Computer Standards & Interfaces 36 (2014) 704–710

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Mutual authentication in self-organized VANETs

Cándido Caballero-Gil, Pino Caballero-Gil *, Jezabel Molina-Gil

Dept. Statistics, Operations Research and Computing, University of La Laguna, 38271 La Laguna, Tenerife, Spain

ARTICLE INFO

Available online 31 December 2013

Keywords:
Vehicular Ad-hoc NETwork
Authentication
Security
Self-organization
Wireless communication

ABSTRACT

The practical deployment of vehicular networks is still a pending issue. In this paper we describe a new self-organized method of authentication for VANETs, which allows their widespread, fast and secure implementation. Our proposal does not involve any central certification authority because the nodes themselves certify the validity of public keys of the other nodes. On the one hand we propose an algorithm that each node must use to choose the public key certificates for its local store. On the other hand, we also describe a new node authentication method based on a cryptographic protocol including a zero-knowledge proof that each node must use to convince another node on the possession of certain secret without revealing anything about it, which allows non-encrypted communication during authentication. Thanks to the combination of the aforementioned tools, the cooperation among vehicles can be used for developing several practical applications of VANETs, such as detection and warning about abnormal traffic conditions. One of the most interesting aspects of our proposal is that it only requires existing devices such as smartphones, because the designed schemes are fully distributed and self-organized. In this work we include an analysis of both an NS-2 simulation and a real device implementation of the proposed algorithms, which enables us to extract promising conclusions and several possible improvements and open questions for further research.

1. Introduction

Among the wireless networks that have received more attention of both the research and the industry communities in the last years are Vehicular Ad-hoc NETworks (VANETs). A VANET may be defined as a spontaneous wireless network of vehicles, which allows them to communicate and share information, with the main goal of improving traffic conditions. In particular, communications among vehicles have a tremendous potential to improve road safety, traffic efficiency, and comfort for both drivers and passengers. Therefore, a rapid deployment of VANETs would be very useful to save time and money spent on the road, and to reduce environmental pollution and consumption of fuel reserves.

Security of communications in VANETs is one of the most important issues to enable their practical deployment because of the variety and severity of possible attacks. On the one hand, false traffic warning messages can influence drivers' decisions, waste drivers' time and vehicles' fuel, and even lead to traffic accidents. Therefore, VANETs should prevent that attackers can send untruthful information about road conditions such as traffic jams in order to mislead other vehicles. This implies that VANETs should not provide full vehicle anonymity because the possibility of sending false messages would compromise their safe practical application. In fact, node authentication is necessary both to guarantee that only trustful vehicles can communicate and to allow law enforcement to track offending vehicles as an aid in investigations about stolen cars or hit-and-run accidents for example. However, on the other hand, VANETs must provide a way to retain privacy in order to avoid that vehicles can be tracked under normal circumstances, because that could provide information about past and current locations of vehicles, which would lead to the lack of driver's privacy and even be misused for crimes such as kidnapping and robbery. In conclusion, since vehicles in VANETs require privacy, it is important to devise a method to authenticate them while maintaining privacy.

The aforementioned security requisites of VANETs are added to other needs related to efficiency, such as scalability, cooperation, stability and low communication delay, which should be considered too. All those requirements are more challenging in these networks than in other wireless networks due to their specific characteristics, such as lack of fixed infrastructure and rapidly changing scenarios ranging from rural roads with little traffic to cities or roads with a large number of vehicles. Consequently, communication security can be considered one of the most challenging research issues that have to be taken into account before carrying out a broad deployment of VANETs. In recent years there has been abundant research on vehicular networks, but so far no proposal can be found in the bibliography, which implies the feasibility of their secure, broad and rapid deployment of these networks. Nowadays, IEEE standardization efforts are converging towards the definition of the so-called Wireless Access in Vehicular Environment (WAVE) protocol, and of the draft 802.11p [18] that will be the standard for medium access control in inter-vehicle communications.

* Corresponding author.
E-mail addresses: ccabgil@ull.es (C. Caballero-Gil), pcaballe@ull.es (P. Caballero-Gil), jmmolina@ull.es (J. Molina-Gil).

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.12.005

The starting point of this proposal is the conclusion that nowadays it is infeasible to introduce a complete model of VANET according to the classical definition found in the literature and in the 802.11p standards, which include Road Side Units (RSUs) and On Board Units (OBUs). The deployment of such a type of VANET would be extremely costly, both for users as they would have to buy new cars or install specific devices (OBUs) in their vehicles, and for the state that would have to deploy a large infrastructure on the roads (RSU) to support VANET services. Thus, in the current global economic situation, such large-scale disbursements are infeasible. Therefore, this paper proposes an alternative self-organized approach to VANETs that does not require any infrastructure and any economic investment neither by users nor by governments. Besides, our proposal could be used as a quick and secure introduction to more comprehensive and standardized VANETs in the future.

This paper is structured as follows. Section 2 reviews some related work. In Section 3, proposals for the generation of public keys, for node characterization and for beacon management are included. Section 4 presents a new zero-knowledge authentication protocol, and its analysis through a proof of concept implementation. In Section 5, a new method to choose certificates for the local key stores is described, and analyzed through simulation. Then, Section 6 includes a brief comparison with other proposals. Finally, Section 7 presents our conclusions and outlines some topics for future research.

2. Literature review

The main objective of this work is the definition of a simple, scalable and practical design for the immediate deployment of VANETs by exploiting the potential of current smartphones. The proposed scheme is based on the collaboration among users through their mobile devices by providing and obtaining updated information of interest about nearby traffic conditions in order to enable them to choose the best route to their destinations. Our proposal takes into account the gradual deployment of VANETs, because initially they will have neither RSUs nor OBUs, and in fact they will have only a few mobile devices. Since the growth of VANETs will be faster or slower depending on its popularity, acceptance, ease of use and cost, all these features have been prioritized in the design. Thus, scalability, efficiency and minimization requirements have been considered in the scheme proposed here.

In this paper we focus on the first phase of VANET deployment, when the number of devices in the network will be smaller. Once the VANET has spread and the number of vehicles belonging to it has increased, the model should be revised to avoid unnecessary communications that can degrade the network. [12] includes an analysis of the effect of high vehicle densities in VANET communications under these circumstances. Group-based solutions for authentication are proposed for such situations in [1], where the specific characteristics of inter-vehicle and vehicle-to-roadside communications are taken into account to define different authentication services. Also a group-based method is proposed in [21] in particular for 802.11p vehicular networks.

The practical requirement minimization is a criterion used in several studies focusing on different aspects and applications of VANETs. For example, [11] proposes a notification scheme of free parking lots that does not require any complete infrastructure but only RSUs located in the parking lots. Moreover, [16] proposes a key management scheme for VANETs, which is used to authenticate messages, identify legitimate vehicles and prevent access to malicious vehicles. However, such a proposal is based on the use of a public key infrastructure, which involves several problems, such as the certification of public keys. On the other hand, with the changing topology of VANETs, it is challenging to sustain connections for extended periods of time, so broadcasting messages is the most scalable solution. However, flooding of messages can result in a huge number of collisions in the network and hence in a hard degradation of performance. This particular problem is analyzed in [7] for the case when signature flooding is used for authentication.

In general, security in VANETs is a critical concern that has been studied by many researchers. For instance, [14] uses anonymous certificates to hide the true identities of users, but in that proposal privacy can still be invaded by tracking senders until identities are discovered. The issue of privacy in VANETs is discussed in several papers such as [5] and [20]. [13] proposes the protection of privacy through the combination of symmetric and asymmetric cryptography. On the other hand, [17] uses session keys to protect privacy. Finally, [10] presents a privacy-preserving vehicular communications protocol that is based on group signatures, but its main trouble is that the proposed method cannot deal with the exclusion of compromised vehicles. Another security scheme for vehicular networks that includes authentication with privacy preservation is [15], where public key cryptography is used, and the notion of adaptive privacy and a group-based authentication protocol are proposed.

There are many references on the issue of node authentication in VANETs that offer different types of self-managed schemes, but using methods that are totally different from the one presented here. For example, [3] proposes an authentication scheme that relies exclusively on pseudonyms, while [9] describes a scheme that combines authentication, key establishment and blind signature techniques. On the other hand, in [20] each RSU maintains an on-the-fly generated group consisting of vehicles that occasionally enter the RSU communication range so that the RSU periodically broadcasts its own certificate and its neighbor RSU certificate to the vehicles within its range. However, verification is not efficient enough due to the length of the signature. With respect to certification of public keys, [8] presents a method for revoking certificates based on epidemic distribution car-to-car, and [6] proposes a different mechanism that needs a central Certification Authority (CA) and certificate revocation lists.

The secure and self-organized approach of VANETs followed in this work is not used in any of the aforementioned papers. In particular, our authentication proposal is focused on enabling the immediate and rapid deployment of VANETs through existing mobile devices.

3. Basic elements

The proposed authentication method is based on a Zero-Knowledge Proof (ZKP), which is a cryptographic protocol that a prover can use to prove possession of a certain piece of information to a verifier without revealing anything about it. During the authentication procedure, the prover, denoted *A*, must answer to a number of challenges issued by the verifier, denoted *B*. The admission control included in the authentication proposal described below uses the general scheme of ZKP defined in [2] based on the graph isomorphism problem, for the particular case of the Hamiltonian Cycle Problem (HCP), which involves the determination of whether a graph contains a cycle that visits each node exactly once.

Our proposal is based on certificate graphs [4], so that each node *A* has a private/public key pair and a key store ($KeyStore_A$) including a list of all node certificates that *A* trusts. The set of stored public keys and certificates may be represented as an undirected graph $G = (V,E)$, known as a certificate graph, in which each vertex represents both a public key and its owner, and each edge (A,B) symbolizes two public key certificates: of node *A* signed with the private key of node *B*, and vice versa. A certificate chain is an undirected path in a certificate graph. The subgraph G_A of the certificate graph *G* contains exactly the current certificates stored by node *A* in $KeyStore_A$.

The following subsections include brief explanations of the generation of public keys, characterizations of nodes and management of beacons.

3.1. Public key generation

The node authentication process described below is based on the implementation of the ZKP for the HCP. That is the reason why we use the