Ad Hoc Networks 10 (2012) 1115–1133

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Chains of Trust in vehicular networks: A secure Points of Interest dissemination strategy

David Antolino Rivas *, Manel Guerrero-Zapata

Department of Computer Architecture, Polytechnic University of Catalonia, Barcelona 08034, Spain

ARTICLE INFO

Article history:
Received 24 May 2011
Received in revised form 12 January 2012
Accepted 17 February 2012
Available online 3 March 2012

Keywords:
Security
VANETs
Chains
Trust
POI
Reputation

ABSTRACT

This article describes a scheme which to the best of our knowledge is the first one to use user signatures to share information about *Points of Interest* in *Vehicular Ad hoc Networks*. In this scheme, users rate restaurants, hotels, etc. and sign those rates with their private key. Then, they broadcast that information and other vehicles store it for future use. When another user needs a *Point of Interest* recommendation he queries the system for the other users stored reviews and after he visits that *Points of Interest* for himself, he evaluates it and his level of trust in the reviewers with rates similar to his own increases. In the end, a user will be able to request to his vehicle information on a certain *Point of Interest* category and it will respond with the recommendations made by other users, prioritizing the ones in the user's *Web of Trust*. *poiSim* is the tool designed to simulate this scheme. It processes a 24 h mobility trace produced by a Multi-Agent Traffic Simulator, which realistically simulates public and private traffic over regional maps of Switzerland. The result is a *Chains of Trust* simulation with over 260,000 nodes, which shows that the proposed scheme performs satisfactorily in a realistic scenario.

1. Introduction

With the massive deployment of wireless technologies on motorized vehicles, the automotive industry has opened a wide range of possibilities for drivers and passengers alike: theoretically, anything from finding out the road conditions ahead to watching a movie through streaming is possible. So different requirements will lead to the deployment of different kinds of applications over the network. In [1,2] applications are classified based on the service they provide:

1. Safety related applications:
   (a) *Traffic information messages*: used to disseminate traffic conditions over an area; they affect public safety only indirectly (they are not time-critical).
   (b) *General safety-related messages*: used by public safety applications such as cooperative driving and collision avoidance (in order to prevent traffic accidents time is certainly an issue; at least they should satisfy an upper bound delay in delivering the information).
   (c) *Liability-related messages*: they are only exchanged in liability-related situations such as accidents. The senders' identities should be kept hidden from the other users in the network and only revealed to the law authorities (time is not an issue).
2. Other applications (some examples):
   (a) *Toll applications*: electronic toll collection systems like *AutoPASS* in Norway allow drivers to continue driving without having to stop at tolls.
   (b) *TV and other multimedia content*: used to provide users with entertainment and information (movies, newspapers, etc.).
   (c) *Advertisements*: businesses along the road (such as gas-stations and restaurants) could advertise themselves to drivers before they reached their location, giving them enough time to compare different offers.

* Corresponding author. Tel.: +34 93 405 40 44.
E-mail address: antolino@ac.upc.edu (D. Antolino Rivas).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2012.02.011

Messages from safety applications should ensure their integrity and their non-repudiation albeit maintaining at the same time the user's privacy. Other applications may also need to encrypt their traffic to transmit sensitive information, whereas that may be unnecessary for applications in the first group.

Architecture wise, applications can also be divided in two groups. On one hand, there are *Zero-infrastructure applications* where the only hardware requirement is the installation of *On Board Units* (OBUs) in the vehicles. OBUs provide the vehicles with sensing, processing and wireless communication capabilities for *Vehicle to Vehicle* (V2V) communications, like in [3]. On the other hand, there are applications that also need *Road Side Units* (RSUs) to provide a *Vehicle to Infrastructure* (V2I) link, generally because they use *Public Key Infrastructure* (PKI) and they require access to a *Certification Authority* (CA) outside the network or to an Internet Service Provider [4–11]. However, with the recent development of cellular technologies like GPRS and UMTS the V2I link could by provided by the OBU itself, minimizing the dependency on road side infrastructure.

This article presents *Chains of Trust*, a secured *Zero-infrastructure* dissemination scheme based on a reputation system, focused on the distribution of *Points of Interest* (POIs) information.

Briefly summarized, every user or vehicle creates its own pair of public and private keys (of length *L*), and is responsible for its private key securing; the protocol does not require a CA. When users visit POIs they evaluate them and input their reviews into the system. The private key is used to sign those POI reviews, whereas the public key is attached to the transmitted information so that the rest of the network can verify the signatures.

The remainder of this work is organized as follows. In Section 2, several solutions to distribute information in VANETs are presented. Section 3 describes *Chains of Trust* in further detail, followed by a description of the simulation tool *poiSim* in Section 4 and the experimentation results in Section 5. Finally, the article closes with the conclusions drawn from those results.

2. Related work

This article introduces an information dissemination technique, which to the best of our knowledge is the first one to build a reputation scheme using user signatures to distribute *Points of Interest* (POIs) information in a *Vehicular Network* (VANET).

Nevertheless, there are other works that consider the distribution of content in VANETs. For instance, in [12] the authors describe a protocol for the distribution of advertisements. They propose a virtual cash scheme where the following actors are involved:

- *Certification Authority* (CA): every vehicle is loaded with a pair of keys (public and private) issued by a CA and with the CA's public key.
- *Vehicular Authority*: entity that approves every advertisement to be loaded in an *Ad Distribution Point*.
- *Ad Distribution Point*: broadcasts advertisements to the vehicles passing by.
- *Virtual Cashiers*: users are rewarded with virtual cash for forwarding advertisements. They sign each other receipts to prove the message forwarding. Later on, that cash can be exchanged for other services at the *Cashiers*.
- *Road Side Units* (RSU): provide a link to the CA for keys revocation purposes.

In [13] the authors present Roadcast, a popularity aware P2P content sharing scheme. Their technique relies on the idea that by ensuring that popular data is widely shared with other vehicles the overall query delay can be improved. If users request popular data, which is densely disseminated in the network, their queries can be answered in much shorter time than a request for rare data, because the chance of meeting another vehicle with that particular piece of information is much higher. In the opportunistic and unreliable VANET, the authors expect users to be more willing to receive data which approximately matches their request with a short delay than waiting for a longer time to receive exactly what they requested. Thus the need to forward the popular information with higher priority.

Data aggregation is another aspect of *Chains of Trust* that should be taken into consideration, since the number of POI and user reviews is so large. In [8], the authors detail several signature techniques to achieve data aggregation:

1. *Concatenated signatures*: each user's signature is appended (together with his certificate) to the original message. The greatest benefit, in contrast to other schemes, is that an invalid signature does not affect the whole message.
2. *Onion signatures*: every user signs the last user's signature and appends his certificate to the message. This technique is very good in terms of data aggregation, since not only the data, but also the signatures are aggregated. However, a single invalid signature could corrupt the whole message.
3. *Hybrid signatures*: several concatenated onion signatures, each of a given depth. This solution looks for a compromise between the previous two, both on their advantages and drawbacks.

Onion and hybrid signatures achieve better aggregation, which means that users can transmit more information in their messages. However, whenever the number of reviews in a message reaches its maximum size the chain of

Table 1
Percentage of received broadcasts for every simulated scenario.

Percentage of received broadcasts					
Number of packets/ period	60	120	180	240	300
100	95.97	97.99	98.62	98.96	99.15
200	91.57	95.91	97.27	97.93	98.38
300	86.86	93.72	95.82	96.87	97.54
400	82.16	91.50	94.37	95.78	96.64
500	77.23	89.28	93.01	94.80	95.85
600	71.93	87.00	91.57	93.73	94.98
700	66.30	84.58	90.03	92.57	94.06
800	60.54	82.19	88.51	91.48	93.22