Computer Standards & Interfaces 36 (2013) 188–197

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

A collaborative protocol for anonymous reporting in vehicular ad hoc networks

Carolina Tripp Barba, Luis Urquiza Aguiar, Mónica Aguilar Igartua, Javier Parra-Arnau, David Rebollo-Monedero, Jordi Forné *, Esteve Pallarès

Department of Telematics Engineering, Universitat Politècnica de Catalunya (UPC), C. Jordi Girona 1-3, 08034 Barcelona, Spain

ARTICLE INFO

Article history:
Received 4 December 2012
Received in revised form 15 April 2013
Accepted 14 June 2013
Available online 22 June 2013

Keywords:
Anonymous reporting
Anonymous-communication systems
Crowds protocol
Multi-hop routing
Vehicular ad hoc networks

ABSTRACT

Vehicular ad hoc networks (VANETs) have emerged to leverage the power of modern communication technologies, applied to both vehicles and infrastructure. Allowing drivers to report traffic accidents and violations through the VANET may lead to substantial improvements in road safety. However, being able to do so anonymously in order to avoid personal and professional repercussions will undoubtedly translate into user acceptance. The main goal of this work is to propose a new collaborative protocol for enforcing anonymity in multi-hop VANETs, closely inspired by the well-known Crowds protocol. In a nutshell, our anonymous-reporting protocol depends on a forwarding probability that determines whether the next forwarding step in message routing is random, for better anonymity, or in accordance with the routing protocol on which our approach builds, for better quality of service (QoS). Different from Crowds, our protocol is specifically conceived for multi-hop lossy wireless networks. Simulations for residential and downtown areas support and quantify the usefulness of our collaborative strategy for better anonymity, when users are willing to pay an eminently reasonable price in QoS.

1. Introduction

Road safety has become an important issue for governments and vehicle manufacturers in the last twenty years. Vehicular ad hoc networks (VANETs) [1] have recently emerged as a platform to support intelligent inter-vehicle communication to improve road safety. VANETs aim to provide vehicles and roads with capabilities to make roads more secure and to make driving time on the road more enjoyable, enabling communications among nearby vehicles (vehicle-to-vehicle communication) as well as between vehicles and nearby fixed equipment (vehicle-to-infrastructure communication). Concordantly, intelligent transportation systems (ITSs) have appeared to leverage the power of modern communication technologies, applied to both vehicles and infrastructure, in order to improve road safety.

Allowing drivers to report traffic accidents and violations through the VANET may lead to substantial improvements in road safety. Being able to do so anonymously in order to avoid personal and professional repercussions will undoubtedly increase user acceptance of such valuable service. Consider for example the potential risk incurred by a user who files a complaint against somebody who is also responsible for processing the corresponding violation. If such complaint were not anonymous, the reported individual may attempt to take action against the reporting user. Not to mention the fact that user behavior may be profiled on the basis of location and other sensitive information contained in the report.

Particularly in ad hoc networks, users may prefer not to place their trust on intermediaries such as anonymizing proxies [2] and mix networks [3,4]. Privacy-enhancing technologies based on user collaboration avoid the need for these trusted third parties (TTP). On the other hand, it is crucial that the anonymity-enforcing mechanisms implemented be aware of their impact on network performance that translates into quality of user experience (QoE). Although there exists a number of collaborative anonymity systems in the literature [5,6], to the best of our knowledge none of them is perfectly suited to the specific requirements of vehicular networks highlighted here.

With these challenges in mind, the main objective of this paper is to propose a new collaborative protocol for enforcing anonymity in multi-hop VANETs. The approach here presented is closely inspired by Crowds [5], a protocol according to which each user probabilistically decides to send a message directly to a common receiver, or else to forward it to a peer, who is asked to repeat the process. Our protocol differs from the original Crowds in that, first, it does take into account transmission losses, and secondly, it is specifically conceived for multi-hop VANETs, rather than for wired networks. Precisely, this second difference makes our approach dependent on the underlying multi-hop routing protocol, since the authority processing the reports may not be within communication range of every user. Motivated by this, this work assesses the suitability of our approach in combination with two standard routing protocols, AODV [7] and GPSR [8], and under two urban scenarios. Our extensive performance

* Corresponding author. Tel.: +34 93 401 1871.
E-mail addresses: ctripp@entel.upc.edu (C.T. Barba), luisfelipe@lfurquiza.com (L.U. Aguiar), monica.aguilar@entel.upc.edu (M.A. Igartua), javier.parra@entel.upc.edu (J. Parra-Arnau), david.rebollo@entel.upc.edu (D. Rebollo-Monedero), jforne@entel.upc.edu (J. Forné), esteve@entel.upc.edu (E. Pallarès).

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.06.001

evaluation contemplates not only privacy, but also the impact on quality of service (QoS) of the privacy mechanism. On the one hand, QoS is measured in terms of packet loss, end-to-end delay and average number of hops; on the other, we measure anonymity as the attacker's probability of error when guessing the identity of the sender, in keeping with [9].

Section 2 examines the state of the art on anonymous-communication systems and reviews the routing protocols AODV and GPSR. Section 3 first describes the adversary model and anonymity metric assumed in this work. Afterwards, this section presents our anonymous-reporting protocol. Then, Section 4 is entirely devoted to the empirical evaluation of our approach under two distinct urban scenarios. Finally, conclusions are drawn in Section 5.

2. State of the art

As stated previously, our main contribution is an anonymous-reporting protocol that, on the one hand, is inspired by the anonymous-communication protocol Crowds [5], and on the other, builds on a *generic* multi-hop routing protocol. In this section, we first provide a broad perspective of anonymous-communication systems, and secondly, describe in detail two widely-used routing protocols, one of them intended for mobile ad hoc networks, and the other specifically conceived for vehicular networks.

2.1. Anonymous-communication systems

In this subsection, we explore the underlying technologies of anonymous-communication systems. With this aim, we examine those systems based on the original mix devised by Chaum, and afterwards, analyze Crowds, a popular collaborative protocol for anonymous Web transactions.

In anonymous communications, one of the goals is to conceal who talks to whom against an adversary who observes the inputs and outputs of the anonymous communication channel. Mix systems [10,3,11] are nodes that forward messages so that it is unfeasible for an attacker to link an outgoing message to its corresponding input message. The idea behind Chaum's mix [3] is conceptually simple. Users wishing to submit messages to other peers encrypt the intended recipients' addresses by using public key cryptography and send these messages to the mix. The mix collects a number of these encrypted messages and stores them in its internal memory. Afterwards, these messages are decrypted and the information about senders is removed. In a last stage, when the number of messages kept reaches a certain threshold, the mix forwards *all* these messages to their recipients in a random order.

In the literature, this process of collecting, storing and forwarding messages when a condition is satisfied is normally referred to as a *round*. An important group of mixes called *pool* mixes operate on this basis. Depending on the *flushing* condition, we may distinguish different types of pool mixes. Possibly, the most relevant form of pool mixes are *threshold* pool mixes [10], where the condition is imposed on the number of messages stored, as in the case of Chaum's mixes. The main difference is that threshold pool mixes do not flush all messages in each round, but keep some of them. Clearly, this strategy degrades the usability of the system—any incoming message can be stored in the mix for an arbitrarily long period of time. But on the other hand these systems achieve a better anonymity protection. The reason is that the set of possible incoming messages linkable to an outgoing target message increases substantially, as it includes all messages that entered the mix before this target message was flushed.

Another important group of pool mixes outputs messages based on time [12]. Essentially, these *timed* mixes forward all messages kept in the memory every fixed interval of time called timeout. The major advantage of these mixes is that the delay experienced by messages is upper bounded, in contrast to the case of threshold pool mixes. The flip side is that the unlinkability between incoming and outgoing messages may be seriously compromised when the number of messages arriving in that interval of time is small. Motivated by this, some of the current mix designs implement a combination of the strategies based on threshold and those based on time. Namely, these systems flush messages when a timeout expires, provided that the number of messages stored meets a threshold [13].

The use of networks of mixes has also been thoroughly studied in the literature. The reason is evident—on the one hand, routing messages through several mixes makes it more difficult for an attacker to track messages, and on the other hand, it improves the availability of the anonymous-communication system. Depending on the network topology, we may classify the existent approaches into *cascade mixes*, *free-route networks* and *restricted-route networks*. The application of cascade mixes was already suggested by Chaum in his original work [3]. Fundamentally, this approach contemplates the concatenation of mixes to endue the system with higher robustness. In contrast to this alternative where messages are routed through a fixed path, free-route networks recommend that users choose random paths to route their own messages [14]. In the end, restricted-route networks consider the case where every mix in the network is connected to a reduced number of neighboring mixes [15].

Apart from the systems based on mixes, other approaches attempt to anonymize the communication channel by relying on user collaboration. A protocol for enhancing privacy in communications, relying on user collaboration and message forwarding, is [6]. The objective of the cited work is to obfuscate the relationship between user identities and query contents even from the intended recipient, an information provider. The main difference with respect to a protocol such as Crowds is that instead of resorting to probabilistic routing with uncertain path length, it proposes adding a few forged queries [16]. In the application scenario of location-based services, users submit queries along with the location to which those queries refer. An example would be the query “Where is the nearest Italian restaurant?”, together with the geographic coordinates of the user's current location. In this context, [17] proposes a peer-to-peer spatial cloaking algorithm whereby users send their queries to an untrusted LBS provider without disclosing their precise location. The authors propose using k-anonymity as privacy metric. Accordingly, when a user wishes to submit a query to the provider, first they must find a group of k-1 neighboring peers willing to collaborate. Once the group is formed, the originator of the query computes a geographical region including all users belonging to the group. After that, the user in question selects uniformly at random one of the members of the group. Ultimately, the originator sends both the query and the coordinates of that region to the selected user, which in turn is responsible for forwarding this information to the LBS provider on their behalf.

The use of pseudonyms as well as the encryption of IP addresses are two alternatives to provide anonymous communications in VANETs. In [18], the authors analyze the challenges to apply pseudonymity in VANET communication systems. They present a feasible multi-layer addressing scheme with support for pseudonymity, which provides privacy guarantees at the different layers. Their proposal enhances the packet forwarding based on the use of pseudonym id's and the use of a location service capable of working with periodic changing pseudonyms. The main issue with this approach is that it requires all addresses (pseudonyms id's) across a node's protocol stack be changed at the same time. This is controlled by software in their proposed scheme. The authors conclude that the costs of pseudonymity in terms of delay can be decreased. The authors provide an implementation showing a low impact on the overall performance and a reasonable trade-off between the driver's privacy and deployability of changing pseudonyms. The authors in [19] present a novel privacy addressing-based anonymous communications (PAAC). It is an end-to-end solution based on privacy addressing for VANETs which combines privacy addressing and public key cryptography to improve the privacy and security of vehicles. The paper focuses