Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems

Stylianos Gisdakis, Vasileios Manolopoulos, Sha Tao, Ana Rusu, and Panagiotis Papadimitratos

***Abstract*—Increasing smartphone penetration, combined with the wide coverage of cellular infrastructures, renders smartphone-based traffic information systems (TISs) an attractive option. The main purpose of such systems is to alleviate traffic congestion that exists in every major city. Nevertheless, to reap the benefits of smartphone-based TISs, we need to ensure their security and privacy and their effectiveness (e.g., accuracy). This is the motivation of this paper: We leverage state-of-the-art cryptographic schemes and readily available telecommunication infrastructure. We present a comprehensive solution for smartphone-based traffic estimation that is proven to be secure and privacy preserving. We provide a full-blown implementation on actual smartphones, along with an extensive assessment of its accuracy and efficiency. Our results confirm that smartphone-based TISs can offer accurate traffic state estimation while being secure and privacy preserving.**

***Index Terms*—Privacy, security, traffic information systems.**

I. Introduction and Background

TRAFFIC congestion deteriorates the quality of life of citizens and contributes significantly to environmental pollution and economic loss. Traffic information systems (TISs) aim at solving this problem by collecting traffic data, producing traffic estimates, and providing drivers with location-specific information. The increasing smartphone penetration, along with the wide coverage of cellular networks, defines an unprecedented large-scale network of sensors, with extensive spatial and temporal coverage, able to serve as traffic probes for TISs.

To reap the benefits of smartphone-based TISs, users must participate in large numbers. Ideally, anyone possessing a smartphone should contribute to the TIS. Nevertheless, this very openness of such systems renders them vulnerable to adversaries and malicious users. It is thus necessary to secure the collection of data and render the contributing users (smartphones) accountable. This is a task that cannot be achieved only by relying on the security of the mobile-to-cellular infrastructure communication.

At the same time, as TISs require fine-grained location information, the privacy of the contributing participants must be protected. This need for privacy is intensified in the context of smartphone-based TISs. Smartphones already reveal a great deal of, possibly sensitive, information to the cellular operators (e.g., user identity, coarse-grained location, and calling/messaging actions among others). Thus, it is important that the introduction of smartphone-based TISs does not, under any circumstances, deteriorate user privacy.

These points define a challenging tradeoff; although users should be able to participate in the system in an anonymous manner, they should be held, at the same time, fully accountable for their actions. Furthermore, the introduction of security and privacy protection mechanisms should neither deplete the user platform resources (i.e., computation resources, battery, and bandwidth) nor should it come at the expense of the TIS's efficiency and accuracy.

Balancing security, privacy, effectiveness and efficiency is not straightforward. In most cases, the literature considers the aforementioned aspects separately, either overlooking security and privacy and focusing on the traffic estimation aspects of TISs or considering security and privacy without evaluating their effect on the efficiency and the accuracy of the TIS. This sets the challenge ahead: *Can we leverage smartphones and build efficient, secure, and privacy-preserving TISs of unprecedented spatial coverage?*

Contributions: We meet this challenge by addressing security and privacy protection aspects of smartphone-based TISs. Moreover, we assess their effect on the accuracy of traffic estimation. More specifically, building on our prior work [1]–[3], we present a smartphone-based TIS and assess its accuracy through Global Positioning System (GPS) traces in the presence of traffic estimation errors and for different values of location reporting rates and accumulation frames. Furthermore, by leveraging cellular providers, existing telecommunication standards and state-of-the-art cryptographic schemes, we propose a comprehensive security and privacy-preserving architecture, resilient against offending users and TISs entities. We formally assess the security and privacy properties of the system and demonstrate its efficiency through extensive evaluations.

This paper is organized as follows. The remainder of this section surveys the literature. Section II presents an overview of our smartphone-based TIS and discusses the sought security and privacy properties. In Section III, we present the proposed architecture protocols. Section IV provides a detailed security and privacy analysis. We evaluate the performance of our system in Sections V and VI. Finally, we conclude in Section VII.

Manuscript received December 3, 2013; revised April 14, 2014, June 27, 2014, and September 18, 2014; accepted October 16, 2014. Date of publication December 18, 2014; date of current version May 29, 2015. The Associate Editor for this paper was Prof. X. Cheng.

S. Gisdakis and P. Papadimitratos are with KTH Royal Institute of Technology, 100 44 Stockholm, Sweden (e-mail: gisdakis@kth.se; papadim@kth.se).

V. Manolopoulos, S. Tao, and A. Rusu are with KTH Royal Institute of Technology, 164 40 Kista, Sweden (e-mail: vama@kth.se; stao@kth.se; arusu@kth.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2014.2369574

A. TISs

State-of-the-practice traffic data collection relies on roadside sensors, e.g., inductive loop detectors (ILDs), to gather information about traffic flow at fixed points on the road network [4], [5]. Although widely accepted, the use of fixed sensors comes with a high deployment cost. Moreover, roadside sensors are deficient in estimating the speed over an entire road link because they measure the speed at the spot of deployment.

The literature also suggests the use of dedicated vehicles, i.e., probe vehicles (PVs), as floating traffic probes [6], [7]. PVs are equipped with GPS receivers and dedicated communication links. A large number of such dedicated vehicles render accurate traffic status estimations feasible [8]. Nevertheless, the cost of having dedicated communication links between the in-vehicle equipment and the traffic management center is still a limiting factor [9]. Moreover, PVs, usually chosen from a particular group of vehicles, e.g., taxis or buses, may provide biased traffic information [10].

Mobile phones are increasingly used for traffic data collection. Smartphone-based road status estimation avoids considerable installation and maintenance costs, both in terms of vehicle equipment and roadside infrastructure. In addition, mobile phones, serving as traffic probes, offer increased coverage (particularly) when compared with dedicated PVs. In the end of 2013, there were approximately 6.8 billion mobile subscriptions [11], corresponding almost to 100% of the world's population. Any mobile phone that is switched on, even if not in use, can act as a probe. Additionally, the sales of smartphones, most of which are equipped with assisted GPS (A-GPS) modules, shows a strong growth; the total shipments in 2012 were 1597 million, thus, making smartphones 32% of all handsets shipped [12].

Past field trials introduced the idea of using mobile phones as traffic probes in TISs [10], [13]–[15]. Nevertheless, they did not consider urban arterial roads. In [10], it was suggested that future research efforts should focus on arterial roads rather than freeways, for which traffic sensors have already been deployed. Nonetheless, this is challenging as arterial roads entail lower traffic volumes with varying speeds, and they are controlled by signals at intersections [6], [14], [16].

Previous works employed network-based probe methods that leverage network signaling information, e.g., handoff information or time/angle (difference) of arrivals. Nevertheless, a few of them were handset based (i.e., using GPS-enabled phones). Handset field trials were held by *Globis Data* [17] and *Mobile Century* [18]. Their results demonstrated that network-based probe systems cannot provide accurate traffic estimations in the case of arterial roads due to their additional complexity. On the other hand, a handset-based mobile probe system could be more suitable for arterial roads; however, this has not yet been verified (by either of the aforementioned field tests). Two points were identified as obstacles toward a large-scale deployment of mobile-phone-based TISs [19]: The communications cost and the slow uptake of GPS-enabled phones. Nonetheless, these obstacles have been bypassed by the increasing capacity of modern cellular networks [e.g., third generation and Long Term Evolution (LTE)] and the current smartphone market share.

B. Security and Privacy Issues

Developing TISs that collect location samples from devices, carried by individuals in their everyday lives, poses serious privacy implications. At the same time, the exchanged data must be trustworthy as the feedback provided by the TIS affects the actual traffic conditions. TISs require strong guarantees with respect to the security of the communications and the privacy of the individuals contributing to the TIS. To this end, *authentication*, *access control*, and *confidentiality* mechanisms must be in place. Moreover, attacks targeting the location privacy of the participating users should be mitigated. Even when location samples are collected in an anonymous manner (thus not revealing the real identity of users), breaching user privacy is still possible. More specifically, successive anonymous location updates from smartphones still reveal spatial and temporal correlations that can be used as indirect identifiers. Such correlations can be exploited by tracking techniques [20], [21] to reconstruct a vehicle's whereabouts and, thus, infer frequently visited places, e.g., home or workplace. In such cases, user deanonymization could be easy. To overcome these threats, path cloaking [22] and privacy-preserving sampling techniques [23] have been proposed. In this paper, we do not consider threats against data sets of location samples; rather, we try to address the problem of securing communications and interactions within the system while removing any direct link between a device and its location.

The Mobile Century team presented a privacy-preserving smartphone-based TIS [18] that leverages a scheme, known as virtual trip lines (VTLs), that defines the road points at which samples should be submitted. Their system comprises a client application running on mobile phones, an ID proxy server, the traffic server, and a VTL generator. The mobile clients and the traffic server, or the VTL generator, communicate through the ID proxy, which is responsible for user authentication. Each location update, submitted by a mobile client, to the traffic server contains the location and the identity of the phone, each encrypted with a different key. The identity of the device is encrypted with a symmetric key known to the ID proxy. Similarly, the location information is encrypted with the public key of the traffic server; thus, it is accessible only by it. These keys are established and installed on the mobile client during its initialization. The scheme achieves privacy under the assumption that the traffic and the ID proxy servers do not collude and it requires a third party for the identity management. This point introduces an extra burden for deployment and requires a third party that establishes trust relations with the clients participating in the TISs.

Vehicular ad-hoc networks (VANETs) are related to TISs. The industry, academia, and standardization bodies [24], [25] have converged to the use of pseudonymous authentication for protecting the location privacy of vehicles [24], [26]–[31]. These ephemeral identities are public/private key pairs, used for identifying and authenticating vehicles both in the context of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [32].

Group signatures provide conditional anonymity and have been proposed for VANETs [33], [34]. In the context of location-based services, a privacy-preserving key management

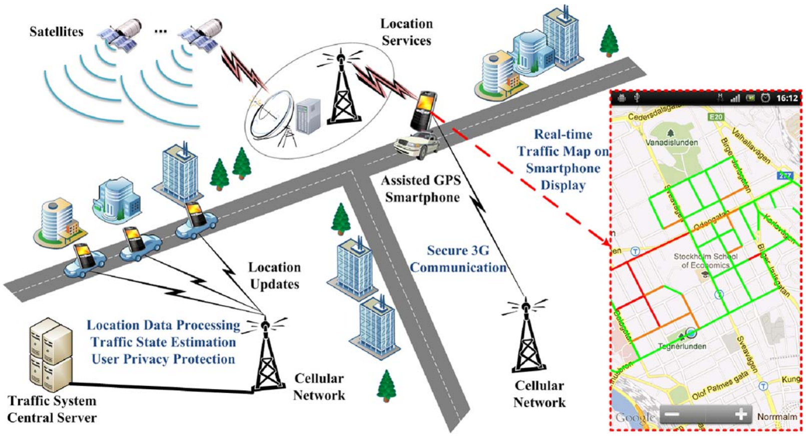


Fig. 1. Overview of a smartphone-based TIS (inspired by [3]).

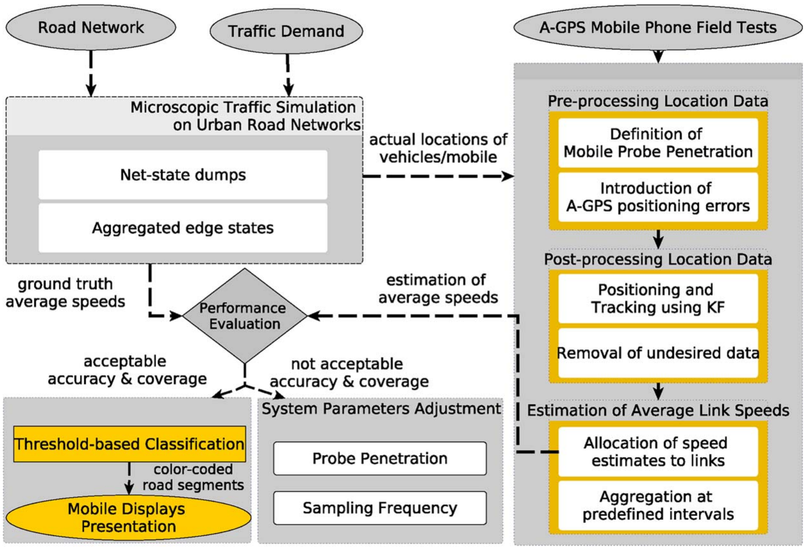

Road Network
Traffic Demand
A-GPS Mobile Phone Field Tests
Microscopic Traffic Simulation on Urban Road Networks
Net-state dumps
Aggregated edge states
actual locations of vehicles/mobile
Pre-processing Location Data
Definition of Mobile Probe Penetration
Introduction of A-GPS positioning errors
Post-processing Location Data
Positioning and Tracking using KF
Removal of undesired data
ground truth average speeds
Performance Evaluation
estimation of average speeds
acceptable accuracy & coverage
not acceptable accuracy & coverage
System Parameters Adjustment
Probe Penetration
Sampling Frequency
Threshold-based Classification
color-coded road segments
Mobile Displays Presentation
Estimation of Average Link Speeds
Allocation of speed estimates to links
Aggregation at predefined intervals

Fig. 2. Traffic estimation component.

scheme for VANETs was proposed in [35]. However, none of these works considers traffic estimation. In [35], roadside unit (RSU)-based communications (not yet broadly deployed) were assumed; here, in contrast, we focus on the existing cellular infrastructure. While RSUs may be a lesser threat to location privacy (e.g., due to limited deployment or functionality), cellular operators maintain detailed connectivity to infrastructure and thus location information. They could even link interactions of a mobile with the TIS, or any other service, by means of unique identifiers such as the International Mobile Subscriber Identity (IMSI) and the International Mobile Station Equipment Identity (IMEI). Even worse, in case cellular providers collude with the TIS server, to which users submit their traffic reports, it is trivial to identify users and completely reconstruct their whereabouts. Finally, smartphone-based TISs can be viewed as an instantiation of participatory sensing (PS) systems, which raise similar security and privacy challenges (see [36]). A number of solutions have been developed for security and privacy protection in PS systems, without leveraging cellular security architecture. We refer the interested reader to a recent work for the state-of-the-art [37].

II. Secure and Privacy-Preserving TISs

Fig. 1 presents an overview of our smartphone-based TIS. The system comprises smartphone clients, equipped with A-GPS receivers, and a traffic estimation server as the back-end infrastructure. An application is installed on each smartphone to report periodically the location of the device to the traffic information server or to query the server for traffic conditions in its proximity. The traffic estimation server processes the client-submitted data and responds to queries with predefined values representing the average speed on every road link in the area of the querying smartphone. These values are classified as traffic congestion levels (i.e., "low," "medium," "high") that are subsequently illustrated with different colors, on top of a map, so that drivers can choose the optimal route (see Fig. 1). Communications between the smartphones and the back-end system are done over the cellular network.

We have developed a simulation framework for traffic estimation leveraging our previous work [1]. This framework emulates smartphone-based urban traffic estimation and has three parts (Fig. 2): a *microscopic traffic simulation*, a *location data processing and speed aggregation* module, and a *performance evaluation and results representation* module. We simulate urban road networks and traffic conditions by generating "actual" location tracks for each vehicle/mobile. The generated location samples are preprocessed and degraded to emulate "realistic" measurements. This preprocessing defines the percentage of vehicles that are equipped with A-GPS mobile phones (according to a penetration rate) and introduces statistical errors to the location updates. Then, the location data are postprocessed by a two-step filtering process. A simple data screening scheme is employed to filter out unexpected position and speed estimates. This filtering process assigns speed estimates to all road links that are later aggregated at predefined time intervals. Based on specified thresholds, the estimated link speeds are classified into several traffic condition levels, illustrated as colored road segments on the smartphone displays (see Fig. 1). The assessment of the accuracy and the coverage of our system are discussed in Section VI.

A. Security and Privacy for TIS

1) Adversarial Model: Smartphone-based TISs are inherently open systems and thus vulnerable to adversarial behavior. We first consider *external adversaries*, i.e., unauthorized entities that try to harm the system operation. Such adversaries can eavesdrop, intercept, and modify the communication of the system entities (see Section III-A). They can also launch jamming attacks, but we do not dwell on such attacks; we rely on the cellular operator for their mitigation.

We also consider *internal adversaries*, i.e., user devices or TIS entities, that exhibit malicious behavior. Malicious or comprised mobile devices might submit faulty traffic reports to pollute the traffic estimation process (e.g., by claiming nonexistent traffic jams or accidents). After a disruptive action, adversaries might repudiate it (e.g., deny having sent a message that falsely indicates an accident). For the infrastructure components, we consider *honest-but-curious system entities* that correctly execute protocols but try to harm the privacy of users, possibly using inference and filtering techniques to reconstruct the whereabouts of vehicles. More than one system entity could collude to harm user privacy.

2) Security and Privacy Requirements: In the presence of such adversaries, the system should satisfy the following security and privacy requirements.

- *Authentication and authorization* (R_1): Only authorized devices shall be able to submit traffic reports or retrieve traffic status updates from the TIS.
- *Anonymity* (R_2): Transactions should be performed in a privacy-preserving manner. More specifically, the TIS should receive guarantees for the eligibility of the device with respect to the TIS service. No information concerning the real identity of the device and, consequently, of the subscriber should leak. Moreover, traffic reports should not be traced back to devices.
- *Report unlinkability* (R_3): Ideally, the TIS should not be able to link reports originating from the same device. However, inference techniques can (with some probability) link anonymous reports from the same device [38]. To this end, the TIS system should render such inference attacks hard.
- *Confidentiality/Integrity* (R_4): The confidentiality and the integrity of the communications between the system entities (i.e., infrastructure and smartphones) should be ensured.
- **Accountability** (R_5): User devices should be held liable for actions disrupting the system operation. The system should provide the necessary means for the identification (deanonymization) and the eviction of faulty devices.[1] After their eviction (revocation of their credentials), offending devices should no longer be able to participate in the TIS.

III. Security and Privacy Architecture

We employ the architecture first presented in [2], based on the Generic Bootstrapping Architecture (GBA) proposed by the 3G Partnership Project consortium. GBA leverages cellular network authentication mechanisms and enables user access to third-party applications and services. In addition to being a widely accepted telecommunication standard, the GBA integrates identification and authentication schemes already deployed by network operators. Furthermore, it integrates universal integrated circuit cards (UICCs) in the authentication process. The tamper-proof properties of these secure modules enhance the trustworthiness of our system. Nevertheless, the GBA does not consider subscriber privacy. To this end, our architecture achieves enhanced privacy protection, by employing state-of-the-art anonymous authentication schemes.

A. System Components and Trust Establishment

- *Mobile device*: A mobile application runs on drivers/ passengers' smartphones. It calculates the location of the smartphone (i.e., via GPS or A-GPS), and it reports it to the TIS server (see Section II).
- *GBA gateway*: The GBA gateway is administered by the cellular operator. It authenticates devices to the cellular network, and sets up security associations between a device and the here introduced group signature center (GSC).
- *GSC*: This authority manages and issues anonymous credentials to the registered users (discussed later in this section). The GSC is an addition to the GBA that permits the creation, distribution, revocation, and management of anonymous credentials.
- *Traffic estimation server*: This entity performs traffic estimation based on the samples submitted by legitimate users. It also exposes the required interfaces that allow authorized users to query for traffic conditions at an area of interest.

Fig. 3 presents an overview of our architecture. When the user launches our mobile application, the device initiates the authentication process with the GBA gateway (see Section III-C). If this process is successful, the mobile device gets authorized by the GSC, and it receives anonymous credentials to protect its privacy. Then, the device can participate in the traffic estimation process by submitting or requesting information.

[1] The detection of faulty behavior is orthogonal to this investigation.

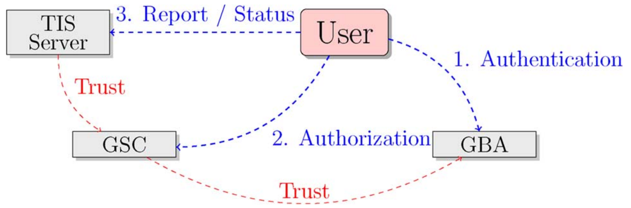


Fig. 3. System overview.

Our goal is to provide authentication while ensuring unlinkability and anonymity of traffic reports. An honest-but-curious TIS server or an outsider getting access to the accumulated data should not be able to map location information to users. Moreover, the mobile operator, which administers the GBA gateway and has access to the user identities, should not be able to retrieve their fine-grained location data.

We establish trust by means of digital certificates and cryptographic keys. More specifically, the mobile application possesses the certificates of the GBA gateway and the GSC. This way, it can establish secure communication channels with these entities. To authenticate the traffic estimation server, its certificate must be installed on the smartphone. We assume that these certificates are generated by one (or multiple) certification authority (CA) and that the mobile application trusts the corresponding root certificates. Similarly, the GBA and the GSC establish trust by exchanging their digital certificates.

B. System Initialization

To bootstrap the system, the GSC initializes a group signature scheme. Our system supports (but it is not limited to) two cryptographic schemes, i.e., *"short group signatures"* (known as the BBS scheme) [39] and *"group signatures with verifier local revocation"* (GS-VLR) [40]. They are initialized as follows:

- Two multiplicative cyclic groups G_1 and G_2 of prime order p, with g_1 and g_2 being their respective group generators;
- an isomorphism ψ from G_1 to G_2;
- a map $e : G_1 \times G_2 \rightarrow G_T$ (where G_T is also multiplicative and of prime order p) that satisfies the following properties:
  - — e is bilinear: $\forall\, u \in G_1, v \in G_2$ and $a, b \in \mathbb{Z}$, we have: $e(u^a, v^b) = e(u, v)^{ab}$
  - — $e(g_1, g_2) \neq 1$ (nondegeneracy property).

During the initialization phase, the KeyGen(n) algorithm (with n being the number of mobile devices participating in the TIS) is executed, as defined in [39] and [40]. This algorithm, given g_2 and ψ, computes $g_1 \leftarrow \psi(g_2)$. Moreover, additional parameters used by the GSC are defined as follows.

- $h \leftarrow G_2 \setminus \{1_{G_1}\}$ (where 1_{G_1} is the identity element of G_1).
- $\xi_1, \xi_2 \leftarrow \mathbb{Z}_p^*$ so that for $u, v \in G_1 : u^{\xi_1} = v^{\xi_2} = h$.
- A secret parameter $\gamma \leftarrow Z_p^*$ and a parameter w so that: $w = g_2^{\gamma}$.

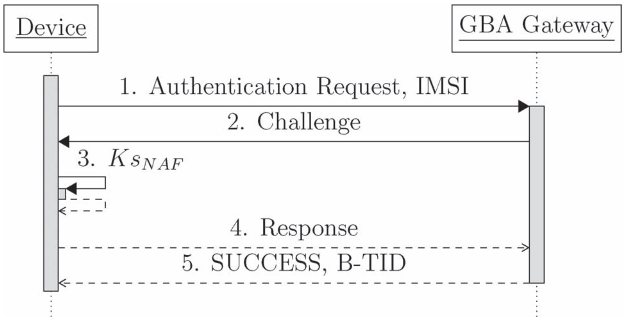


Fig. 4. GBA authentication flow.

KeyGen(n) generates a group public key gpk from the tuple (g_1, g_2, h, u, v, w). The pair (ξ_1, ξ_2) is the secret key (gmsk) of the GSC. It is used whenever a signature produced by a group member must be opened (traced back to its source). All n devices that submit traffic reports to the TIS form a group.

C. Device Authentication and Report Submission

Each mobile device is equipped with a UICC module, i.e., a tamper-proof card, where the mobile operator stores the key each device uses to get authenticated to the cellular network. More specifically, each device possesses a *long-term* key MK shared with the mobile operator. The GBA protocol [41] (see Fig. 4) leverages this key for authentication.

- *Step 1*: The device that wishes to be authenticated sends to the GBA gateway an *authentication request* that contains its *identity* (i.e., IMSI).
- *Step 2*: The GBA gateway responds with an HTTP Unauthorized (401) message and dispatches the following challenge to the device:

$$\text{Challenge} : \text{RANDOM}, \text{AUTN} \tag{1}$$

where RANDOM is a one-time nonce, and AUTN is a token used to authenticate the GBA gateway to the device.

- *Steps 3 and 4*: The UICC calculates an *integrity key* (IK), a *cipher key* (CK), a session key (SK), a response to the challenge, and an application key (Ks_{NAF}) as

$$\text{IK} : f_1(\text{RANDOM}, \text{MK}) \tag{2}$$
$$\text{CK} : f_2(\text{RANDOM}, \text{MK}) \tag{3}$$
$$\text{KS} : \text{IK} \,\|\, \text{CK} \tag{4}$$
$$\text{RES} : f_3(\text{RANDOM}, \text{MK}) \tag{5}$$
$$Ks_{\text{NAF}} : f_{\text{ks}}(\text{KS}, \text{RANDOM}) \tag{6}$$

where f_1, f_2, f_3, and f_{ks} are secure key generation functions. The device sends RES to the GBA gateway.

- *Step 5*: The GBA computes Ks_{NAF} and validates the response; upon success, it sends to the device a bootstrapping-temporal ID (B-TID). Furthermore, it pushes to the GSC (via a secure and authenticated channel) Ks_{NAF} and B-TID.

After the bootstrapping process is finished, the device authenticates itself to the GSC using the HTTP digest authentication, over a secure transport layer security (TLS) tunnel, using

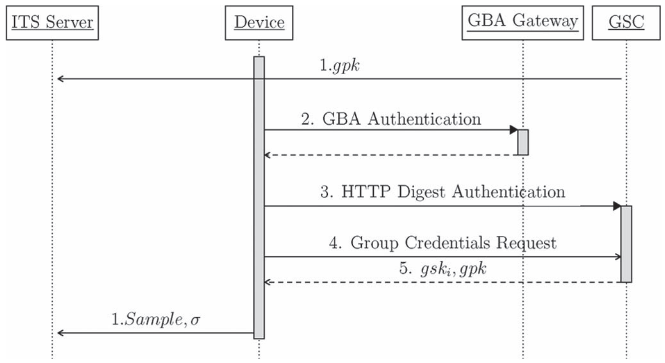


Fig. 5. Device authentication and sample submission.

the previously acquired Ks_{NAF} and B-TID. Once a device i is authenticated, the GSC creates its private key (gsk_i), that is $(g_1^{1/(\gamma+x_i)}, x_i)$ where $x_i \leftarrow \mathbb{Z}_p^*$ [39]. Both the gpk and the corresponding gsk_i are pushed to the mobile device via a secure TLS channel. These group credentials allow the application to submit traffic reports to (or query) the TIS server in a privacy-preserving manner. The GS-VLR scheme generates a revocation token $\mathrm{grt}_i = g_1^{1/(\gamma+x_i)}$. These tokens are used during the signature verification process to identify if a device is evicted or not (Section III-D).

Smartphones submit traffic reports and traffic status queries (for an area of interest) through cellular networks or RSUs (if they are within their proximity), To provide guarantees concerning the authenticity of the TIS server, we use one-way TLS authentication. To prevent unauthorized devices from accessing the TIS, we ensure the integrity of the submitted reports. Reports have

$$\mathrm{report}_i = \left\{\mathrm{loc} \parallel t \parallel \sigma_{\mathrm{sgsk}_i}\right\}.$$

loc denotes the coordinates of the smartphone, t is a timestamp ensuring the *freshness* of the report, and σ_{sgsk_i} is the cryptographic signature produced with gsk_i. By executing the corresponding signature verification algorithm, the TIS server can assess the authenticity of the submitted message. If required, the traffic server can request the latest gpk directly from the GSC. If the GS-VLR scheme is used, the traffic server performs additional checks regarding the revocation status of the device that produced the signature (see Fig. 5).

To reduce the cryptographic overhead, we introduce the notion of *packaging of traffic reports*. More specifically, we decouple the sampling period from the reporting period. A mobile device does not send to the TIS individual traffic reports but packages (i.e., groups) of them. This reduces the number of signatures a device generates and the number of connections established with the server. However, this trades off privacy for performance: Location samples grouped together can be trivially linked. We investigate this tradeoff in Section VI.

D. Device Eviction

If the traffic server determines that some of the submitted samples significantly deviate from the rest, it can initiate a revocation process to prevent the offending devices from further accessing the system. This process requires the gmsk (see Section III-B) to open the signature of a report and reveal the identity of the device. The traffic server (that provides the signature σ to be opened) and the mobile operator (that keeps a map of the Ks_{NAF} keys issued along with the corresponding device identities) must cooperate to revoke the offending device.

In [39] and [40], the $\mathrm{Open}(\mathrm{gpk}, \mathrm{gmsk}, M, \sigma)$ algorithm is defined: it outputs the $g_1^{1/(\gamma+x_i)}$ part of gsk_i. Based on this, it is trivial to identify the device that generated the signature. The identified device is revoked, by adding the corresponding grt_i to the revocation list (RL) published by the GSC. Consequently, once the traffic server receives a request or a sample from a revoked device, it can reject it by checking the RL.

IV. Security and Privacy Analysis

A systematic analysis of the properties of the group signature schemes is presented in [39] and [40]. Here, we focus on the security and privacy properties of our architecture, with respect to the requirements defined in Section II-A2.

Communication confidentiality and integrity are achieved by the TLS channels (requirement R_4). Furthermore, each system component is provided with credentials (i.e., certificates and keys) for authentication (R_1). Unauthorized devices will not be authenticated and thus will not receive a gsk_i. As a result, they will not be able to participate in the TIS (R_1). Samples signed with the same gsk_i cannot be linked. Nevertheless, location data submitted during one TLS session can be trivially linked based on the network identifiers of a device (IP and MAC addresses). To overcome this, we use the TOR anonymization network, which conceals the identity of devices by forwarding traffic through a network of relays ($R_{2/3}$).

The employed cryptographic schemes ensure nonrepudiation. More specifically, in [39], an interactive *JOIN* protocol that guarantees that only the device possesses gsk_i is defined; thus, the GSC cannot forge signatures. This ensures *exculpability* (no entity can forge signatures except the intended holder of the key [42]). Devices that deemed misbehaving can be evicted from the system by leveraging the revocation protocol described in Section III-D (R_5).

An honest-but-curious TIS server has access to the location samples submitted (anonymously) by the mobile devices, and it can reconstruct their whereabouts by leveraging filtering techniques (see Section III-D).

The GBA gateway cannot harm user privacy because it has no access to the samples submitted by their devices. As a result, it cannot reconstruct the whereabouts of the vehicles. Accordingly, the GSC can infer no user identifying information because it only knows the temporal identifiers (B-TID) of the devices (see Section III-C).

A. Formal System Analysis

We verify our system in π-Calculus with ProVerif, an automated protocol verifier [43] that models each system entity as a process and the authentication protocols as parallel compositions of these processes. ProVerif assumes sets of *names* and *variables* along with a finite *signature* Σ that comprises

TABLE I
FORMAL SECURITY ANALYSIS

Datum	Relevant Entities	Secrecy	Strong Secrecy
IMSI	Device, GBA	✓	-
B-TID	Device, GBA, GSC	✓	✓
MK	Device, GBA	✓	-
IK	Device, GBA	✓	✓
CK	Device, GBA	✓	✓
Ks_{NAF}	Device, GBA, GSC	✓	✓
gsk_i	Device, GSC	✓	✓
Report	Device, TIS	✓	✓

all the function symbols along with their *arity*. The basic cryptographic primitives are modeled as symbolic operations over bit strings that represent messages and are encoded with the use of *constructors* and *destructors*. Constructors generate messages, whereas destructors retrieve parts of the messages they are applied to.

The correctness of the protocols is examined in the presence of Dolev–Yao adversaries [44]; they can eavesdrop, modify, and forge messages according to the cryptographic keys they possess. To examine if the adversary can obtain a piece of information i, ProVerif uses the predicate attacker(i). This initiates a resolution algorithm with its input being a set of Horn clauses that describe the protocol. The algorithm outputs true if and only if i can be obtained by the attacker, and false otherwise. If i cannot be obtained by the attacker, then its *secrecy* is ensured. Furthermore, ProVerif can prove *strong secrecy* properties; the adversary cannot infer changes over secret values. To examine strong-secrecy for data i, the predicate noninterf is used.

We examine the secrecy and strong secrecy properties of our architecture with respect to all the critical pieces of information. Table I summarizes our findings, based on which we can see that our system ensures both properties. The adversary cannot obtain or infer cryptographic keys (i.e., $\mathrm{MK}, \mathrm{IK}, \mathrm{CK}, Ks_{\mathrm{NAF}}, \mathrm{gsk}_i$) $(R_{1,4})$ and device identifiers, i.e., IMSI and B-TID (R_2). Moreover, although some of the cryptographic keys are ephemeral, the adversary cannot infer changes over them. We do not evaluate the strong secrecy of IMSI and MK as they do not change over time.

We also use ProVerif to model adversary-controlled system entities that individually or collaboratively try to harm the privacy of users. As such scenarios are not captured by the Dolev–Yao model, we employ *spy channels*; they are accessible to the adversary, and used by adversary-controlled entities to publish their state, keys, and variables. Accordingly, to emulate colluding infrastructure entities, we assume multiple spy channels for each of them. Such an analysis allows us to examine what happens, in terms of privacy, for various combinations of honest-but-curious (colluding) entities.

Table II summarizes our findings. If the GBA and the GSC collude, they can infer that a device participates in the TIS system. Nevertheless, they cannot link traffic reports to the device; thus, the location privacy of the device is preserved. Similarly, even if GBA and TIS collude, they cannot link traffic reports to devices since they do not possess the corresponding gsk_i. A collusion between the GSC and the TIS does not harm privacy as they do not know device identities. To completely deanonymize users and their whereabouts, the GBA gateway must reveal user identities and publish all Ks_{NAF} and B-TIDs.

TABLE II
PRIVACY LEAKAGE FOR ADVERSARY-CONTROLLED SYSTEM ENTITIES

Collusion	IMSI	KS_{NAF}	MK	gsk_i	report-device
GBA-GSC	✓	✓	✓	✓	-
GBA-TIS	✓	✓	✓	-	✓
GSC-TIS	-	-	-	✓	✓
GBA-GSC-TIS	✓	✓	✓	✓	✓

TABLE III
COMPLEXITY ANALYSIS BASED ON [45]

Function	Complexity	Entities
Sign BBS	$12ME + 5PE$	User Device
Verify BBS	$18ME + 10PE$	TIS Server
Sign GSVLR	$7ME + 2PE$	User Device
Verify GSVLR	$10ME + 4PE + 2rPE$	TIS Server

TABLE IV
SPACE COMPLEXITY [45] AND SIGNATURE SIZE (BITS)

-	BBS	GSVLR
Signature Size	$9L$	$7L$
Group Key Size	$6L$	$3L$
Member Key Size	$2L$	$2L$
Report Packet Size	384 + $9L$	384 + $7L$

With these pieces of information, the GSC and the ITS server can invoke the revocation protocol (see Section III-D) to link all samples to their respective device identities. Nevertheless, as these entities belong to different administrative domains (i.e., GBA is administered by the cellular provider), we consider such a scenario a rather improbable one especially since users can be subscribed to multiple cellular providers.

V. SIMULATION SETUP

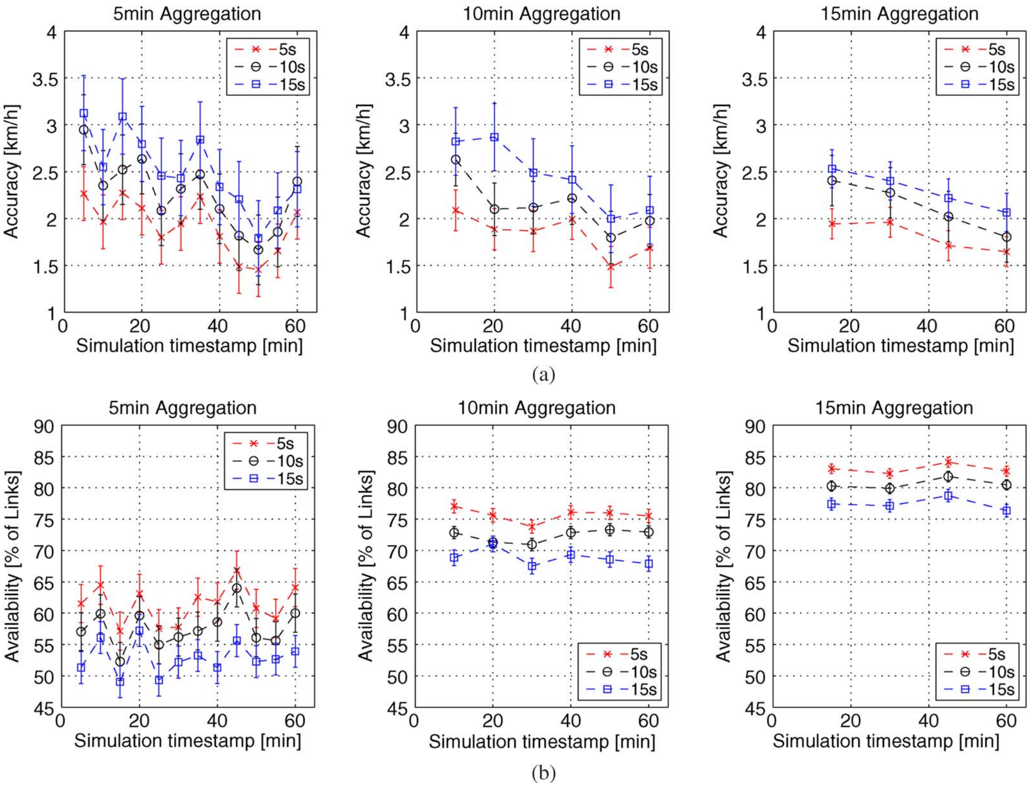
We model urban traffic on arterial roads, with the SUMO microscopic road traffic simulator [46]. To emulate realistic field conditions, we degrade the quality and the quantity of the collected location samples: We define the percentage of tracked vehicles and the error statistics for A-GPS location updates.

We proceed with a two-step *postprocessing*: a Kalman filter (KF) transforms the A-GPS measurements to dynamical state estimates of position and velocity. Then, we use data screening schemes to eliminate undesired data. A challenge for network-based mobile probe systems is the detection of nonvalid probes (e.g., probes from users in buildings or pedestrians). Although such outliers affect the accuracy of the traffic estimation [47], we can safely assume that users use our application only in their vehicles. Nonetheless, by leveraging the broad gamut of sensing capabilities of smartphones it is now feasible to recognize user activity (i.e., walking, driving or standing still[2]).

As the estimated trajectories still deviate from the real ones, due to the introduced location errors, we apply *map-matching* to get traffic information for each link. Finally, aggregates (i.e., according to the aggregation period) of the average speed estimations are calculated for every road link.

To estimate the CPU footprint of the security and privacy protection mechanisms, we consider two setups: one with all the security and privacy mechanisms in place and another where we simply rely on a TLS channel with one-way authentication

[2] http://developer.android.com/training/location/activity-recognition.html



(a)

(b)

Fig. 6. Traffic Estimation Evaluation. (a) Speed estimation accuracy in km/h with 95% confidence interval. (b) Speed estimation availability in percentage with 95% confidence interval.

(i.e., clients are not authenticated by the server). The difference, in terms of performance, between these two setups is an indication of the overhead that our scheme introduces.

We have also implemented a tracker in Java to emulate *honest-but-curious* traffic servers that leverage KFs to reconstruct the whereabouts of the vehicles. Once a vehicle enters the simulation, a KF is created for it and tracks it throughout its trip. Based on a "ground truth file," included in the simulation, we assess the achieved privacy.

VI. Performance Evaluation

1) Complexity Analysis: Table III gives an overview of the complexity of the cryptographic primitives in our system. We provide the number of *modular exponentiations* (MEs) and *pairing evaluations* (PEs) needed by the two group signature schemes. For the GS-LVR scheme, r is the number of revoked devices. Table IV presents the size of the keys as a function of L, which signifies the desired security level. For example, for a security level of 112 bits, we have $L = 224$. To calculate the report packet size, we sum the sizes of the IP/TCP headers, the digital signature (see Section III-C), the GPS coordinates (32 bits) and the timestamp (32 bits).

2) Traffic Estimation: The first metric we consider is the *speed estimation availability* within each time interval, i.e., the number of links for which an estimated average traffic speed exists, divided by the total number of road links. The second metric is the *mean accuracy of speed estimation* for the road links. To calculate it, the estimated speed is compared against the "ground truth" speed of the simulations. We identify two parameters that affect the accuracy of traffic estimation: *Sampling period*, i.e., the frequency at which smartphones report their location to the traffic estimation server and the *aggregation period*, i.e., the time period over which the server accumulates location data before processing them (to produce traffic estimations). Our findings show, as expected, a clear correlation between the sampling frequency and the accuracy of the traffic estimation: Higher reporting frequencies improve accuracy. Nevertheless, requesting more frequent location updates results in a marginal improvement of the speed estimation availability. On the other hand, the aggregation period has a clear effect on speed estimation availability, but it does not significantly influence the accuracy of the traffic estimation. More specifically, longer aggregation periods yield improved availability.

We obtained our data sets from ten simulation runs with randomness in selecting 10% (250 vehicles) of the total number of vehicles. The reason we assumed such a penetration rate is to be close to the minimum requirements (more than 7%) for reliable arterial state estimation [6], [48], [49]. Fig. 6(a) presents the accuracy of our TIS for different location sampling frequencies and aggregation windows. As the figure shows, increasing the location sampling rate yields better accuracy. More specifically, when smartphones submit location samples every 5 s, our system produces accurate estimations, which, as the simulation progresses, converge toward the "ground truth." As the sampling frequency decreases, the estimated value diverges from the actual values because the KFs are provided

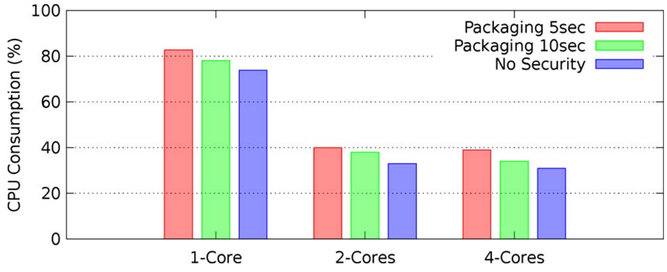


Fig. 7. CPU Load (BBS scheme).

with fewer samples and thus cannot produce accurate estimates. Even in this case, the estimation error is not significant (average accuracy error 3 km/h in the worst case). Regarding the aggregation intervals, we observe that different aggregation windows affect the accuracy of the estimation. Larger aggregation intervals imply more accurate results. The reason is that the samples collected are simply proportional to the aggregation window size.

Next, we examine how the speed estimation availability varies for different aggregation periods. As Fig. 6(b) shows, larger aggregation windows significantly increase the number of road links for which our system has produced estimates. An aggregation interval of 15 min allows our traffic estimation module to produce estimations for approximately 80% of the road links. The actual value depends on the sampling frequency because more frequent location sampling provides slightly better system coverage. Nevertheless, even for low aggregation windows (i.e., 5 min), our system still produces accurate estimates for the majority of the road links.

3) Security Overhead: The security and privacy mechanisms of our architecture introduce overhead. This is important considering the resource-constrained (compared with personal computers) smartphones. The cryptographic schemes induce delays both at the server (verification of signatures) and at the client side (during sample transmission).

Fig. 7 shows the CPU load of three smartphones running our application; they come with different specifications (single, dual, and quad core). The overhead is primarily due to signature generation. To further quantify this overhead, we execute our traffic application on the mobile phones in the following configurations: 1) with no security; and with 2) either of the two group signature schemes considered. We assume a sampling period of 5 s and packaging size (see Section III-C) of one and two samples. We chose these values to get an indication of the CPU stress under realistic, yet resource demanding, scenarios. The total load includes all functionality: communication, map display, and security. On the single-core device, 80% of CPU's duty cycles are consumed by our application. Nevertheless, the contribution of the security and privacy mechanisms is quite small. The comparison of the CPU load in the three application configurations shows that the overhead introduced due to the use of group signatures is approximately 7% on all three phones. Although our application is demanding for lower end phones, state-of-the-art smartphones with multiple cores can easily support it. By doubling the size of sample packages (i.e., a signature is produced for pairs of location samples), we observe a reduction of approximately 5% on the CPU load.

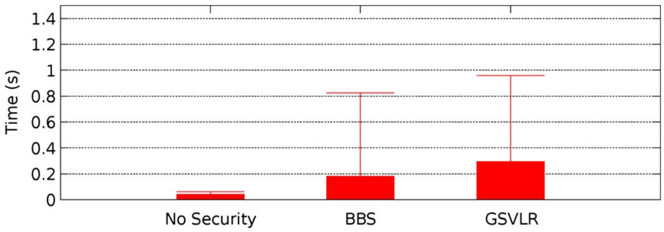


Fig. 8. Latency Evaluation for the single-core device.

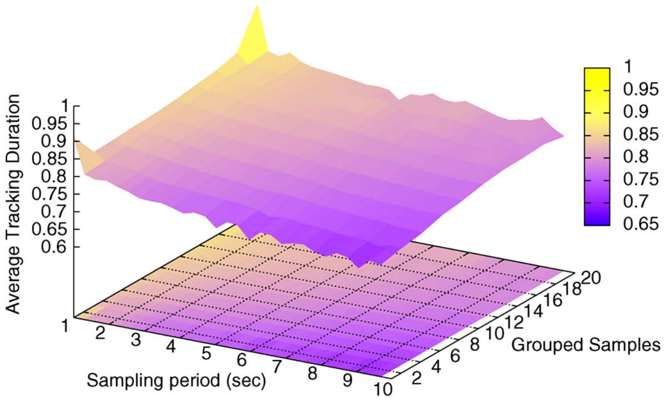


Fig. 9. Average Tracking Duration for different sampling/packaging periods (in seconds).

We also measure the latency introduced due to the security and privacy mechanisms (see Fig. 8). For this, the sampling rate is 5 s, and no packaging of samples is used. We average the results over 50 observations. On the y-axis, we plot the time interval between a sample s_i and sample s_{i-1}. As we can see, without security, the latency is around 5 ms. This means that the actual sampling rate is 5 ms more than the desired one. This latency corresponds solely to network delay. When the BSS group signature scheme is employed, a small additional latency of 0.2 s is introduced. For the $GS-LVR$ scheme, latency is higher (approximately 0.3 s) but still not significant. In both cases, the use of group signatures does not affect the performance of the TIS. For example, a latency of 0.5 s is equivalent to requesting a sampling rate of 5.5 s. Even in this case, our traffic estimation system achieves high accuracy and coverage (see Section VI-2).

4) Privacy: We consider the *average tracking duration metric*, which averages the tracking duration of all vehicles with respect to their whole trip. In Fig. 9 we plot the average-tracking duration as a function of two variables, package size (see Section III-C), and sampling frequency. As expected, more frequent location samples result in increased privacy loss as the KF of the tracker receives more corrections, and it produces better short-term predictions. Moreover, packaging reports together deteriorates location privacy but not significantly. When the sampling period is 1 s and no packaging is used (each sample is sent separately), the average tracking duration is 91%, whereas for the same sampling period, a packaging of ten samples results in an average tracking duration of 97%. By reducing the sample frequency to 10 s (a more realistic scenario for traffic monitoring systems), the average tracking duration drops to 60% and 85% for sample packaging sizes of 1 and 20 samples, respectively.

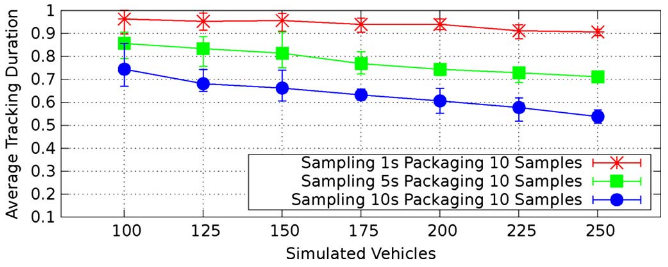


Fig. 10. Average Tracking Duration for different smartphone/vehicle populations.

The performance of the tracking algorithm depends on the population of vehicle/mobile phones. To analyze this dependence, we simulate different populations of vehicles and mobile phones. As this increases, the performance of the tracker deteriorates. This is expected: Higher vehicle density makes tracking harder (more vehicles at intersections with smaller distances between them). In Fig. 10, we present the performance of our tracker with respect to the population size, ranging from 100 vehicles to 250. We plot the results for sampling frequencies of 1, 5, and 10 s and for packaging of ten samples per package.

VII. Conclusion and Future Work

This paper has shown an extensive analysis on the feasibility of deploying smartphone-based TISs. We presented a localization algorithm, suitable for GPS location samples, and evaluated it through realistic simulations. Furthermore, leveraging state-of-the-art cryptographic and telecommunication schemes, we presented a comprehensive security and privacy-preserving architecture for smartphone-based TIS.

Our results confirm it is feasible to build accurate and trustworthy smartphone-based TIS. Nevertheless, there are still challenges ahead: Security and privacy cannot, alone, incentivize uses to participate in large numbers. Toward this, it is interesting to provide fair and privacy-preserving incentive mechanisms.

References

[1] S. Tao, V. Manolopoulos, S. Rodriguez, and A. Rusu, "Real-time urban traffic state estimation with A-GPS mobile phones as probes," *J. Transp. Technol.*, vol. 2, no. 1, pp. 22–31, Jan. 2011.

[2] V. Manolopoulos, P. Papadimitratos, T. Sha, and A. Rusu, "Securing smartphone based ITS," in *Proc. 11th Int. Conf. ITST*, 2011, pp. 201–206.

[3] V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, "Smartphone-based traffic information system for sustainable cities," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 16, no. 4, pp. 30–31, Feb. 2013.

[4] Y. Wang, M. Papageorgiou, and A. Messmer, "Real-time freeway traffic state estimation based on extended Kalman filter: A case study," *Transp. Sci.*, vol. 41, no. 2, p. 167, May 2007.

[5] J. Guo, J. Xia, and B. Smith, "Kalman filter approach to speed estimation using single loop detector measurements under congested conditions," *J. Transp. Eng.*, vol. 135, no. 12, pp. 927–934, Dec. 2009.

[6] M. A. Ferman, D. E. Blumenfeld, and X. Dai, "An analytical evaluation of a real-time traffic information system using probe vehicles," *J. Intell. Transp. Syst.*, vol. 9, no. 1, pp. 23–34, 2005.

[7] Y. Chen, L. Gao, Z. Li, and Y. Liu, "A new method for urban traffic state estimation based on vehicle tracking algorithm," in *Proc. ITSC*, 2007, pp. 1097–1101.

[8] R. Clayford and T. Johnson, "Operational parameters affecting use of anonymous cell phone tracking for generating traffic information," in *Proc. 82nd TRB Annu. Meet.*, 2003, pp. 1–20.

[9] R. L. Cheu, C. Xie, and D. Lee, "Probe vehicle population and sample size for arterial speed estimation," *Comput.-Aided Civil Infrastruct. Eng.*, vol. 17, no. 1, pp. 53–60, Jan. 2002.

[10] M. A. Bacchus, B. Hellinga, and M. P. Izadpanah, "An opportunity assessment of wireless monitoring of network-wide road traffic conditions," Dept. Civil Eng., Univ. Waterloo, Waterloo, ON, Canada, 2007.

[11] "ICT facts and figures," Geneva, Switzerland, Feb. 2013. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

[12] "Mobile future in focus," Reston, VA, USA, Feb. 2012. [Online]. Available: https://www.comscore.com/Insights/Presentations-and-Whitepapers/2012/2012-Mobile-Future-in-Focus

[13] Y. Yim, "The state of cellular probes," Inst. Transp. Studies, Univ. Calif., Berkeley, CA, USA, Jul. 2003, Research Reports.

[14] M. Fontaine, B. Smith, A. Hendricks, and W. Scherer, "Wireless location technology-based traffic monitoring: preliminary recommendations to transportation agencies based on synthesis of experience and simulation results," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1993, pp. 51–58, 2007.

[15] J. C. Herrera *et al.*, "Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment," *Transp. Res. C, Emerg. Technol.*, vol. 18, no. 4, pp. 568–583, Aug. 2010.

[16] B. Hellinga, "Reducing bias in probe-based arterial link travel time estimates," *Transp. Res. C, Emerg. Technol.*, vol. 10, no. 4, pp. 257–273, Aug. 2002.

[17] "Development and demonstration of a system for using cell phones as traffic probes," Kanata, ON, Canada, Feb. 2005.

[18] S. Amin *et al.*, "Mobile century—Using GPS mobile phones as traffic sensors: A field experiment," in *Proc. 15th World Congr. Intell. Transp. Syst.*, New York, NY, USA, 2008, pp. 1–4.

[19] G. Rose, "Mobile phones as traffic probes: practices, prospects and issues," *Transp. Rev.*, vol. 26, no. 3, pp. 275–291, 2006.

[20] J. Krumm, "Inference attacks on location tracks," in *Proc. 5th Int. Conf. Perv. Comput.*, Toronto, ON, Canada, 2007, pp. 127–143.

[21] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Proc. Int. Conf. IEEE/IFIP WONS*, Kranjska Gora, Slovenia, 2010, pp. 176–183.

[22] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in GPS traces via uncertainty-aware path cloaking," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, Alexandria, VA, USA, 2007, pp. 161–171.

[23] B. Hoh *et al.*, "Enhancing privacy and accuracy in probe vehicle-based traffic monitoring via virtual trip lines," *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 849–864, May 2012.

[24] *Draft Standard for Wireless Access in Vehicular Environments (WAVE). Security Services for Applications and Management Messages*, IEEE Std. P1609.2/D12, Jan. 2012.

[25] Car2Car Communication Consortium. [Online]. Available: http://www.car-to-car.org/

[26] T. Moore *et al.*, "Fast exclusion of errant devices from vehicular networks," in *Proc. 5th IEEE-CS Conf. SECON*, San Francisco, CA, USA, 2008, pp. 135–143.

[27] A. Festag *et al.*, "NoW—Network on Wheels: Project Objectives, Technology and Achievements," in *Proc. 5th WIT*, 2008, pp. 211–216.

[28] P. Papadimitratos *et al.*, "Architecture for secure and private vehicular communications," in *Proc. IEEE ITST*, Sophia Antipolis, France, 2007, pp. 1–6.

[29] N. Alexiou, M. Lagana, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "VeSPA: Vehicular security and privacypreserving architecture," in *Proc. ACM HotWiSec, colocated with ACM WiSec*, Budapest, Hungary, 2013, pp. 19–24.

[30] N. Alexiou, S. Gisdakis, M. Lagana, and P. Papadimitratos, "Towards a secure and privacy-preserving multiservice vehicular architecture," in *Proc. IEEE 14th Int. Symp. WoWMoM*, 2013, pp. 1–6.

[31] S. Gisdakis, M. Lagana, T. Giannetsos, and P. Papadimitratos, "SEROSA: SERvice oriented security architecture for Vehicular Communications," in *Proc. IEEE VNC*, 2013, pp. 111–118.

[32] L. Yang and F.-Y. Wang, "Driving into intelligent spaces with pervasive communications," *IEEE Intell. Syst.*, vol. 22, no. 1, pp. 12–15, Jan./Feb. 2007.

[33] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[34] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Mobile Netw. Veh. Environ.*, 2007, pp. 103–108.

[35] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[36] T. Giannetsos, S. Gisdakis, and P. Papadimitratos, "Trustworthy people-centric sensing: Privacy, security and user incentives road-map," in *Proc. Med-hoc-Net*, 2014, pp. 39–46.

[37] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR: Security & Privacy-preserving Architecture for Participatory-sensing Applications," in *Proc. ACM WiSec*, Oxford, U.K., 2014, pp. 39–50.

[38] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications—Assumptions, Requirements, Principles," in *Proc. 4th Workshop ESCAR*, Berlin, Germany, 2006, pp. 5–14.

[39] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. CRYPTO*, *LNCS series*, 2004, pp. 41–55.

[40] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Washington, DC, USA, 2004, pp. 168–177.

[41] "Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)," Sophia Antipolis, Greece, Mar. 2011.

[42] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in *Proc. Adv. Cryptol.—CRYPTO*, vol. 1880, *Lecture Notes in Computer Science*, 2000, pp. 255–270.

[43] B. Blanchet, "Automatic proof of strong secrecy for security protocols," in *Proc. IEEE Symp. Secur. Privacy*, 2004, pp. 86–100.

[44] D. Dolev and A. C. Yao, "On the security of public key protocols," Stanford Univ., Stanford, CA, USA, Tech. Rep., 1981.

[45] M. Manulis, N. Fleischhacker, F. Gunther, K. Franziskus, and B. Poettering, "Group Signatures: Authentication with Privacy," Bundesamt fur Sicherheit in der Informationstechnik, Bonn, Germany, Tech. Rep., 2012.

[46] Simulation of Urban Mobility. [Online]. Available: http://sourceforge.net/projects/sumo/

[47] N. Caceres, J. Wideberg, and F. Benitez, "Review of traffic data estimations extracted from cellular networks," in *Proc. IET Intell. Transp. Syst.*, 2008, pp. 179–192.

[48] X. Dai, M. Ferman, and R. Roesser, "A simulation evaluation of a real-time traffic information system using probe vehicles," in *Proc. Intell. Transp. Syst.*, 2003, vol. 1, pp. 475–480.

[49] S. Turner and D. Holdener, "Probe vehicle sample sizes for real-time information: The Houston experience," in *Proc. Veh. Navigat. Inf. Syst. Conf.*, 1995, pp. 3–10.

Stylianos Gisdakis received the Diploma in computer science from Athens University of Economics and Business, Athens, Greece, in 2008 and the M.Sc. degree in information and communication systems security from KTH Royal Institute of Technology, Stockholm, Sweden, in 2011. He is currently working toward the Ph.D. degree in networked systems security with the Royal Institute of Technology.

Vasileios Manolopoulos received the First degree in electrical and computer engineering from Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2007, the M.Sc. degree in Internetworking, and the Licentiate degree in technology, with a focus on communication systems, from the KTH Royal Institute of Technology, Kista, Sweden, in 2009 and 2012, respectively.

He has been researching security and privacy challenges of location-based services and mobile networks. He is a System Engineer with Saab AB, Stockholm, Sweden.

Sha Tao received the B.S. degree in electronic engineering from Beijing Jiaotong University, Beijing, China, in 2007 and the M.S. degree in system-on-chip design and the Licentiate degree in electronic and computer systems from KTH Royal Institute of Technology, Kista, Sweden, in 2009 and 2012, respectively. She is currently working toward the Ph.D. degree in information and communication technology with the Royal Institute of Technology.

Ana Rusu received the Dipl.-Eng. degree (M.S. degree) in electronics and telecommunications engineering from Technical University of Iasi, Iasi, Romania, in 1983 and the Ph.D. degree in electronics engineering from Technical University of Cluj-Napoca, Cluj-Napoca, Romania, in 1998.

In 2006 she was a Docent in circuit theory with Royal Institute of Technology, Stockholm, Sweden. Since September 2001 she has been with KTH Royal Institute of Technology, Kista, Sweden, where she is currently a Professor of electronic circuits for integrated systems. Her main research interests include low/ultralow-power high-performance circuits and systems for mobile communications and biomedical devices to applications development. She has participated in several national and international research projects and has authored or coauthored more than 100 international scientific publications in journals, conference proceedings, books, and book chapters. Her research interests include circuits using emerging technologies, such as graphene and SiC, with applications on smartphone-based traffic information system and implantable system-on-chip biosensors.

Panagiotis Papadimitratos received the Ph.D. degree from Cornell University, Ithaca, NY, USA, in 2005.

He then held positions with Virginia Polytechnic Institute and State University, Blacksburg, VA, USA; École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland; and Politecnico of Torino, Torino, Italy. He is currently an Associate Professor with Royal Institute of Technology, Kista, Switzerland, where he leads the Networked Systems Security Group. His research interests include a gamut of security and privacy problems, with an emphasis on wireless networks.