Computer Communications 46 (2014) 29–42

Contents lists available at ScienceDirect

Computer Communications

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

A secure alert messaging system for safe driving

Wafa Ben Jaballah [a,*], Mauro Conti [b], Mohamed Mosbah [a], Claudio E. Palazzi [b]

[a] University of Bordeaux, Polytechnic Institute of Bordeaux, LaBRI, CNRS, UMR 5800, France
[b] Department of Mathematics, University of Padua, Italy

ARTICLE INFO

Article history:
Available online 8 April 2014

Keywords:
Inter-vehicular communication
Vehicular safety
Alert messaging warning
Position cheating attack

ABSTRACT

Vehicular safety is an emergent application in inter-vehicular communications. As this application is based on fast multi-hop message propagation, including information such as position, direction, and speed, it is crucial for the data exchange system of the vehicular application to be resilient to security attacks. To make vehicular networks viable and acceptable to consumers, we have to design secure protocols that satisfy the requirements of the vehicular safety applications. The contribution of this work is threefold. First, we analyze the vulnerabilities of a representative approach named Fast Multi-hop Algorithm (FMBA) to the position cheating attack. Second, we devise a fast and secure inter-vehicular accident warning protocol which is resilient against the position cheating attack. Finally, an exhaustive simulation study shows the impact of the attack on the protocol FMBA on delaying the transmission of alert messages. Furthermore, we show that our secure solution is effective in mitigating the position cheating attack.

1. Introduction

Annually, road crashes result in almost 120,000 fatalities and 2.4 million injuries in the European Region [1]. Road traffic injuries represent the leading cause of death among adolescents and young adults. Moreover, the economic burden of road crashes is as much as 3% of gross domestic product. Although, many potential preventive strategies exist [2], they are not completely effective. Hence, it is desirable to take up the challenge and reduce the burden of road traffic injuries. The basic approach consists in using advanced technologies that can prevent vehicles from being involved in accidents. In this direction, one of the most promising techniques is based on the use of inter-vehicular communication (IVC) [3]. In fact, many applications are possible in this context, yet local danger warning systems remain the most prominent ones. Clearly, the effectiveness of such safety related application is based on the reliability of the broadcast information.

Alert messaging is a building block component of intelligent transportation systems and an emergent application for vehicular communications. Vehicles can communicate between each other, without needing the intervention of any external communication infrastructure. However, to effectively broadcast an alert message from a vehicle involved in an accident to all the following vehicles in the car platoon, the transmission of the message should be done as quickly as possible.

Current approaches are generally based on intermediate neighboring nodes, since the transmission of the alert message through infrastructures on the road would add delays that could have fatal consequences on life loss, injuries, and vehicle damages. For this purpose, different alert messaging applications have been proposed to broadcast an alert message very fast [4–7]. However, it is crucial for such data exchange to be resilient to security attacks in order not to lose its potential effectiveness in saving lives. Attackers might run malicious actions to inject false information or alarm, thus rendering ineffective the safety application [8–12]. Although many alert message applications have been thoroughly studied in the past years [4–6], most of the obtained results did not take the security threats into account. Instead, the benefits in terms of reduced number of vehicles involved in a chain accident, thanks to a properly working alert message broadcast, is clearly shown by Palazzi et al. [5].

Contribution. In this paper, we review the contribution of [13] and further thoroughly investigate the impact of the position cheating attack on a representative algorithm for alert messaging, i.e., the Fast Multi-hop Broadcast Algorithm (FMBA) [4] for vehicular safety application. First, we highlight the vulnerability of FMBA to the position cheating attack and we study the impact of this attack on this algorithm. We show that this weakness we found could be leveraged by an adversary in a very effective way. Then, we discuss a solution we developed for broadcasting safety related messages, which is both fast and secure against the position cheating attack. We named this solution Secure FMBA and we assessed its effectiveness with a thorough simulation study.

* Corresponding author.
E-mail addresses: wafa.benjaballah@labri.fr (W. Ben Jaballah), conti@math.unipd.it (M. Conti), mosbah@labri.fr (M. Mosbah), cpalazzi@math.unipd.it (C.E. Palazzi).

http://dx.doi.org/10.1016/j.comcom.2014.03.010
0140-3664/

Organization. This paper is organized as follows. The next section presents the notation and model assumptions. Section 3 reviews the proposed solutions in the literature, and provides the necessary background information related to the FMBA protocol. In Section 4, we show the vulnerability of FMBA to the position cheating attack. In Section 5, we present our position verification method. In Section 6, we evaluate the performances of FMBA under different position cheating attacks, and Secure FMBA with position cheating detection. Finally, in Section 7 conclusions are drawn.

2. Notation and model assumptions

In this section, we present the assumptions and the notation (Table 1) used in this paper. In our model, we assume that one malicious vehicle is on the network, in order to show the impact of the attack with a minimum number of attackers. We did not assume and model the presence of obstacles or buildings along the road. We considered a symmetric communication range: if a verifier vehicle *V* hears a verified vehicle *P*, then we can also assume that *P* can hear *V*.

Moreover, we assume that *V* does not know in advance its transmission range and that it communicates directly with the prover node *P*. Each vehicle knows its own location, for instance, using GPS that provides accurate information about current time and actual position. All the vehicles belong to a Public Key Infrastructure [14,15]; i.e., each vehicle has a public/private pair of keys and a unique identity certified by a Certification Authority. We assume that the certification authority corresponds to the government agency responsible to assign license plates: a vehicle can be used only if it is provided with a unique license plate, a PKI certificate associated to its plate ID, and the public key of the Certification Authority. We assume also that certificate revocation lists are updated at given time interval (e.g., daily) by the vehicle and stored in a local memory. The power and computational resources are supposed to be large enough for our application's requirements, and the network is loosely time synchronized.

3. Related work

The past decade has witnessed a growing interest in inter-vehicular communication (IVC) and its panoply of potential applications [16,17]. IVC enables a vehicle to communicate with other vehicles, both directly and in a multi-hop fashion. Minimizing the broadcast delivery time is one of the main challenge for IVC. In the literature, it has been proven that this broadcast time is strictly related to both the number of relays of the messages (hops) and the network congestion [4,6].

Table 1
Notation.

Symbol	Definition
CMBR	Current Maximum Back Range
CMFR	Current Maximum Front Range
LMBR	Latest-Turn Maximum Back Range
LMFR	Latest-Turn Maximum Front Range
MaxRange	How far the transmission is expected to go backward before the signal becomes too weak to be intelligible
d	Distance between two vehicles
CW	Contention Window
CWMax	Maximum Contention Window
CWMin	Minimum Contention Window
TR	Transmission Range
Hello	Hello message
drm	Declared transmission range in the *Hello* message
P	The prover vehicle
V	The verifier vehicle
R	The geographical region

In order to minimize the number of hops that a message experiences during its propagation over the network, the approach in [18] assigns different contention windows to each vehicle receiving the message. The contention windows of the vehicles are inversely proportional to the distance from the previous sender. Each of these vehicles randomly selects a waiting time within its contention window before forwarding the message. These approaches generally assume a unique, constant and well-known transmission range for all vehicles; unfortunately, this assumption is not realistic [4].

In [4], the authors propose a fast broadcast algorithm (FMBA). It aims at reducing the number of hops traversed by a message, in order to minimize its propagation delay. Vehicles in a car platoon dynamically estimate their transmission range and exploit this information to efficiently propagate a broadcast message with as few transmissions as possible. In essence, the farthest vehicle in the transmission range of a message sender or forwarder will be statistically privileged in becoming the next (and only) forwarder. In [6], authors have enhanced the fast broadcast algorithm using heterogeneous transmission range. Unlike [4], the authors select the forwarder of the message as the vehicle which transmission spans farther. In [6], the forwarder of a message is not chosen as the farthest vehicle in the transmission range of the sender.

The problem of providing security in vehicular communications has been a roadblock to their large scale deployment; yet it is still in its infancy. Accurate information on position is crucial for IVC based vehicular safety applications. In particular, several multi-hop broadcast algorithms have been proposed [4,6,19] without security in mind, whereas security is a fundamental problem in this context which should not be overlooked. Indeed, attackers might run malicious actions to inject false information or alarm, thus rendering ineffective the safety application [10]. To this aim, detection mechanisms have been proposed in this context to recognize nodes cheating about their location [20,21]. Position verification approaches can be grouped into two main categories [20]: infrastructure based and infrastructure-less based approaches.

3.1. Infrastructure based approach

This class of approaches is based on special hardware dedicated infrastructure to verify the position of other vehicles. Some verification approaches are based on distance and angle estimation techniques. These techniques include time difference of arrival, time of arrival, received signal strength, and angle of arrival [22]. However, these methods are not secure in presence of attackers. In [23], the authors propose range-free protocols that do not require distance or angle measurements, but are also insecure in adversarial environments. The technique of distance bounding does not prevent an attacker from declaring a position farther away than it really is [24]. Moreover, in [25], they assume that each verifier is trusted, which is not realistic.

The solutions in [20] use multiple sensors to monitor and calculate trust values for position information. There are two classes of position verification sensors: autonomous and cooperating sensors. In fact, autonomous sensors work autonomously on each node and contribute their results to the overall trust ratings of neighbors. Cooperating sensors use the information exchange between the neighbors to verify positions. The solution in [26] uses verifiers at special locations. This solution needs specific infrastructure: the verifiers. These verifiers attempt to verify location claims for region *R* that are "near" a verifier *V*.

In [21], the proposed solution depends on two directional antennas. Each vehicle periodically sends a message containing its location together with its own two lists of front and back neighbors. A vehicle decides on the relative positions of its one-hop neighbors based on the messages it receives.