Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Controlling and filtering users data in Intelligent Transportation System

Catalin Gosman [a], Tudor Cornea [a], Ciprian Dobre [a], Florin Pop [a,*], Aniello Castiglione [b]

[a] University Politehnica of Bucharest, Splaiul Independentei 313, Bucharest, Romania
[b] University of Salerno, Via Giovanni Paolo II, 132, I-84084 Fisciano (Salerno), Italy

HIGHLIGHTS

- Data sharing policies for users' personal information, captured by an ITS.
- Quantify the level of trust for the users' information retrieved from an ITS.
- Quality parameters: spatial accuracy, temporal closeness, source's reputation.
- Security and privacy-aware model designed for ITS applications.
- Evaluate a pilot security implementation under real-world assumptions.

ARTICLE INFO

Article history:
Received 13 April 2016
Received in revised form
30 October 2016
Accepted 11 December 2016
Available online 23 December 2016

Keywords:
Privacy
ITS
Data sharing
Trust in information

ABSTRACT

Intelligent Transportation Systems (ITS) provide mechanisms so that users are better informed in order to use efficiently the existing and future transportation capabilities. However, in order for ITS to be helpful and reliable in real-life situations, security and privacy considerations have to be taken into account. Users are contributing with data captured from private sensors, raising privacy risks when sharing this within the ITS context. For example, GPS data can facilitate the construction of ITS services for route discovery, but in the same time malicious users can use the information in order to derive location patterns and geographical habits. Several ITS companies could gain interesting insights about the traffic and safety events, if they put together owned private data. However, at this moment, the security risks prohibit such an endeavor. In this paper, we illustrate a security model where ITS participants can specify how data sharing captured by an ITS application will behave in regards to their own privacy requirements. The proposed solution is able to mediate the differences between ITS applications needs regarding data usage under various context based constraints and user focused constraints defined using security policies for their shared data. The next topic discussed in the paper is our proposal of an appropriate ITS mechanism that manages to establish the level of trust in the information disseminated in the system. The trust level mechanism is used in order to decide whether an ITS event should be are advertised or not to other users or ITS applications. In systems like ITS that are dynamic and changing frequently, trust in shared data must be calculated taking into consideration both the contextual information disseminated in the system, but also the sources' reputation. Our proposals' evaluations is done using ITS implementations in real-world conditions.

1. Introduction

ITS provide benefits in many areas of transportation, having contributions in the construction of new models of traffic, reducing congestion times, making traffic safer. In order to be effective, ITS applications rely on large volumes of information provided by different traffic and infrastructure sensors, but also on information sent by the participants that willingly participate in the process of data collection. Some of the most popular ITS applications today (e.g. Waze, Google Traffic) are being developed by companies that offer little to no transparency regarding the collection information process from their users. Their applications are not interconnected with the ones of other vendors, they have non-standardized

[*] Correspondence to:.
E-mail addresses: catagosman@gmail.com (C. Gosman), tudor.cornea@cti.pub.ro (T. Cornea), ciprian.dobre@cs.pub.ro (C. Dobre), florin.pop@cs.pub.ro (F. Pop), castiglione@ieee.org (A. Castiglione).

http://dx.doi.org/10.1016/j.future.2016.12.014
0167-739X/© 2016 Elsevier B.V. All rights reserved.

data formats, most of the times their solutions are proprietary and closed-source. Users contributing to such ITS services have no control in the data sharing process, they do not have any mechanisms to protect their sensitive information from being reveled or not. For example, location traces can disclose the users' habits and their driving preferences. Therefore, sharing data becomes an intrusive process when thinking of ITS users' privacy demands. Users and ITS applications must be transparent when deciding who is the beneficiar of the data collection process, but also in regards to the circumstances that define how the sensitive information can be used by ITS applications. Most of today's ITS applications do not provide any mechanisms for users to control or influence the data collection and sharing process [1–4]. Participants contributing with their collected data in such ITS lose control over their own shared information.

First of all, the paper proposes a mechanism that provides ITS participants the means to specify their own data sharing policies when contributing with collected info for an ITS service/application. The security policies make use of different fields from the information collected like timestamp, location, possible speed etc., combine them using logical operations in order to create logical filters that specify data sharing policies. To put in practice the model proposed, we have implemented an ITS routing application that demonstrates how data sharing policies defined in the mobile clients influence the data collection process in an ITS application.

Second, our interest is finding a solution to quantify the level of trust for the information the users get back from the ITS for personal use. In order to construct an ITS service/application that provides reliable results to its users, information quality is an important factor that must be taken into consideration. In order to decide whether or not to use the shared data, the information in use must meet certain conditions: it should reflect the true state of the ITS context, it should contain all the necessary fields that are relevant for the creation of the ITS service/application, it should be consistent with the general information provided by other ITS participants. Information published by an ITS application/service is useless as long as neither the ITS users, neither the ITS service can determine if it is trustworthy or not. Therefore, our proposal for establishing whether ITS information is trustworthy or not is based on the quality parameters of the data disseminated, like: geographical closeness, temporal accuracy, aggregated with the reputation of the participants that share data about a particular ITS event.

In addition to the article published [5], the paper brings the following contributions:

- a thorough analysis of existing security threats in ITS and how the proposed solutions solves some of the ITS security requirements.
- theoretical demonstration for the proposed security policies applicable in ITS.
- complex experimental scenarios that evaluate the proposed mechanism that establishes how trustworthy is the shared information in ITS.

The paper has the following structure: In Section 2 we analyze existing ITS security solutions and see how they relate to our proposed approaches. In Section 3 we make a thorough analysis of existing security threats and available mitigation solutions in ITS. Next, in Section 4 we present our security policy approach, followed by a brief theoretical demonstration in Section 5. In Section 6 we present our mechanism for determining the degree of trust in ITS shared data. The practical implementation with the results are described in Section 7. Section 8 presents conclusions and future work.

2. Related work

In order to construct ITS applications that can intercooperate and become of real use for traffic participants, we need to identify and solve the security problems existing in ITS. In what follows, we present some existing approaches that are trying to mitigate the security challenges specific in ITS.

PEPSI [6] developed a privacy solution based on a cryptographic approach. The solution is constructed around an offline actor, the Registration Authority, that does not interfere with in participants' actions, like Mobile Nodes or other Queriers, or in privacy matters. Reports and queries passed in the system are encrypted using public key encryption in order to be protected from malicious attackers. Nodes can encrypt sensed data using reports labels with the (public) encryption key. The private decryption keys are obtained from the Registration Authority. The Service Provider sends the reports to the Queriers to find out about their information of interest. In order to do this, Queriers need to possess the decryption keys. To address the decryption overhead at the Querier level, they apply a tagging mechanism on Mobile Nodes reports. Tags are computed using the same labels used to derive encryption keys. Similarly, Queriers compute tags for the labels defining their interests (using the corresponding decryption keys) and provide them to the Service Provider at query subscription. The main disadvantage of this approach is the Registration Authority that acts as a single point of failure. If it gets compromised, attackers manage to identify users and contextual information requests. Therefore, PEPSI schema becomes vulnerable to attacks targeted on compromising the Registration Authority.

For the development of a secure system, authors in [7] proposed a modular concept, divided into several layers. The lowest layer is in charge with nodes' registration, i.e. the mapping of the owner to its identifier. The test and certification layer evaluates the validity of nodes' operations. The operation validity is guaranteed by digital nodes certificates. The test and certification process determines unauthorized accesses in the system. The pseudonym layer gives user the possibility to use pseudonyms in order to fulfill their anonymity requirements. The revocation layer is concerned with excluding nodes from the system. If node revocation becomes an issue, additional mechanisms must be set in place to ensure that the node is revoked. Besides this, node-local detection and reaction is necessary to minimize the impact of malicious or malfunctioning nodes.

Having a mechanism that helps ITS users share data according to their own privacy needs, the research efforts have been concentrated on finding a way to establish whether or not the shared data is trustworthy so that it can be used in the development on ITS services/applications. Various techniques have been identified in the literature: majority principle, the most trustworthy source principle (can isolate and identify participants that look more "trustworthy" than others), Bayesian inference, Dempster–Shafer theory. Dempster–Shafer theory is defined by the fact that ITS participants are able to transmit information about ITS events with a certain degree of uncertainty, while the Bayesian inference is constructed using a binary approach: participants can only confirm or infirm the ITS events.

Our experimental results have been obtained in the context of the MobiWay and DataWay projects. For purposed of the Mobiway project is to build an interconnection ITS platform that brings together ITS entities (systems, applications, users) willing to contribute with data in order to introduce new ITS services or maintain existing one. Collected data is stored in users/groups specific logic storage facilities called Data Vaults. The purpose of the Data Vaults is to provide control by means of restricting access to the information using security policies. Before ITS services/applications can process or extract data, the