Secure and Reliable Identity Management for VANETs

Jenny Torres
Laboratoire d'Informatique de Paris 6
UPMC-Sorbonne, France
Email: Jenny.Torres@lip6.fr

Michele Nogueira
Department of Informatics
Federal University of Paraná, Brazil
Email: michele@inf.ufpr.br

Guy Pujolle
Laboratoire d'Informatique de Paris 6
UPMC-Sorbonne, France
Email: Guy.Pujolle@lip6.fr

***Abstract*—Identity Management plays a fundamental role in VANETs due to wireless medium that makes eavesdropping easy, and a set of abuses and attacks becomes possible such as the loss of node's privacy, the disclosure of personal information, identity theft and impersonation. In this paper, a Reliable and Anonymous Communication scheme for VANETs (RACE) is presented. It provides a secure and efficient node identification and message authentication for vehicle-to-vehicle and vehicle-to-infrastructure communications, as shown by evaluation analyses.**

I. Context

Vehicular networks have demonstrated huge potential and also special characteristics, which yield new challenges and opportunities. As shown in Figure 1, VANETs comprise vehicles equipped with wireless communication devices, On-Board Units (OBU), allowing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, supporting applications, such as road traffic control, safety, emergency, and entertainment [1]. Along the road, there are Road-Side Units (RSU) and a trusted third party, called Identity Management Server (IMS). Differently from other kind of networks, VANETs own a high dynamic topology due to vehicles mobility, requiring unique solutions and efficient actions under real-time constraints.

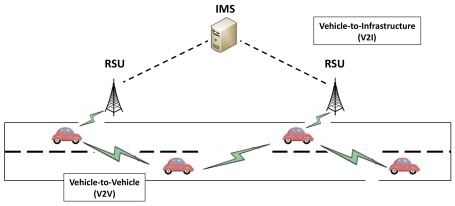

Fig. 1: VANETs - V2V and V2I communications

II. Motivation

VANETs are prone to different attacks concerning the identity of nodes. False or stolen personal information such as vehicle information, driver behavior or road condition data can cause damage if the network is not secure and if privacy of the vehicles is not protected. Attackers can eavesdrop private information and using a false identity, they can suppress, modify, replay messages or introduce misinformation about other drivers and traffic into the network [2]. Managing identities in VANETs is an important challenge due to network characteristics such as mobility, real time processing and infrastructureless. VANETs inherit all the features presented in traditional IdM systems but at the same time brings new ones, such as an effective identity management, pseudonym management, privacy and security.

III. Proposal: A Reliable and Anonymous Communication Scheme (RACE)

RACE is a reliable and anonymous communication scheme for VANETs based on pseudonyms that provides a secure and efficient node identification and message authentication for V2V and V2I communications. The scheme illustrated in Figure 2 is designed based on a secure foundation of Elliptic Curve Cryptography (ECC), particularly the usage of the elliptic curve version of Schnorr's identification and signature protocol, which provides zero-knowledge proof. RACE consists of four main phases: Key Generation, Identification, Authentication and Revocation.

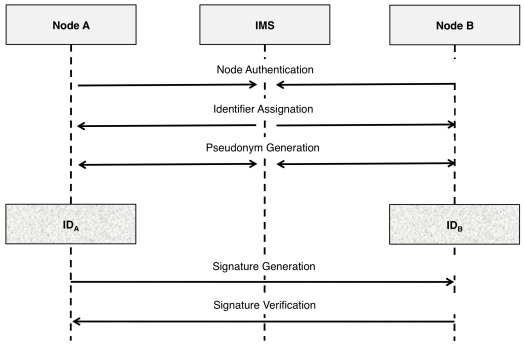

Fig. 2: RACE - Reliable and Anonymous Communication schemE

The **key generation** is executed the first time a node (A) joins the network. The two parties select a random number $d \in [1, n-1]$ and compute $Q = dG$. IMS's and A's public/private key pair are (Q_{IMS}, d_{IMS}) and (Q_A, d_A) respectively. The private key, called long-term identity, is unique and is kept secret by the corresponding party. In the case of public keys, everyone knows IMS's public key while node's public key is only known by the IMS.

In the **identification** phase, the node authenticates with the IMS in order to receive an identifier. The node should prove its identity through a zero-knowledge identification protocol (commitment-challenge-response), without giving away any identifying information concerning its real identity, instead, using temporary secret keys that will let the node to blind it. If the protocol is successful a node registration phase is accomplished in order to conclude the identification process. The IMS selects a random number $id_A \in [1, n-1]$ and computes A's identifier, such that $K_A = id_A G$ and sends it to A. With this identifier, the node is allowed to generate a different pseudo identity (pseudonym) for each session or

message computing $ID_A = d_A K_A$. The node is able to renew its pseudonym in connectivity periods, when it can contact the IMS, accomplishing the identification process mentioned before. The IMS computes $ID_A = id_A Q_A$ and registers node's pseudonym associated with the tuple (K_A, id_A) in case of revocation. Now, both, A and IMS share the pseudonym ID_A since $ID_A = d_A K_A = id_A Q_A = d_A id_A G$. Node's real identity remains anonymous for other nodes, which are going to contact it only by this pseudonym registered in the IMS.

Once the identification of the node is done, and in order to contact a node B, a message **authentication** phase is accomplished. The message is authenticated through a signature and its corresponding verification. For signing, a randomized algorithm takes as input a private key d_A, and a message M, and outputs a signature σ. For the security of the signature process it is necessary to apply a hash function $H : \{0,1\}^* \leftarrow [1, n]$. In the verification process, an algorithm takes as input the public key associated with signer's private key (signer's pseudonym ID_A), the message M, the signature σ and outputs either *accept* or *reject*.

Since node's pseudonym does not reveal any information about node's real identity, other nodes in the network cannot identify a misbehaving node. The **revocation** should be decided by the IMS based on administrative or technical reasons in order to prevent misbehaving nodes from causing damage into VANETs. When the decision of revocation is reached, the IMS search in all the records from its repository the entry corresponding the node's identifier with the corresponding pseudonym in order to restraint the node from future communications in the VANET system. The IMS is the only authorized party that can perform the tracing to reveal a node identifier. No one can obtain node's real identity, neither the IMS. Nevertheless, IMS can revoke node's pseudonym storing it, with the identifier assigned, into a revocation list.

IV. Results and Security Discussion

Our scheme is based on ECC, because it allows the use of fewer bits than conventional public key cryptography. A 1024-bit RSA key is equivalent to a 192-bit key when using ECC. A more secure RSA key will require twice the number of bits, it means a 2048-bit key, while an equivalent ECC key is 224-bit key, which is only a 16.66% longer than the previous one. ECC increases security with smaller key sizes, which provides less storage area and less bandwidth, as well as efficiency and high-speed, as shown in Figure 3.

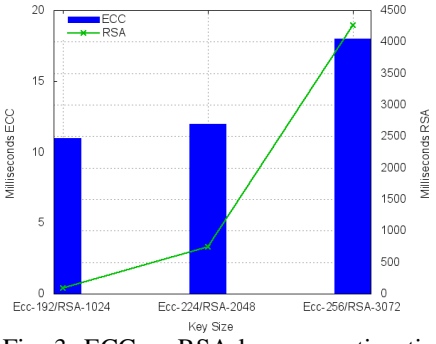

Fig. 3: ECC vs RSA key generation time

In the key generation phase, ECC does not need pre-computation time for the generation of prime numbers as RSA does, thus, it can create the key pair in a higher speed. Figure 4 gives an idea of how fast the key generation operation is for variable key lengths and variable number of nodes.

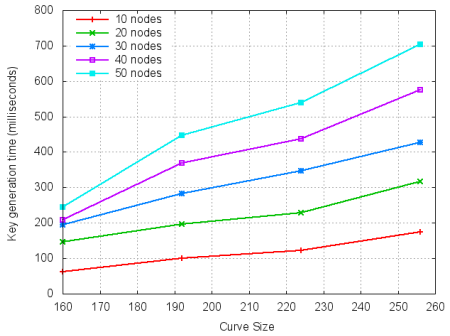

Fig. 4: ECC key generation time vs curve size

Identification and Authentication are the main operations considered in this scheme for controlling access to computer resources. The security of the scheme is supported by *node identification*. In order to guarantee node privacy, anonymous node identification will let verify its legitimacy without revealing its real identity. This anonymity is achieved through the use of a zero-knowledge identification protocol, where the node does not disclose any information concerning its real identity. Node's identities are classified into long-term and short-term. Long-term identities are blinded by temporary secret keys used in the identification process. The generation of these keys is considered as a negligible timing value, thus they do not increase overhead in communication. If node identities are not set up in a secure way, then how they are managed becomes irrelevant, having as consequence an unreliable authentication. On the other hand, establishing *message authentication* in the scheme ensures the reliability of the communication, because it let verify sender identity and protect the integrity of a message. *Integrity* will ensures that each message that is received and considered acceptable, arrives in the same condition that it was sent out. A node should be able to verify that a message was really signed and sent by another node without being modified by anyone.

V. Conclusion

Identity privacy is an important issue in VANETs, however the management of identities is an unconcerned area. Most of the works focus on message authentication instead on node identification, thus node privacy remains unconcerned. The proposed scheme provides secure node identification and message authentication, protecting identity data through advanced cryptography. Node's authentication is accomplished through an identification protocol, while digital signatures provide message authentication, both of them built on a secure foundation of Schnorr identification and signature protocol based on ECC, an ideal candidate for implementation on devices with low computational power.

References

[1] A. Squicciarini, D. Lin, and A. Mancarella, "PAIM: Peer-based automobile identity management in vehicular ad-hoc network," in *IEEE 35th Annual Computer Software and Applications Conference (COMPSAC)*, July 2011, pp. 263 –272.

[2] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, February 2012.