Designing Communication-Oriented Node Authentication for VANETs[*]

P. Caballero-Gil and C. Hernández-Goya

Department of Statistics, Operations Research and Computing. University of La Laguna. 38271 La Laguna. Tenerife. Spain. {pcaballe, mchgoya}@ull.es

ABSTRACT

Vehicular Ad-hoc NETworks (VANETs) present unique challenges such as high node mobility, real-time constraints, scalability, gradual deployment and privacy. No existent node authentication technique addresses all these requirements. In particular, both inter-vehicle and vehicle-to-roadside wireless communications have different privacy and efficiency needs that must be taken into account when defining node authentication services.

1. Introduction

A Vehicular Ad-hoc Network may be seen as a particular Mobile Ad-hoc Network used for communication among vehicles and between vehicles and roadside equipment [1] [2]. A special electronic device called On-Board Unit (OBU) is placed inside each vehicle to provide ad-hoc network connectivity. Communications between OBUs are referred to as Vehicle-TO-Vehicle (V2V) communications, while communications between an OBU and the Road-Side Unit (RSU), which is fixed equipment on the road, are referred to as Vehicle-TO-Infrastructure (V2I) communications. V2V and V2I communications enable both the improvement of safety, efficiency and comfort in everyday road travel, and the offer of other value-added services such as commercial information or Internet access. The security of both types of communications is a necessary pre-requisite for the general adoption of VANET technology. In order to achieve security, node authentication is the most fundamental piece, but authentication in such a mobile environment poses a great privacy risk [3].

2. Proposal

It is generally assumed that messages sent through a VANET may be digitally signed by the sender with a public-key certificate that is generally emitted by a Certification Authority (CA). The moments corresponding to the vehicle purchase and to the periodic technical inspections might be respectively associated to the emission and renovation of its public-key certificate. However, the use of a Public-Key infrastructure in VANETs implies the problem of the enormous cost of the management of a huge CA, with the corresponding high consumption of resources. Moreover, it makes it very difficult to deal with anonymity. Since public keys should be frequently updated in order to protect privacy, it becomes impractical that all vehicles store the public keys of the remaining nodes. Thus, proposals such as self-organized and distributed public-key certification might be good solutions.

Group formation is here proposed as a strategy to strengthen privacy and provide authentication, while reducing communications in VANETs. In particular, we propose location-based group formation according to dynamic cells dependent on the characteristics of the road, and especially on the average speed. In this way, any vehicle that circulates at such a speed will belong to the same group within its trajectory. We also propose that the leader of each group be the vehicle that has belonged to the same group for the longest time. According to our proposal, V2V between groups will imply package routing from the receiving vehicle towards the leader of the receiving group, who is in charge of broadcasting it to the whole group if necessary. In the two phases corresponding to group formation and node joining, each new node has to authenticate itself to the leader through asymmetric authentication. Later, the leader sends a shared secret key to it, encrypted with the public key of the new node. This secret key is shared among all the members of the group and used both for V2V within the group and for V2V between groups. We propose the use of different cryptographic primitives for node authentication, paying special attention to the efficiency of communications and to the need of privacy. We analyze four different types of authentication in the following subsections.

2.1. I2V Authentication

Since privacy-preserving authentication is not necessary in I2V, we propose for I2V the use of Identity-Based Cryptography as it allows avoiding the difficult public-key certificate management problem. It is a type of public-key cryptography in which the public key is some unique information about the identity of the user [4]. A proposal for VANETs could be based on the Boneh/Franklin's pairing-based encryption scheme [5], which is an application of Weil pairing over elliptic curves and finite fields.

2.2. V2I Authentication

In V2I communications, privacy is an essential ingredient. Here we propose a challenge-response authentication protocol based on a secret-key approach where each valid user is assigned a random key-ring with k keys drawn without replacement from a central key pool of n keys [6]. During authentication each user chooses at random a subset with c keys from its key-ring, and uses them in a challenge-response scheme to authenticate itself to the RSU in order to establish a session key, which is sent encrypted under the RSU's public key. This scheme preserves user privacy due to the feature that each symmetric key is with a high probability shared by

[*] Research supported by the Spanish Ministry of Science and Innovation, and the FEDER Fund under Project TIN2008-02236/TSI

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.6911
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.6911

several vehicles. If a vehicle wants to communicate with the RSU, it sends an authentication request, a set of *c* keys taken at random from its key-ring and a timestamp. All this information is encrypted with the established session key. Note that a set of keys, instead of only one key, is proposed for authentication, because there is a high probability to have one key shared by a large amount of vehicles. This makes it difficult to identify a possible malicious vehicle if just one key is used. However, there is a much lower probability that a set of *c* keys be shared by a large number of vehicles, and so it is much easier to catch a malicious vehicle in the proposal. After the RSU gets the authentication request from the vehicle, it creates a challenge message by encrypting a random secret with the set of keys indicated in the request. Upon receiving the challenge, the vehicle decrypts the challenge with the chosen keys and creates a response by encrypting the random secret with the session key. Finally, the RSU verifies the response and accepts the session key for the next communications with the vehicle. In the first step, in order to make easier the task of checking the key subset indicated in the request by the RSU, we propose a tree-based version where the central key pool of *n* keys may be represented by a tree with *c* levels [7]. Each user is associated to *k/c* leaves, and each edge represents a secret key. In this way, the key-ring of each user is formed by several paths from the root to the leaves linked to it. During each authentication process the user chooses at random one of its paths, which may be shared by several users. In this way, to check the keys, the RSU has to determine which first-level key was used, then, it continues by determining which second-level key was used but by searching only through those second-level keys below the identified first-level key. This process continues until all *c* keys are identified, what at the end implies a positive and anonymous verification. The key point of this proposal is that it implies that the RSU reduces considerably the search space each time a vehicle is authenticated.

2.3. V2V Authentication inside Groups

At the group formation and group joining stages, each new node has to authenticate itself in front of the group leader by using public-key signatures [8]. After group formation or group joining, the group leader sends a secret shared key to every new member of the group, encrypted with the public key of this new node. Such a secret group key is afterwards used for any communication within the group both for node authentication and for secret-key encryption if necessary (e.g. for commercial applications). In this way, the efficiency of communications inside the group is maximized because on the one hand certificate management is avoided, and on the other hand, secret-key cryptography is in general more efficient than public-key. Note that the use of a shared secret key also contributes to the protection of privacy.

2.4. V2V Authentication between Groups

In order to protect privacy, group signatures are proposed for node authentication between groups. A group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group so that everybody can verify such a signature with the public key of the group. This group signature identifies the signer as a valid member of the group and does not allow distinguishing among different group members [9]. The so-called group leader is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. In our proposal, the group leader issues a private key to each vehicle within the group, which uniquely identifies each vehicle, and at the same time allows it to compute a group signature and prove its validity without revealing its identity. In this way, any vehicle from any group will be able to communicate with any vehicle belonging to other group anonymously. In particular, our proposal for group signature is based on the cryptographic primitive of bilinear pairings, which was also proposed for I2V authentication.

3. Conclusions

We have briefly described different services for node authentication in VANETs that depend on the participants in the process. For I2V, since privacy is not needed, in order to avoid certificates management Identity-Based cryptography is proposed. In V2I a challenge-response authentication protocol that uses a secret-key approach based on random key-trees is described. To provide privacy between groups we propose group signatures. For V2V inside groups, secret-key authentication is defined. Since this is a work in progress, many open questions remain: concrete definitions of proposals, analysis of interactions, comparison with other previous solutions, and NS-2 implementation.

References

[1] Hubaux J, Capkun S, Luo J. The security and privacy of smart vehicles. IEEE Security and Privacy 2004 4(3): 49-55.

[2] Raya M, Hubaux J. The security of vehicular ad hoc networks. 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, USA, Nov. 2005: 11-21.

[3] Calandriello G, Papadimitratos P, Lloy A, Hubaux J P. Efficient and robust pseudonymous authentication in VANET. Fourth ACM VANET 2007, Canada: 19-28.

[4] Shamir A.: Identity-Based Cryptosystems and Signature Schemes. Proc. CRYPTO 84, LNCS 7: 47-53.

[5] Boneh D., Franklin M. K.: Identity-Based Encryption from the Weil Pairing. Proc. CRYPTO 2001, LNCS 2139: 213-229.

[6] Xi Y., Sha K., Shi W., Scnwiebert L., Zhang T.: Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks. Eighth ISADS 2007: 344-351.

[7] Buttyán L., Holczer T., Vajda I.: Optimal Key-Trees for Tree-Based Private Authentication. Privacy Enhancing Technologies: 332-350 (2006).

[8] Sampigethava K., Huang L., Li M., Poovendran R., Matsuura K., Sezaki K.: CARAVAN: Providing Location Privacy for VANET, International workshop on Vehicular ad hoc networks (VANET) (2006).

[9] Chaum D., van Heyst E.: Group signatures, Proc. EUROCRYPT'91, LNCS 547: 257-265.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.6911
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.6911