Research Inventy: International Journal Of Engineering And Science
Issn: 2278-4721, Vol. 2, Issue 7(March 2013), Pp 45- 49
Www.Researchinventy.Com

Enhancing the Privacy through Pseudonymous Authentication and Conditional Communication in Vanets

[1,]S. John Moses, [2,]P. Anitha Christy Angelin

[1](*PG Scholar, Department of Computer Science and Engineering ,Karunya University, Coimbatore, India,)*

[2](*Assistant Professor, Department of Computer Science and Engineering ,Karunya University, Coimbatore, India)*

Abstract - *An efficient privacy preservation scheme named Pseudonymous Authentication-based Conditional Privacy for providing anonymous and conditional communication to the vehicles in Vehicular Ad-hoc Networks (VANET'S). The Pseudonymous Authentication based Conditional Privacy scheme provides pseudonym-based anonymity to vehicles in VANETs. The Conditional Privacy in this scheme is that the vehicles in VANET must follow certain conditions to operate, communicate and transfer messages between vehicles in order to provide privacy to the vehicles in VANET. By all means the privacy and anonymity of the vehicles in VANET must be preserved, which is the primary goal of the Pseudonymous Authentication-based Conditional Privacy scheme.*

Keywords - *CA, ECPP, OBU, Pseudonym, RSU, VANET*

I. Introduction

Vehicular Ad-hoc Networks (VANET'S) consists of Group of vehicles, Road Side Units (RSU) and a Motor Vehicles Division (MVD), Which is a centralized or nodal trusted authority. The Road Side Units (RSU's) are the base stations or the router's through which the vehicles communicate with the Motor Vehicles Division (MVD) for obtaining authentication. The Motor Vehicles Division (MVD) is the centralized trusted authority to provide authentication to the vehicles and also to control and manage the operations of the vehicles. According to the Pseudonymous Authentication based Conditional Privacy scheme, all the vehicles in VANET that are using the scheme must register with the Motor Vehicles Division (MVD) using its identity. The Motor Vehicles Division (MVD) in response to the successful registration of the vehicle will gives back a ticket to the vehicle as an acknowledgement. The vehicle then uses that ticket to communicate with the Road Side Units (RSU) in its neighborhood to obtain tokens. The tokens are used by the vehicle to generate pseudonyms for anonymous broadcast communication with other vehicles.

II. System Assumptions

The assumptions that are made in the system are that all vehicles are registered with a central trusted authority (TA), i.e., the Motor Vehicles Division (MVD), before they are approved for driving on the road. Registration of a vehicle includes registration of the vehicle's license plate number, identity, owner's address, and any other information needed to uniquely identify the vehicle and its owner. Since the MVD is assumed to be trusted and cannot be compromised, the initial security parameters and keys are issued by the MVD. RSUs are not fully trusted since they are usually exposed in open unattended environments, which are subject to physical breaches. However, we assume that the functions of RSUs are monitored and that their compromise can be detected in a bounded time period. Consequently, at a given time, very few RSUs are compromised. Because RSUs can be compromised, we assume that the security keys and corresponding identity information cannot be directly generated by RSUs. Other vehicles are not trusted.

III. Network Model

The network model for our anonymity scheme is shown in Fig 1. It comprises on- and off-road units. The on-road units consist of the vehicles, the RSUs, and the communication network. The RSUs are managed and regularly monitored by a local transportation department office such as the MVD. The RSUs and the MVD are connected via the Internet. Existence of a central trust authority such as the MVD helps expedite revocation as all RSUs can contact it for updated vehicle RLs. Each vehicle is assumed to be equipped with an OBU, which is a tamper-proof device (TPD) that stores the secret information, an event data recorder (EDR), and a Global Positioning System. The RSUs and the vehicles are equipped with network cards that can provide support for the dedicated short-range communication (DSRC) service or WiFi access, hence enabling high-data-transfer rates with minimal latency.

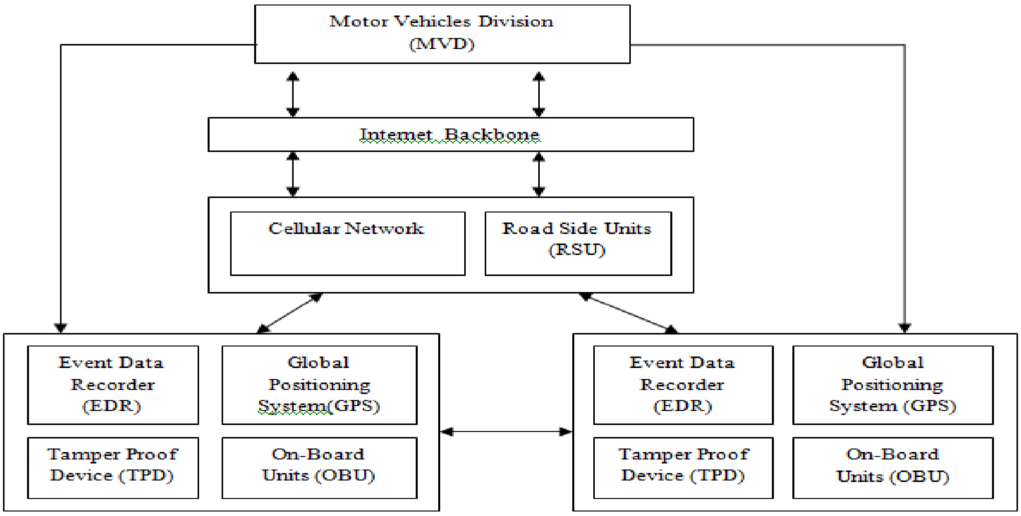
Motor Vehicles Division (MVD)
Internet Backbone
Cellular Network
Road Side Units (RSU)
Event Data Recorder (EDR)
Global Positioning System(GPS)
Tamper Proof Device (TPD)
On-Board Units (OBU)
Event Data Recorder (EDR)
Global Positioning System (GPS)
Tamper Proof Device (TPD)
On-Board Units (OBU)

Fig. 1. Network model for VANETs

IV. Attack Model

The attackers in a VANET may be classified as either internal attackers or external attackers. External attackers are powerful attackers that can observe and analyze the traffic in the network. They are not part of the system; hence, they cannot decrypt the messages, but they can obtain related information from the messages and use it for traffic and data analysis. We assume that the external attackers are more powerful than the vehicles or the RSUs; however, their powers are bounded. Usually, it takes multiple colluding external attackers to observe the whole system. Internal attackers are compromised vehicles. Internal attackers are potent as well since they are part of the system and have access to shared secrets. Here, we present all possible attack scenarios in a VANET. An attacker can (a) modify or replay existing messages, (b) inject fake messages, (c) impersonate a legitimate node (RSU or vehicle), (d) compromise an RSU or a vehicle, or (e) perform a denial-of-service attack. The attacks may be performed by a single attacker or a group of colluding attackers. We note that, of the aforementioned attacks, attacks (c), (d), and (e) are those that result in loss of privacy. Our scheme handles the rest of the attack scenarios and ensures that the anonymity of communication is preserved.

V. Pseudonymous Authentication-Based Conditional Privacy (PACP)

This scheme provides pseudonym-based anonymity to vehicles in VANETs. Before presenting our scheme in detail, we first give a general overview. A vehicle that uses our scheme registers with the motor vehicle department using its identity and gets a ticket. It uses the ticket to communicate with an RSU in its neighbourhood to obtain tokens. The tokens are used by the vehicle to generate pseudonyms for anonymous broadcast communication with other vehicles.

VI. System Setup

The scheme uses a set of publicly known system parameters params = (G1,G2, e, P,H,H1,H2), which are stored in each vehicle by the MVD at the time of registration. The MVD generates its public key as PMVD = αP, where $\alpha \in Z_p^*$ is the private key of the MVD. Our scheme uses the identity-based encryption (IBE) scheme proposed by Boneh and Franklin [20] for secure communication. All signatures generated in our scheme utilize the BLS short signature scheme proposed by Boneh because of its efficiency and low computation cost.

VII. PACP Protocols

In this scheme, pseudonym generation for a vehicle requires three types of entities, namely, the vehicle, the MVD, and the RSU. The interaction between these three entities is shown in. A vehicle Va provides the required identity information to the MVD as part of the registration process. Then, the MVD issues Va a ticket.

The ticket uniquely identifies Va; however, it does not reveal Va's true identity. When moving on the road, Va authenticates itself with the nearest RSU and obtains a pseudonym token. Then, Va uses the token to generate its pseudonyms. Here, we must note that the RSU only provides the credential (i.e., signature) and restrictions (i.e., a timestamp) for the vehicle to generate its pseudonyms, and it does not learn any private information of the vehicle. As a result, the RSU is unaware of the vehicle's true identity, which is mapped to the pseudonym that the vehicle will generate using the token. We note that the RSU can map a ticket to a pseudonym token and the generated pseudonym. However, this mapping cannot review the real identity of the vehicle. The only information possessed by the RSU is the token, which will be used in the revocation phase. We will discuss more about the resultant improvement in security in the security analysis section. Our system consists of three building blocks, namely, registration, generation, and extraction.

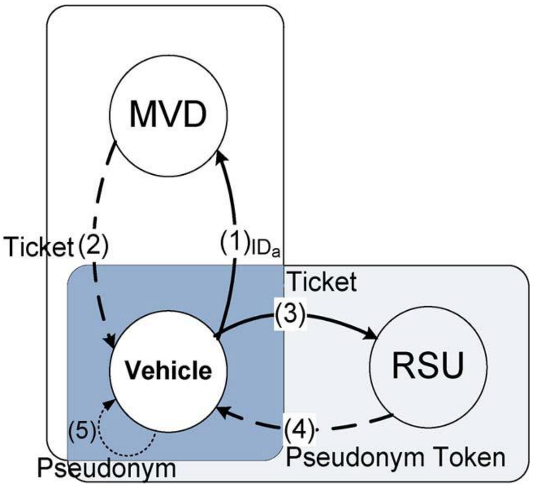

Fig. 2.State transition diagram for pseudonym generation

7.1 ANONYMOUS COMMUNICATION

The anonymous communication using our scheme is illustrated. We use two vehicles, namely, Va and V*b*, for our illustration. Consider a scenario where Va needs information about the road conditions. V*a* sends a broadcast request for the information using its pseudonym PN*j*(*a*,*i*). Vehicle V*b* that has the information uses pseudonym PN*j*(*a*,*i*) to encrypt it in a message and sends it to *Va*. On receiving the encrypted message, Va decrypts the message using private key *Sj*(*a*,*i*). In another scenario, vehicle V*a* can itself initiate a road conditions broadcast. When V*a* broadcasts a message with road conditions in its vicinity, other vehicles can use the public key of its pseudonym $\tau\ j(a,i) = \gamma j(a,i)SaP$ to verify the BLS signature generated by *Va* using private key $\gamma j(a,i)Sa$.

7.2 EVALUATION RESULTS AND ANALYSIS

The schemes proposed in the literature can be broadly categorized into those based on elliptical curve cryptography and those based on RSA. We compare our protocol with the best schemes in each category. The schemes we compare with are the elliptical curve-based VANET standard named ECIES, the ECPP scheme and the RSA-based schemes. We compare the schemes on the basis of average latency experienced at the RSUs for pseudonym generation, the time taken to perform the encryption and decryption protocols that ensure anonymity, and the running time complexity of revocation. The latency experienced at the RSU has to be as small as possible because high latency results in a few number of vehicles obtaining their tokens in a given time period. Not all schemes can be compared with this scheme on the aforementioned comparison criteria. For the latency measurements, we compare with ECPP; for encryption and decryption, we compare with the ECIES- and RSA-based schemes; and for complexity analysis of revocation, we compare with the ECPP scheme. For the RSA-based schemes, the basic building block is RSA; hence, instead of comparing with each scheme, we compare our scheme with only RSA.

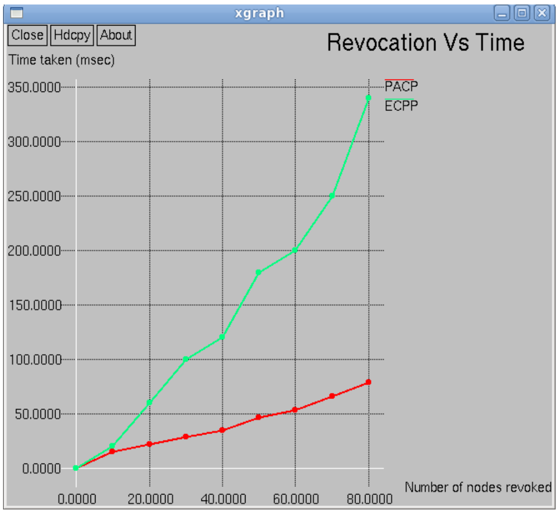

Fig.3. Comparison of time taken for revoking malicious nodes in our scheme and ECPP

When the ECPP, and our schemes are used. we study the total time for token generation at the RSU because it is also an overhead of the anonymity protocols, and the lower the total time required, the more desirable the protocol. The number of vehicles communicating with the RSU was increased from 10 to 100, and for each vehicle, ten tokens were requested. As we have pointed out before, low latency at the RSU is desirable as it allows more vehicles to obtain tokens from the RSU. The latency at the RSU for the generation of a single token using each of the two schemes is given as *Tl* ECPP = 154.3 ms, and *Tl* PACP = 58.86 ms. For ECPP, the latency is computed as the total time taken by the RSU to perform 13-point multiplication and six pairing operations . The time consumed by other operations such as random number generation is ignored. In our scheme, the latency is the sum of the time taken by the RSU to decrypt the message, verify the signature of the ticket and generate the signature of the token. The scheme has a protocol latency that is comparable to the faster schemes based on RSA. The RSA based solutions have the least latency, followed by our scheme and ECPP schemes. The reason for low latency in RSA is because of the efficiency of the public key operations for encryption.

VIII. CONCLUSION

The discussed methodology provides high level of anonymity to the vehicles in the VANET'S. It also makes the computation very effective in terms of privacy ensuring mechanism and revoking the unanonymous vehicles and protocols. This scheme is more secure and efficient and has less latency and it takes much less time to search the revoked node. In addition our scheme provides high security and better scalability and it has the least payload size. Thus the Privacy, Authentication and Anonymity of the vehicles in VANET'S is ensured by the discussed Pseudonymous Authentication based Conditional Privacy Mechanism

References

[1] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, Apr. 2008, pp. 1229–1237.

[2] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput.Security, vol.15, no. 1, pp. 39– 68, Jan. 2007.

[3] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications,"IEEE Wireless Commun., vol. 13, no. 5, pp. 8–15, Oct. 2006.

[4] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications,"IEEE Trans.Veh.Technol., vol.56, no.6, pp.344–345, Nov.2007.

[5] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," J. Commun. Netw., vol. 11, no. 6, pp. 574–588, 2009.

[6] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux Antonio Lioy, "Efficient and Robust Pseudonymous Authentication in VANET,"VANET'07, 10 September, (2007).

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

[8] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya "Architecture for Secure and Private Vehicular Communications''in Telecommunications, ITS, vol.5, no.6, pp.1-6 ,June/July 2007.

[9] L.Butty´an,T.Holczer,I.Vajda,"On the effectiveness of changing pseudonyms to provide location privacy in VANETs"In Proc.of Privacy in Ad hoc and Sensor Networks (ESAS 2007).

[10] Hang Dok, Huirong Fu, Ruben Echevarria, and Hesiri Weerasinghe, “Privacy Issues of Vehicular ad hoc networks” in International Journal Of Future Generation Communication and Networking Vol .3, No.1, March 2010.

[11] M. Raya, P. Papadimitratos, and J. Hubaux, “Securing vehicular communications,” IEEE Wireless Commun., vol. 13, no. 5, pp. 8–15, Oct. 2006.

[12] X. Lin, X. Sun, P. Ho, and X. Shen, “GSIS: A secure and privacy preserving protocol for vehicular communications,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[13] A. Wasef and X. Shen, “PPGCV: Privacy preserving group communications protocol for vehicular ad hoc networks,” in Proc. IEEE ICC, May 2008, pp. 1458–1463.

[14] H. Xie, L. Kulik, and E. Tanin, “Privacy-aware traffic monitoring,” IEEE Trans. Intell. Transp. Syst., vol. 11, no. 1, pp. 61–70, Mar. 2010.

[15] U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety CommunicationsProject—FinalRep.,Apr. 2006. [Online]. Available: http://www.nhtsa.gov/DOT/NHTSA/ NRD/Multimedia/PDFs/Crash%20Avoidance/2005/CAMP3scr.pdf.

[16] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in Proc. 3rd ACM Workshop Security Ad Hoc Sens. Netw., 2005, pp. 11–21. 746 IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 12, NO. 3, SEPTEMBER 2011