pp. 11–21 (2005)
14. Studer, A., Shi, E., Bai, F., Perrig, A.: TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs. In: IEEE SECON 2009, Rom, Italy, pp. 1–9 (2009)
15. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of VANET 2004, pp. 29–37 (2004)

16. Sampigethaya, K., Li, M., Huang, L., Poovendran, R.: AMOEBA: Robust Location Privacy Scheme for VANET. IEEE JSAC 25(8), 1569–1589 (2007)
17. Guo, J., Baugh, J.-P., Wang, S.: A Group Signature Based Secure and Privacy- Preserving Vehicular Communication Framework. In: Proc. of the Mobile Networking for Vehicular Environment (MOVE) workshop in conjunction with IEEE INFOCOM, pp. 103–108 (2007)
18. Calandriello, G., Papadimitratos, P., Lioy, A., Hubaux, J.-P.: Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the Workshop on Vehicular Ad Hoc Networks (2007)
19. Lu, R., Lin, X., Zhu, H., Ho, P.-H., Shen, X.: ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of the Workshop INFOCOM (2008)
20. Verma, M., Huang, D.: SeGCom: Secure Group Communication in VANETs. In: 6th IEEE Consumer Communications and Networking Conference (CCNC 2009), pp. 1–5 (2009)
21. Lin, X., Sun, X., Wang, X., Zhang, C., Ho, P.-H., Shen, X.: TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving. IEEE Trans. on Wireless Communications 7(12), 4987–4998 (2009)
22. Zhang, C., Lin, X., Lu, R., Ho, P.-H.: RAISE: an efficient rsu-aided message authentication scheme in vehicular communication networks. In: Proc. IEEE ICC 2008, Beijing, China (2008)
23. `http://nsl.csie.nctu.edu.tw/nctuns.html`
24. Shamus Software Ltd. MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library, `http://indigo.ie/~mscott`