ROYAL INSTITUTE
OF TECHNOLOGY

SECURITY AND PRIVACY IN SMARTPHONE BASED INTELLIGENT TRANSPORTATION SYSTEMS

VASILEIOS MANOLOPOULOS

Licentiate Thesis
KTH – Royal Institute of Technology
Stockholm, Sweden, 2012

TRITA-ICT/MAP AVH Report 2012:03
ISSN 1653-7610
ISRN KTH/ICT-MAP/AVH-2012:03-SE
ISBN 978-91-7501-236-0

KTH School of Information and
Communication Technology
SE-164 40 Kista
SWEDEN

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av Teknologie Licentiatexamen i Elektronik och Datorsystem tisdagen den 14 Februari 2012 klockan 14.00 i Sal C1, Electrum 229. Kungl. Tekniska högskolan, Kistagången 16 (Isafjordsgatan 22), Kista, Stockholm.

Abstract

Intelligent Transportation Systems aim at facilitating transportation by utilizing technological advances in communications, computing and electronic sensors technologies. The increasing demand for mobility of persons and freights has led to severe problems related to transportations, such as traffic congestions. Traffic congestions are the cause of environmental problems, economical damages, accidents and also they affect negatively our everyday life. However, building new infrastructures in order to match the increasing number of vehicles and transportation demands is highly costly. Therefore, traffic management applications of Intelligent Transportation Systems, which can utilize more efficiently the existing infrastructures, have attracted attention from the research community.

Most of the existing traffic management systems use a network of fixed sensors for monitoring vehicles. One major drawback, preventing their expansion throughout the road network, is their high cost of deployment and maintenance. A promising alternative is the use of smartphones as traffic probes. Smartphones can accurately determine their position, and then communicate with the traffic management servers through the existing cellular network. Moreover, the increased penetration of these devices, especially in the developed countries can produce accurate data for traffic estimation at very low deployment costs. However, several challenges remain until the deployment of a smartphone-based Intelligent Transportation System. A critical challenge is the security of the system and the privacy of its participants. Attacks to the system can cause malfunctioning which could lead to deteriorating traffic conditions or even to accidents. Moreover, a smartphone communicating an individual's position constantly can pose seriously privacy threats.

The goal of the research performed in this thesis is first to identify the security and privacy requirements for an Intelligent Transportation System and then, to propose a solution which meets these requirements. Both security and privacy are achieved by utilizing the existing authentication infrastructure of cellular networks and integrating anonymous authentication with group signatures. Mutual authentication of communicating parties in the system together with encryption preserves the security of communications in the system. On the other hand, the use of group signatures for anonymous authentication assures that users remain anonymous to the service provider. Finally, identity management and authentication is completely separated from location information, thus guaranteeing that no single entity is capable of connecting an identity to a submitted location.

ACKNOWLEDGEMENTS

I would like to express my gratefulness to my supervisor Assoc. Prof. Ana Rusu for all her support and guidance throughout the time until this thesis. I deeply appreciate that she gave me the opportunity, first for my master thesis and then as a Phd student, to work under her supervision. She has been always helpful, supportive, encouraging and giving important advices, through all the phases of my studies. She has been an example not only on the way of working and conducting research but also in thinking in general.

I want to thank all the people that have been in the same research group for these years and made the office a pleasant environment. In particular, my second supervisor, Prof. Mohammed Ismail Elnaggar for his support and help whenever needed. Dr. Saul Rodriguez Duenas and Julian Marcos Garcia for their advices and help in various matters, from daily small things of PhD student life till concerns and worries on work issues. It was always a pleasure discussing with them. A huge thank you goes to my colleague Tao Sha with whom we shared the same office for the last two years and we worked in the same project. She has been the perfect teammate and friend, always in mood to help and share. Our everyday discussions have been invaluable and made my everyday life much more pleasant. I wish that all my future colleagues will be as gentle persons as Tao Sha is.

I want to thank also Assoc. Prof. Panos Papadimitratos for his great help in the last phase of my work towards this thesis. His help, comments and advices have been of critical importance for improving my work.

My acknowledgements also go to the Swedish Foundation for Strategic Research (SSF) for supporting and funding the work for this thesis through the TRAFFIC project.

I am thankful to all my friends in Sweden and Greece whose friendship supported and encouraged me during these years. Special thanks to Sotiris Falieris for providing the equipment for testing and for his advices on programming on Android.

I am deeply grateful to my family in Greece. To my cousin, Filippos and to my sister who were always willing to listen my concerns, to support and encourage me. Last, but not least, to my father and mother whose love and advices have been invaluable during every step of my life.

TABLE OF CONTENTS

Table of Contents

ABBREVIATIONS AND ACRONYMS

AAA	Authentication, Authorization and Accounting
A-GPS	Assisted-GPS
AKA	Authentication and Key Agreement
AS	Application Server
AV	Authentication Vector
BSF	Bootstrapping Server Function
B-TID	Bootstrapping Temporary Identifier
CA	Certificate Authority
CSCF	Call/Session Control Function
DNS	Domain Name System
DSRC	Dedicated Short Range Communication
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GBA_ME	ME-based GBA
GBA_U	GBA with UICC enhancements
GMSK	Group Manager's Server Key
GPK	Group Public Key
GPS	Global Positioning System
GSC	Group Signature Center
GSK	Group Secret Key
GSM	Global System for Mobile Communications
GUSS	GBA User Security Settings
HAS	Health Authentication Server
HSS	Home Subscriber Server
IBC	Identity-based Cryptography
I-CSCF	Interrogating-CSCF
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
ISIM	IMS Identity Module
ITS	Intelligent Transportation System
MAA	Multimedia-Auth-Answer
MAC	Message Authentication Code
MAR	Multimedia-Auth-Request
ME	Mobile Equipment
NAF	Network Application Function
NAI	Network Access Identifier

OBU	On Board Unit
P-CSCF	Proxy-CSCF
PIR	Private Information Retrieval
PKI	Public Key Infrastructure
RA	Regional Authority
RL	Revocation List
RSU	Road Side Unit
S-CSCF	Serving-CSCF
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SQN	Sequence Number
SVPOS	Secure Virtual Point of Service
TA	Trusted Authority
TLS	Transport Layer Security
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Ad-hoc Network
VTL	Virtual Trip Lines

CHAPTER 1

INTRODUCTION

The growing demand for mobility and the continuous increase of population in big cities have created severe transportation problems. The existing transport infrastructures are unable to handle the amount of vehicles, resulting in heavy congestions for significant periods of time each day. These traffic congestions can be incidental due to special circumstances on roads, such as accidents or extreme weather conditions or recurrent congestions occurring periodically during rush hours. In both cases, the negative implications are spread to many different areas. Congestions can be the cause of accidents that might result in injuries or even fatalities; they contribute to the city's environmental pollution, increase the cost of transportations and most importantly, deteriorate the quality of life of individuals. The constant increase of the car fleet number and the high cost of expanding the road network have steered attention to traffic management systems, which address the problem of congestions by utilizing the existing transport network in a more efficient manner.

An Intelligent Transportation System (ITS) utilizes diverse technologies to develop new transportation systems with improved efficiency [1]. By using information technologies and wireless communications, these systems aim at solving different problems related to transportation, such as traffic monitoring and finally make them safer, faster and less polluting. Previous and recent research has generated solutions addressing different aspects of transportation, such as electronic tolls, variable message signs and traffic monitoring systems. Traffic

monitoring systems try to address the critical problem of traffic congestions. Most of the deployed solutions for solving this issue use infrastructures based on fixed sensors for collecting traffic information. These fixed sensors are loop detectors and traffic cameras that communicate traffic information to a backend supporting infrastructure. Then, fleet management is usually accomplished through variable message signs. However, one major disadvantage of these systems is that their deployment and maintenance throughout the road network require high expenses.

Latest developments in wireless communications, computing and sensors have steered the focus on vehicular research towards Vehicular Ad-hoc Networks (VANETs). Modern cars already feature a variety of sensors and computers that enables them to gather information about their environment. The vision is that every car will be equipped with an on-board unit (OBU) gathering all the information from an array of sensors, process them and then communicate this data through wireless interfaces to its surrounding cars and to the road side units (RSUs). Through this collaborative approach a large spectrum of applications can be enabled in the context of ITS. For example, safety applications that can warn drivers about accidents and severe weather conditions or traffic management applications that can provide real-time guidance to drivers. Research in this area is focused mainly on addressing the open challenges concerning the efficiency of networking protocols and security of communications [2]. Though very promising, the success of applications based on these ad-hoc networks depends highly on the penetration rate of cars with the necessary equipment. The optimal situation would be if every vehicle on the streets was equipped with the necessary sensors and an OBU. The OBU should be capable of communicating in a network established between its neighboring cars and RSUs. However, until reaching adequate numbers, drivers would be reluctant to pay an additional cost for their car just for a potential benefit in the future. To overcome this obstacle, researchers have started considering different alternatives, such as smartphones, to be used for developing ITSs.

1.1 Intelligent Transportation Systems using Smartphones

Modern mobile phones and the so called smartphones present a great opportunity for developing new ITSs. Comparing with the dedicated hardware, which is used for communication in VANETs, smartphones cannot be reliable enough for safety applications; however they can be efficient for traffic management applications. Utilizing mobile phones as probes for traffic information is not a new concept. The high penetration of these mobile devices makes them ideal candidates for traffic probes. For 2010, the approximate number of mobile phones in the

developed countries was around 116 devices per 100 inhabitants and therefore it is natural to suppose that almost every commuter in these countries will have a mobile phone with him/her [3]. Early research was focused on network-based location techniques providing data about the mobility of mobile devices. Several efforts [4], [5], [6], [7] tried to assess the potential and the feasibility of accurate data capable of providing reliable travel time estimates. Although the idea is promising, the accuracy of these network-based techniques has not yet been proven sufficient in order to build a working system based on data solely from cellular probes. Nevertheless, commercial applications have emerged, which utilize data from cellular networks. In such applications, data regarding the mobility of cellular devices are merged with data from GPS-enabled navigation devices in a system that provides travel time measurements [8].

Market statistic surveys report that out of the total number of phones shipped worldwide during 2010, almost 21% were smartphones [9]. Smartphones integrate A-GPS receivers that are able to calculate the location of the device with a higher accuracy than network-based methods and therefore the problem of inaccurate location samples can be overcome. Recent research suggests that reliable traffic information and travel time estimates can be produced [10], [11] with data from A-GPS enabled smartphones. Although several challenges are still to be addressed, a recent field experiment [12], with a system implemented solely on smartphones, shows encouraging results for the feasibility and the accuracy of the traffic estimation (compared to that obtained from fixed sensors): a 2-3% penetration of smartphones running the application in the total car flow suffices for accurate estimation of the average speed.

Besides providing comparable accuracy in traffic estimation, smartphone-based ITSs present also other advantages. They can save the high cost of deploying and maintaining the sensor network infrastructure. They do not need special in-car hardware which allows in short time high penetration rates. Practically, any driver with a relatively modern smartphone would be able to join the system by just downloading a mobile application to his/her smartphone. Major application platforms, Apple's iPhone and Google's Android, provide friendly development environments that can be used for testing, prototyping and distributing the application. Mobile phones can act as sensors and the communication can be covered by the existing 3G/4G infrastructure. Furthermore, feedback to the drivers can be provided on the screen. Additional features such as online digital maps or phonetic route guidance could be easily added to enhance the user friendliness of the system. Finally, major car manufacturers have already started equipping their cars with interfaces to smartphones [13], [14] that could be used to develop additional services for the driver.

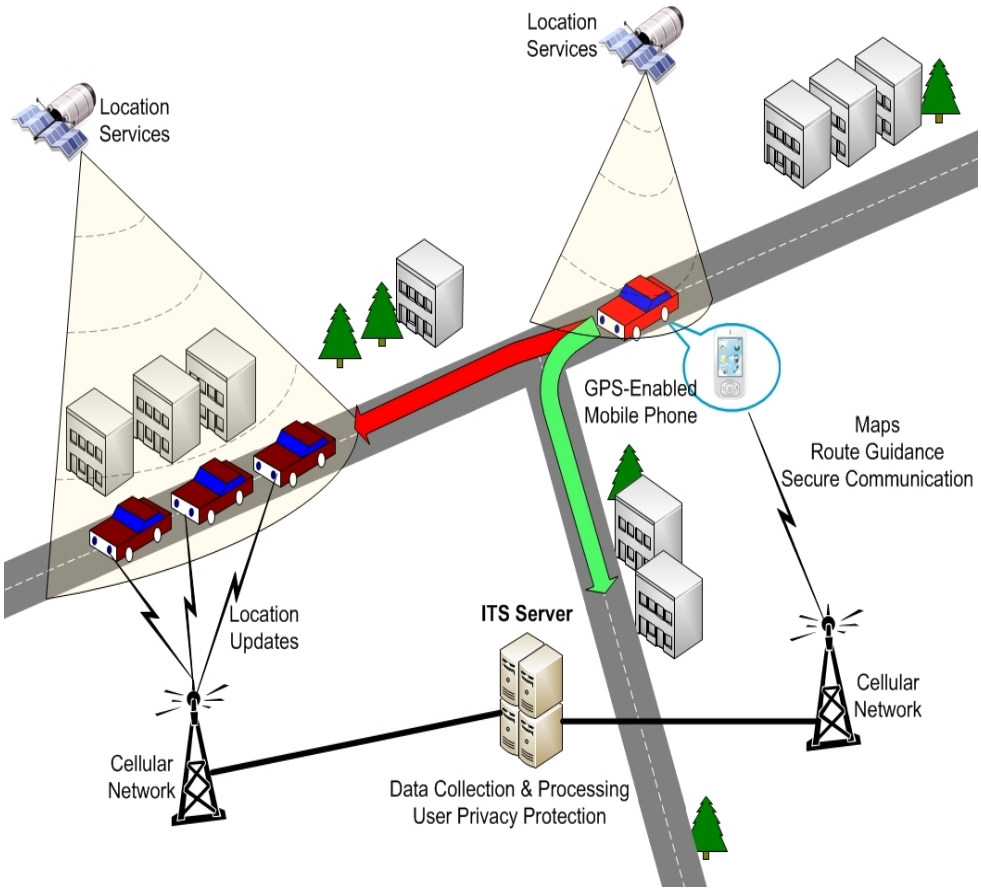

Figure 1.1 System Overview

The main components of an envisioned smartphone-based ITS, as shown in Fig. 1.1 [15], are the smartphones, that each driver who participates in the system carries, and a main processing server that represents the supporting back-end of the system. On the smartphone there is a mobile application running, responsible for calculating the position of the device and sending data to the main server. The server is responsible for data collection, processing and sending feedback to the mobile client. The mobile device's location is calculated using the A-GPS receiver. The communication between the mobile application and the main server is done through the cellular network that the device is subscribed to. Using this communication channel, the device sends its location updates to the server in a timely manner while the user drives to his/her destination. The server, according to the updates that receives, reconstructs a traffic model and calculates, in real-

time, the estimated travel speeds. Proper feedback is sent back to the device for guiding the driver. The updated traffic information sent by the server during the journey is presented on the device's screen on top of a digital map. This information should consist of average travel time to the desired destination and real-time route guidance about the optimal route to be followed by the driver based on parameters such as congested streets, fuel consumption and travel time. Additionally, other dynamic traffic information such as streets under construction or traffic accidents can be sent and displayed on the driver's device.

Such a system seems very promising, but there are still significant challenges to be addressed before deploying such a solution. These challenges can be categorized in two wide areas. Firstly, challenges related to real-time traffic estimation in an efficient and reliable way both on highways and on the urban road network. The second area, in which falls the scope of this thesis, is the security of these systems and the privacy of the users.

1.2 Security and Privacy Issues in ITS

Security of an ITS and the privacy of its users are of paramount importance. In our targeted system, the use of smartphones, besides the obvious benefit of having in short time a big user base, entails also the danger that anyone could possibly participate in the system and start reporting location samples. This means that the system is exposed to potential reporting of forged location data, which could lead to inaccurate or false estimation of the real traffic conditions. Subsequently, erroneous feedback would be sent to the drivers ending up in deteriorating traffic conditions or in extreme cases being the cause of traffic accidents. When it comes to the users participating in the system, it is important to guarantee that the feedback received by the mobile application is reliable.

Location privacy and threats against it has attracted a lot of attention lately. That is mainly due to the numerous location-aware applications that have been developed for smartphones. The ability of using a user’s location can be the starting point for a variety of new applications or even for enhancing the features of existing applications, such as social networks and online games to name a few. On the other hand, a handheld device carried by individuals throughout their casual day can lead to disclosure of sensitive information of their private life, identification and even damages. Together with the popularity of these types of applications comes also a raise in people’s concern about their privacy. Several efforts have been made to inform users about the danger of careless disclosure of their location [16] and to press companies to handle location data in a more privacy preserving way, as seen in a recent case [17]. Privacy concerns are even bigger when it comes to a traffic management system where location is regularly reported to servers. In

[18] the authors explored, among other issues, the willingness of people to share their location and the appeal of location-based services. Most of the questioned participants (i.e. 27 out of 32) answered that they were willing to share their location anonymously, excluding a given area around their homes. However, as the other results show, participants were indeed concerned about their location privacy. Participants' median privacy score, using Tsai's privacy score metric was 5.8 out of 7. An even more interesting finding is the participants' answer to the question on whether the benefits from location data outweigh the risks. The median answer was 3 in a Likert scale of 7, where (1) stands for "the benefit far outweighs the risks" and (7) for "the risks far outweigh the benefit". It is obvious that people are concerned about their privacy even though, depending on the benefit from a given service, they might choose to neglect the privacy risks. Therefore, in order to eliminate these concerns and attract even more drivers to the ITS, it is important to assure forehand the privacy of their whereabouts. Consequently, it must be guaranteed that the identity and location of each individual are not connected and no third party or even an entity in the system can link location samples to a single person.

In traffic monitoring systems there are two main categories of security and privacy challenges. The first category concerns the security and privacy of the communications between the mobile phone and the server. Authentication of users, access management, encryption of communications and privacy of communications are challenges that fall into this category. The second category concerns privacy threats based on location tracking. It should be noted that, even when location samples are gathered in a way not containing any direct identity information, there are still threats against the privacy of the users and private information might be leaked. Successive location updates from a smartphone, even without any identifier, contain spatial and temporal correlations that can be used as indirect identifiers. Correlations can be exploited to reconstruct user paths with tracking techniques [19], [20]. These traces can be processed and matched in order to infer frequently visited places, e.g., home or workplace, and finally reveal the user's identity. To mitigate such threats, several solutions using cloaking techniques [21] or privacy preserving sampling techniques [22] have been proposed. In this thesis, we do not consider this kind of threat against the dataset of location samples, but rather try to address the problem of securing the communications in the system while also removing any direct link between an identity and its location.

1.3 Motivation

Security and privacy are, as described before, essential parameters for the successful deployment of ITSs based on smartphones. The success of this type of systems depends highly on the amount of location samples. On the other hand, for users to find ITS services attractive, it is essential to guarantee their security and privacy.

Security in smartphone-based ITS is not thoroughly studied and there is no single solution that receives the common approval of the scientific community. In general, security and privacy requirements in information systems are properties that can largely vary between different implementations. Therefore, it is of great importance to study each system in particular, in order to identify requirements and possible threats, and based on these, to propose optimal solutions.

In the system proposed by the Mobile Century team [22], the focus is on protecting the users' privacy against attacks on the anonymous locations samples. They propose a novel way of sampling in space (Virtual Trip Lines) and a privacy-aware algorithm for placing these checkpoints for sampling throughout the road network. For communicating these samples anonymously, an ID-proxy entity is used for handling authentication and authorization. The identification part and the location part of each sample are encrypted separately by different encryption keys. In this way, no single entity in their proposed architecture can have access to both identification and location information. Therefore the trust is put on the ID-proxy entity, which will strip off all the identification information. Moreover it is supposed that no entities in the system will collude in order to reveal a user's identity.

Existing commercial solutions offering location-aware services [23], [8], [24] rely on password-based authentication and provide a statement that user's identification is removed from all contributed location samples; they pledge no private information disclosure unless this is required by the authorities. A far more extensively researched area concerns VANETs. Extensive research on the security and privacy of these networks has been conducted, but no single solution has been found mainly due to the high diversity of hardware and topology in this type of networks. New proposals that address mainly the efficiency of used cryptographic algorithms and the communication overhead that is added by the proposed protocols are frequently presented. Despite similarities, these solutions cannot be transferred and applied directly to our targeted system.

It is obvious that security and privacy for an ITS using smartphones must be further investigated. The exact requirements must be identified before proposing a

solution offering security for the system while also preserving privacy against inside and outside threats.

1.4 Research Objectives and Contributions

The focus of this thesis is security and privacy of communications in a smartphone-based ITS. The goal is to propose a solution providing strong security, and authentication of clients' individual contributions. To come with a proposal, first it is necessary to analyze and identify the security and privacy requirements for the targeted system. The first step towards this direction was the implementation of a simple location reporting application described in Publication 1. Next, specific issues, challenges and finally the requirements for a secure and privacy-aware mobile application were identified and presented in Publication 2. According to these requirements, the proposed solution has to provide privacy by design, notably by making location updates anonymous and unlinkable. In particular, deprive not only third parties, but also the ITS server from any chance to trace and identify individuals. The contribution of this thesis is a practical approach to achieve this goal. The initial idea was presented in Publication 3 and the complete description of the architecture with experimental results was presented in Publication 4. The novelty of the proposal lies in leveraging traditional authentication services by cellular infrastructures, augmenting those with anonymous authentication, and keeping the ITS service separate from the mobile operator, thus completely splitting identity and location information.

1.5 Thesis Outline

The thesis is organized as follows. Chapter 2 presents an overview of the related work, which is divided in three categories discussed in the following sections. Section 2.2 presents security and privacy solutions for query-based applications, section 2.3 presents solutions targeting continuous location monitoring applications and section 2.4 presents privacy-aware solutions offering authentication in cellular networks.

Chapter 3 identifies and describes the security requirements for the communications in an ITS and the privacy requirements for the participating users.

Chapter 4 describes the proposed solution for enabling privacy preserving location reporting in an ITS. First an overview of the architecture is presented. Then, each of the building components, namely the IP Multimedia Subsystem (IMS), the Generic Bootstrapping Architecture (GBA) and group signatures, are described. The last section presents the proposed solution in detail, the security analysis and implementation results.

Chapter 5 draws the conclusions and identifies possible future work on this topic.

1.6 List of Publications

Publications included in this thesis:

Publication 1: V. Manolopoulos, S. Tao, S. Rodriguez, M. Ismail and A. Rusu, "MobiTraS: A Mobile Application for a Smart Traffic System," in Proceedings of the 8th IEEE International NEWCAS Conference (NEWCAS), June 2010, Montreal, pp. 365-368.

Publication 2: V. Manolopoulos, S. Rodriguez, M. Ismail, and A. Rusu, "Security and Privacy Issues in a GPS-enabled Mobile Application for Smart Traffic," in Smart Event 2010 in Smart Mobility Conference, September 2010, Sophia-Antipolis. Abstract & Presentation.

Publication 3: V. Manolopoulos and A. Rusu, "Secure and Privacy Preserving Access to Location-Based Services in 3G/4G Mobile Devices," in the 1st Security Conference - Europe, August 2010, Örebro. Extended Abstract & Presentation.

Publication 4: V. Manolopoulos, P. Papadimitratos, S. Tao, and A. Rusu, "Securing Smartphone Based ITS," in Proceedings of the 11th IEEE International Conference in ITS Telecommunications (ITST), September 2011, St.Petersburg, pp. 201-206.

Related publications, not included in this thesis:

Publication 5: S.Tao, V.Manolopoulos, S.Rodriguez, M.Ismail and A.Rusu, "Hybrid Vehicle Positioning and Tracking Using Mobile Phones", in Proceedings of the 11th IEEE International Conference in ITS Telecommunications (ITST), September 2011, St.Petersburg, pp. 315-320.

Publication 6: S.Tao, V.Manolopoulos, S.Rodriguez and A.Rusu, "Real-time Urban Traffic State Estimation with A-GPS Mobile Phones as Probes", accepted for publication in SCIRP Journal of Transportation Technologies, 2011

CHAPTER 2

RELATED WORK

2.1 Introduction

This chapter presents related work targeting security and privacy in location-based services. Section 2.2 describes privacy solutions targeting query-based location applications. To the best of our knowledge two projects have been investigating a similar system with location reporting from smartphones. The field test conducted by Globis Data in 2005 [10] and the research project of Mobile Century in 2008 [25]. However, since the Globis Data project did not investigated the security and privacy aspects, only the Mobile Century solution will be presented. Section 2.3 presents relevant research on continuous location monitoring applications, namely the Mobile Century project and solutions for VANETs. Finally, privacy-aware authentication solutions for cellular networks, which could be utilized for addressing authentication in a smartphone-based ITS, are presented in section 2.4.

2.2 Query-based Location Applications

Applications using location-based queries are becoming very popular for smartphones. In this type of applications, the user issues sporadic queries to a service provider, requesting information relevant to his/her location. For example, a query of this type consists of the question “Where is the closest hotel?” and the actual location of the issuer. The challenge regarding this type of queries is to

protect the privacy of the question issuer from the service provider. The goal is to prevent the service provider from linking a single question to a specific location.
One approach to address this challenge is to introduce a trusted anonymizer between the user and the service provider. Early work [26] suggested spatial and temporal cloaking in order to achieve anonymity. Cloaking is based on the property of *k*-anonymity, meaning that, a user remains anonymous only if his/her location information is undistinguishable among location information from *k-1* other users. In order to achieve this property, the trusted anonymizer selects a sufficient large region so that enough other users (k_{min}) are present at a given time frame. This region is presented to the service provider as the originating location of the query. Several other proposals extend this concept using similar architectures [27], [28], [29], [30]. Other works enhance the cloaking algorithms by introducing also the property of *l*-diversity [31], [32]. Ensuring l-diversity in location-based services prevents the service provider from associating a certain query to an individual. Otherwise, in the case when all k users of a region submit the same query, the service provider could easily conclude that a single user was interested for a certain service.
Other approaches try to eliminate the dependency on a trusted anonymizer. In [33] spatial cloaking is combined with Private Information Retrieval (PIR). In this solution, the user creates the cloaking region around his/her real location and then issues a PIR query to the location services. A peer-to-peer solution is presented in [34], where a user forms a group with nearby peers. In this way, a spatial cloaking area is created, i.e. the region that covers all the members of the particular group. Finally, a hierarchical coding of location information, in the form of country, state, city, coordinates and encryption with different keys, are proposed in [35] in order to allow a user-centric control of privacy.
Approaches targeting query-based location applications can not be applied to our targeted system due to differences both in architecture and in the type of provided services. In our traffic monitoring system, each smartphone is continuously reporting its location to a central server and not in a sporadic query – response way. Furthermore, applying a spatial or temporal cloaking algorithm, either through an intermediate anonymizer or by the application running on the client's device, would affect the accuracy of the provided samples and thus the traffic estimation from the server. Closer to our system are solutions targeting continuous location monitoring applications that will be described in the next section.

2.3 Continuous Location Monitoring Applications

In this type of applications, the location of a user is continuously reported to the service provider or to other users. Two kinds of threats can be considered. The first threat concerns location tracking of users based on the collected location

dataset. The challenge here is to achieve a balance between anonymity and the quality of the provided service, as described in [36]. As mentioned in the introduction, this kind of threat falls out of the scope of our work. A state of the art solution for privacy-aware location monitoring, as the Virtual-Trip Line (VTL) algorithm [22] proposed by the Mobile Century project can be complementary to the solution proposed in this thesis.
The second threat, which this thesis focuses on, concerns the security and privacy of communications. Relevant solutions will be presented in the following section, starting with the authentication architecture of the Mobile Century project, followed by solutions for security and privacy in VANETs.

2.3.1 Mobile Century

Regarding the security and privacy of communications, Mobile Century project suggests an architecture based on separation of entities. The goal is to provide integrity and secure access to the system without disclosing the identity of users. This is achieved by using different encryption keys between entities. The different entities of their architecture are: the client application on mobile phones, an ID-proxy server, the traffic server and a VTL generator. All the communication between mobile clients and the traffic server or mobile clients and the VTL generator is done through the ID-proxy server. The ID-proxy is also responsible for the authentication of each user. Each location update that is sent from the mobile client to the traffic server contains two parts. One part encloses the location information and the other part the identity information. The concept is to encrypt these parts with different keys. In this way, the ID-proxy can have access only on the identity information of this sample since it will be aware of the key that is used in the identifying part, but not on the location information part. In a similar way, the traffic server cannot decrypt the identity part, but can only access the location information of the sample. A detailed description of this technique is provided in [37]. Asymmetric key cryptography is used for the encryption of the location part. The mobile application uses the public key of the traffic server to encrypt this part while a separate symmetric key shared between the ID-proxy and every client is used for the identity part. These keys are established and preinstalled in the initialization phase when a client decides to participate in the system. Further on, it is supposed that they are stored in a tamperproof hardware unit on the device. Authentication to the service is provided based on this shared key. Moreover, the ID-proxy removes the identity part from the sample and forwards it to the traffic server encrypted with a second symmetric key established between the ID-proxy and the traffic server.

This proposal manages to keep the privacy of the clients by removing any direct identification from their location, while also providing authentication of access to

the system. It is based on conventional and well established cryptographic primitives that are reliable and not computational expensive. However, it has one main drawback. The ID-proxy and the traffic server must not collude and should be operated by different organizations. A public authority or a third-party company should develop and maintain an extra registration-authentication system for the users and come with an agreement with the traffic service. This puts an extra burden on the deployment and moreover, this authority should be trusted by the clients participating in the system.

2.3.2 VANETS

VANETs are quite different, in structure and implementation, from a traffic management system based on smartphones. The communication parties and their in-between communication are presented in Figure 2.1. VANETs can be described as hybrid ad-hoc networks. The communication can be Vehicle-to-Vehicle (V2V) between nearby vehicles, which establish an ad-hoc network or Vehicle-to-Infrastructure (V2I). Each vehicle participating in the system is equipped with an On-Board Unit (OBU) consisting of sensors for collecting data (such as speed, acceleration, location and road conditions), a short-range wireless transmitter and a processing unit. The infrastructure consists of Road-Side Units (RSU), which

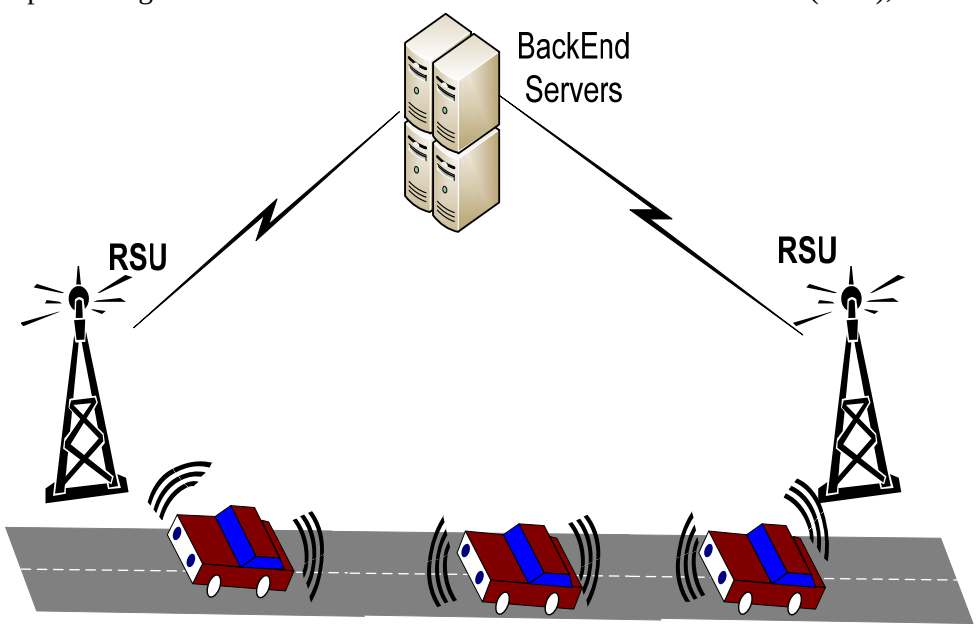

Figure 2.1 VANET Overview

provides access to application servers, Trusted Authorities (TAs) and the back-end infrastructure of the system. Each vehicle listens for updates of information from nearby vehicles or RSUs in its range. Because of the wireless communication and the ad-hoc network architecture, VANETs are vulnerable to attacks that can compromise the whole system's safety and in the end deteriorate the traffic conditions. Therefore, extensive research on describing and implementing the security requirements of these systems is being performed. One major problem in VANETs is the interference of the security requirements of the system with the privacy requirements of the users participating in the system [38]. Therefore, suggested communication protocols must offer high level of security but also be privacy-aware.

The physical and data link layer of communication in most cases, is handled by Dedicated Short Range Communications (DSRC) protocols, the IEEE 802.11p [39] protocol designed especially for vehicular communications . The upper layers are standardized by IEEE 1609 [40] group. In this family of standards, there is also the trail use standard IEEE 1609.2 [41] concerning security services for applications and management messages. It standardizes a security message format, encryption/decryption and authentication using a PKI architecture. However, privacy is not taken into account.

Several research groups have proposed solutions addressing the issue of security of communications in a privacy-aware manner. One of the most popular ideas is the use of pseudonyms which is suggested in many research projects [42], [41], [43], [44], [45]. A pseudonym-based architecture was also proposed in the European project SeVeCom [46]. According to this approach, each vehicle is equipped with a long-term identity associated with a public-private key pair. This key pair is used for the identification of each vehicle when communicating with the Certificate Authorities (CAs). For short-term identification, each vehicle calculates multiple key pairs and sends the public keys to a CA. After authentication, based on the long-term identity, the CA signs these public keys and provides a set of pseudonyms to the vehicle. These pseudonyms are stored in a dedicated hardware secure module, which is supposed to provide physical protection for the pseudonyms and restrict the use of multiple pseudonyms, simultaneously. For revocation and accountability, the CA keeps a record of the pseudonyms and the corresponding identity. Moreover, periodically it publishes revocation lists with the revoked pseudonyms. When a vehicle wants to send a message, it signs the message with the private key corresponding to one pseudonym and it sends out the message with the signature and the pseudonym. Each pseudonym is used for a short period of time and then the vehicle switches to a new one. In this way, linking a pseudonym to a single vehicle is possible only during this short period.

The previously described solution can be considered the basic approach of pseudonyms in a vehicular scenario. Several proposals based on this approach try to address different issues regarding the management of the pseudonyms, the communication overhead and the way of changing them in order to achieve adequate privacy levels. To eliminate the threat of storing in a single entity mappings between pseudonyms and identity, the PRECIOSA project [47] suggests the use of V-tokens [34]. Storage of pseudonym-identity mapping is not needed because identity information is embedded inside the pseudonyms in the form of V-tokens. First, a vehicle is authenticated by a CA and then it obtains a number of V-tokens in a privacy-preserving way by employing a blind signature scheme. Then it contacts a pseudonym provider and it acquires a pseudonym for each V-token. In case that identity resolution is needed, several authorities have to cooperate in order to decrypt the V-token of a pseudonym and reveal the vehicle's identity. This is achieved by sharing the secret key used for signing the V-tokens among multiple authorities in a secret sharing scheme.

One approach to mitigate the complex management of pseudonymous certificates is self-generation on the OBUs. In [48] the authors use the PKI+ system based on elliptic curves to enable the self-generation of pseudonyms [49]. In the initialization phase, a secret key and a corresponding master certificate are obtained from a CA by each vehicle. This secret key, together with the CA's public key, a random number and a version number are used by the OBUs in order to sign their own pseudonyms. The vehicle's secret key is used for tracing purposes and the version number is used for enabling revocation of misbehaving users from the CA.

Group signatures [50] can provide conditional anonymity and therefore have been suggested for applications in VANETs. Nevertheless, they are more computational expensive compared with asymmetric or symmetric cryptography. Therefore, they are usually combined with other schemes for better efficiency. In the hybrid scheme in [51], the authors make use of group signature scheme in order to sign self-generated pseudonyms. A group secret key of each vehicle is obtained by a CA and used to sign every pseudonym. The receiver of a message has to verify, with the group public key, that the pseudonym is signed by an authorized user. Then this pseudonym is used until its expiration time. One issue with this approach is that the CA has no control on the number of pseudonyms created and thus Sybil attacks [52] cannot be avoided. In a follow up work [53], the authors suggest the use of a different cryptographic primitive [54], which limits the number of permitted signing operations in order to prevent these threats. Regional Authorities (RA) are deployed in [55] for issuing short-term pseudonyms, valid only in the area controlled by the specific RA. Authentication to RAs is performed by using a long-term group key, providing conditional anonymity. In [56] group

signatures are combined with Identity-Based Cryptography (IBC). A CA acts as the group manager distributing group keys to vehicles allowing them to be anonymously authenticated. IBC is deployed for authenticating messages from RSUs to OBUs, since in this case there are no privacy requirements. Revocation is addressed by using a group signature scheme with verifier local revocation. However, this is efficient only in the case of small number of revoked vehicles. When the revocation list size exceeds a threshold, then all group members, i.e. all participating vehicles, recalculate new group keys. In [57] a proposal for better revocation efficiency is given. In this scheme, IBC is deployed for vehicles to obtain a pseudonym from a CA. This pseudonym is presented to an RSU, which issues anonymous short-time certificates, based on group signatures, to the participating vehicles in their area. Since these certificates are valid only for a short time, only the RSUs need to maintain the revocation list and accordingly, issue or deny new anonymous certificates.

2.4 Privacy-Aware Cellular Authentication

Since our targeted system is based on data provided exclusively by mobile phones and not from fixed sensor networks or sensors built in vehicles, it is useful to consider the use of security features in mobile 3G/4G networks. Security in these networks is based on a smart card, the Universal Integrated Circuit Card (UICC). The basis of the authentication mechanism between a subscriber and the network operator relies on a shared key between the two parties. This key comes pre-installed in the UICC and it is used for user's authentication and for creating the required session keys for encrypting the communication between the mobile device and the base station. Due to the wide deployment of the 3G/4G networks, the security features of these networks have been thoroughly examined and provide high levels of security. The 3GPP group with the proposal of the Generic Authentication Architecture (GAA) [58] and the Generic Bootstrapping Architecture (GBA) [59] enables the leverage of cellular authentication mechanism to network application level. The GBA provides a mechanism for authentication between a mobile application on the subscriber's device and a network service using the 3GPP AKA protocol of the 3G/4G network. The authentication is based on a challenge-response scheme using the same pre-shared key between the mobile subscriber and the mobile network operator.

In [60] the authors suggest the use of GBA in an application for purchasing media content. A Secure Virtual Point of Service (SVPOS), which acts as the intermediate between a customer and a merchant proving media content is proposed. Their goal is to provide privacy/anonymity (credit information) of customers to merchants. GBA is utilized in order to authenticate the customers

and also the authorized merchants. Each transaction is regulated by the SVPOS, a secure and trusted entity, which holds all the identity and charging information of each customer. Privacy of customers is accomplished by using only a temporary ID and key, provided by means of GBA, in the communication with a merchant. The use of GBA has been also investigated in the context of mobile services for ehealth. In [61], in a similar architecture with SVPOS, a Health Authentication Server (HAS) is introduced. The HAS is the trusted entity acting as an identity provider between user and health services providers. Authentication to HAS is achieved using the GBA. The HAS delivers a security token to every authenticated user, each time when the user wants to access a service. Two concerns related to the use of GBA, as presented in [62], are the use of the Mobile Operator as a third party and the trust on a native software application on the mobile device, which needs to implement the GBA procedures.

2.5 Conclusions

The security and privacy solutions presented in this chapter show that the only similar approach to our targeted system is the Mobile Century project. Although offering security and privacy through anonymity, the deployment of an extra ID-proxy entity managing authentication is needed. Moreover, it is supposed that this entity will never collude with the traffic server for revealing a user's identity. Security and privacy requirements of a smartphone-based ITS are similar with those for VANETs, but there are differences related to the targeted applications and the system's architecture. A common issue in VANETs is the effect of the security solutions on the performance and efficiency of the system, especially for safety applications. However, our targeted application is traffic monitoring, which is not a time critical application and thus time constrains are not so demanding. This fact allows the use of computationally expensive cryptography without the need of complicate solutions dealing with the computational overhead. Moreover, there is no need for communication and thus authentication between users, because reporting is done directly to the ITS server. Consequently, ideas applied in VANETs can be reused in our case, but their application should be investigated and adjusted, taking into account the different architecture and the specific application case. Concerning privacy-aware cellular authentication, the GBA architecture presents an interesting potential for leveraging authentication services without the need of deploying an extra entity. Nevertheless, a parameter that should be further investigated is the role of the mobile operator as a point of trust.

CHAPTER 3

SECURITY AND PRIVACY REQUIREMENTS

3.1 Introduction

This chapter presents the security and privacy requirements for the targeted ITS [63]. In this type of ITS, there are two main actors: 1) The group of authorized users who report their location through the mobile application on their smartphones; 2) the ITS and more specifically the ITS server, which gathers the location information, processes it and provides feedback to the users. There are no privacy requirements for the ITS server, but only security requirements concerning its safe operation. In the next two sections, the security requirements for the system and the privacy requirements of the users will be described.

3.2 Security Requirements

Besides the obvious benefits of a smartphone-based ITS there are several issues related to its security and the privacy of the users. Malfunctioning of the system or sending false guidance information can deteriorate traffic congestion or even worse, be the cause of road accidents. Before deploying such an ITS, it is necessary to guarantee the security of the system and its ability to provide reliable information to drivers. In order to achieve this goal the following requirements have to be fulfilled.

Authentication: This is one of the most obvious requirements. All communications in the system must be done between mutual authenticated parties.

Specifically, users and the central server must be authenticated to each other. The ITS server has to implement an access control mechanism in order to send feedback only to legitimate users. Moreover, it has to be assured for the authenticity of the provided samples. Therefore, authentication of users is needed. On the other hand, the ITS server has to be authenticated to users in order to prevent an outsider from impersonating the ITS server and mislead users into exposing their location.

Access Control: After the identity of a user is authenticated, access to the system should be granted or not. An access control mechanism should allow legitimate users to report their location to the server and get feedback (traffic estimations, instructions), while location samples reported from unauthorized users should be discarded. In this way, only subscribed users, paying for this service, can participate in the system.

Accountability: In case of misbehavior, an authority should be able to disclose the identity of a user and revoke his/her right to participate. Because of the critical runtime environment, every sender should be able to take responsibility for the message that was sent. This is important for preventing false location reporting, which could lead to malfunctioning of the system and finally erroneous information regarding traffic conditions. In such a case the sender should be able to be identified and possibly revoked the right to use the system. Therefore it is necessary to provide a mechanism for easy revocation of a user's access to the system.

Message Integrity: The receiver of a message must be sure that no intermediate has altered the original message. Since accountability is enforced and each user is liable for the information that provides, it is necessary to guarantee that each message in the network is received unchanged.

3.3 Privacy Requirements

There are two main threats against the privacy of the users: 1) Third parties, which might interfere in the communication between a smartphone and the server, and acquire knowledge of its location; 2) The traffic system itself. Being able to associate a user's identity for a long period of time and at different locations visited during the day is a major threat to the privacy of individuals. Users will hesitate to use the service knowing that their location and identity are connected and stored in the system. In such a case, there is a risk that personal data will be exploited in an unauthorized manner either by the company operating the traffic system or by a misbehaving insider. The following requirements have to be fulfilled in order to protect the users' privacy.

Anonymity: The ITS related actions of the mobile clients must not reveal their identity. If messages are not reported anonymously to the ITS server then tracking of individual users can be trivial. Therefore, each message should not contain direct or indirect identification information of its origin. However, this comes in contradiction with accountability and authentication, required properties for securing the ITS server. Thus, only conditional anonymity is feasible in this type of systems. A trusted party has to be able to identify users and to disclose the sender of message, when this is required. However, this operation should be restricted only to a trusted and authorized entity.

Unlinkability: Unlinkability ensures that relationship between items of interest cannot be directly linked to each other. In an ITS, this means that messages reported by a single user cannot be linked and associated together neither by the ITS server nor by any outsider. Linking together subsequent samples in order to reconstruct a track of an individual is one of the most serious privacy threats in location-based systems. Similar tracks observed in a time frame can be grouped together and finally used for identifying a person. For example, it is possible by observing tracks of a person during working days, to deduce his/her home and work location and then fully identify this person using a catalog database.

Message Confidentiality: It is necessary to guarantee each message's confidentiality. Location samples sent by the user to the ITS server must be encrypted and only the authorized recipient, i.e. the ITS server, should be able to read the content of the message. Similarly, only the authorized user should be able to access the content provided as feedback from the server.

3.4 Conclusions

The main challenge regarding the implementation of the described requirements, is to achieve a balance between securing the functionality of the system and preserving the privacy of its participants. Obviously, there is a conflict between authentication and anonymity. Allowing anonymous data reporting to the server is not an option since this will allow anyone to report erroneous location samples and thus alter the estimated traffic conditions. Moreover, charging of the service or revocation of misbehaving users would be impossible. On the other hand, classic authentication schemes based on personal passwords or public key certificates cannot be used, because messages could be trivially associated with a single source and in this way violate the requirement for unlinkability.

In order to mitigate this problem, a trusted third party, which will be responsible for the authentication to the system, should be introduced in the architecture. However, this trusted third party must be prevented from any access on the

location of the users. The ITS server should be able to distinguish legitimate users and grant access to them. However, it should not be able to reveal the identity of a user neither connect subsequent connections to the same user.

CHAPTER 4

PRIVACY PRESERVING LOCATION REPORTING

4.1 Solution Overview

This chapter presents the proposed approach for a privacy preserving security solution in smartphone-based ITSs [64], [65]. The proposed solution is based on the principle of separation of concerns. Thus, authentication and identity management in the system are separated from the ITS services. The goal is to deprive the ability of any entity to have access to both identity and location information.

Since the targeted ITS collects data provided only by smartphones, security features of the cellular networks could be utilized for user authentication. The mobile operator, which can roughly determine a subscriber's position using network-based techniques, receives already much trust from users. Therefore, the mobile operator is chosen to act as the trusted party, handling authentication and identity management, in the ITS. Identification and authentication in cellular networks are based on the Universal Integrated Circuit Card (UICC), which stores a shared key between the subscriber and the mobile operator. The GAA [58] and the GBA [59], proposed by 3GPP, enable the use of the cellular network's authentication mechanism for accessing third-party applications and services. This architecture is used in order to provide identity management and authentication. However, in order to prohibit the operator's access to the reported location updates

and address the privacy requirements, anonymous authentication using group signatures is integrated in the GBA.

The ITS server should receive information containing only location samples provided by the A-GPS receiver of the smartphone and no other direct information regarding the sender's identity. Moreover, sequential samples reported to the ITS server should look completely unrelated. It should be impossible to determine if two or more samples were sent from the same device. However, the ITS needs to implement an access control mechanism, which will allow reporting and provide feedback only to authorized subscribers of the service. In order to enforce this access control, the ITS server needs to authenticate a user and conclude on his/her right to be granted access or not. This access control is implemented using anonymous authentication based on group signatures. Each legitimate user that wants to be granted access to the ITS requests a private group key. For every sample that is about to be transmitted, a group signature is computed by using the user's group secret key. This signature and the location data are transmitted to the ITS server. Updates are accepted or rejected by verifying the signature with the group's public key.

Creation, distribution, revocation and management of group keys is done by an entity called Group Signatures Center (GSC), under the control of the mobile operator. A subscriber, which is registered for the ITS service, authenticates itself by means of GBA and then requests his/her private group key from the GSC. We assume that the ITS service and the mobile operator have come beforehand to a mutual agreement, according to which the ITS service asks the mobile operator to register a person as an authorized user of the ITS service. The subscriber's registry in the mobile operator's network is updated and checked every time a new private group key is requested.

Reporting to the ITS server is conducted through an encrypted end-to-end TLS channel. The TLS connection is established between the ITS server and the user. The server's public key certificate is used for authenticating the ITS server to the user and for encrypting the TLS channel. In this way, information between the two parties is kept confidential and the integrity is protected. Authentication of the user to the ITS server is implemented inside the TLS channel by computing a group signature on a hash of the submitted sample. The group's public key, provided by the GSC, is used for the verification of the signatures and enforcement of access control in the ITS.

The ITS server has access to the location information but cannot identify a single user inside the group, because of the properties of group signatures. Moreover, the connection between sequential location data exists only as long as the user is using the same TLS connection to the server. This is a slight relaxation of the initial

requirement of unlinkability stating that every submitted location sample should be unlinkable to others. However, in a real case scenario, a new connection will be established with the ITS every time the application is started or according to a time threshold, predefined in the application of the smartphone. Due to the properties of group signatures, these sequential connections can not be linked together, even when the user is using the same private group key. On the other hand, the mobile operator has access to the identity information of the user, but can not retrieve his/her location data. The user submits updates directly to the ITS server through a TLS channel encrypted with the server's public key.

In the following sections, the core IMS architecture and its basic features related to identification and authentication are presented; the GBA, the used group signatures schemes and finally, the proposed solution are described.

4.2 IP Multimedia Subsystem

4.2.1 Overview

IMS is an all-IP architecture of 3G/4G networks that enables ubiquitous cellular access to different kind of Internet-based services [66]. It was originally proposed by the 3GPP group with the vision to merge the cellular networks with the Internet. Furthermore, several procedures regarding security of services, authentication and authorization [56], [57], have been standardized under the scope of IMS. Before describing these procedures, this section will present an overview of the IMS system that represents the basis of our solution.

Fig. 4.1 presents the core components of the IMS and the communication interfaces between them. The IMS communications are based on internet standards, namely the Session Initiation Protocol (SIP) [67] protocol for signaling and control of the sessions (Mw, Gm interfaces) and the DIAMETER [68] protocol (Cx, Sh interface) for Authentication, Authorization and Accounting (AAA). The main entities in IMS are the SIP servers, called Call/Session Control Functions (CSCFs) and the User Equipment (UE). The term UE refers to the mobile device or Mobile Equipment (ME) in the 3GPP context and the UICC smart card together. The CSCFs handle registration, session establishment/maintenance and the entire SIP routing/signaling in IMS. There are three different types of CSCFs, which are categorized according to the functionalities that they provide [69].

- **P-CSCF** (Proxy-CSCF): The P-CSCF can be seen as the first access point to the IMS. It acts as an inbound/outbound SIP proxy server. Every IMS terminal connected to the network is allocated to a P-CSCF during the

registration. Compression of messages is supported in the SIP protocol and P-CSCF is responsible for providing this functionality to the end user. Related to security, the P-CSCF offers integrity and confidential protection for SIP signaling. This is done during the registration phase by negotiating the security associations of IPSec with the UE.

- **I-CSCF** (Interrogating-CSCF): The I-CSCF is a SIP proxy that provides routing information for SIP request/answers. It is used mainly to assign an S-CSCF to a subscriber based on the information that it receives from the HSS.
- **S-CSCF** (Serving-CSCF): The S-CSCF is a SIP Server that is the center of the IMS signaling procedures. It handles registration, routing, maintenance of sessions and enforcement of mobile operator's policy. In the context of SIP protocol, it acts as a SIP registrar (i.e. maintains the

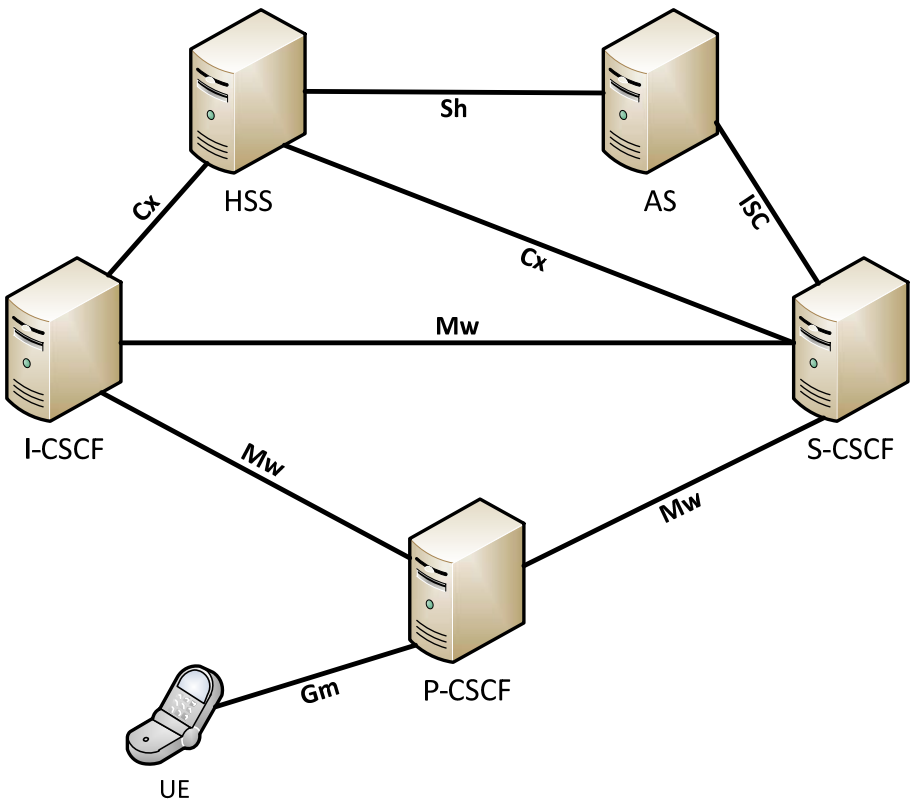

Figure 4.1 IMS Architecture

association between a terminal's IP address and a SIP address record).

The Application Server (AS) is also a SIP entity that hosts any additional services for the users; it can be on the mobile operator's side or from a third-party company. The Home Subscriber Server (HSS) is the main database of the IMS holding information about identities, security (authentication and authorization) and user information (requirements and capabilities) regarding access to particular services.

4.2.2 Identification of Subscribers

Users' identification in the IMS is described in [70]. Identification is based on two types of identities; public and private user identities.

- **Private User Identity**: A unique global private identity is assigned by the mobile operator to all subscribers in the IMS. The format of this identity is a Network Access Identifier (NAI) [71], as user@operator.com. The private user identity is used exclusively for subscription identification and authentication. It is stored in an IMS Identity Module (ISIM) application and in the HSS server on the operator's side.
- **Public User Identity**: One or more public identities are assigned to every subscriber in the IMS. The public identity is the identity used by a user for contacting other users of the IMS. The format of this identity is either a SIP URI [67], as sip:name.lastname@operator.com, or a TEL URI [72], as tel:+1-201-555-0123. Multiple public identities can be registered to the operator and can be used to differentiate the personal identity that a user presents to other users. For example, one identity can be presented to family members and another one to business colleagues. During registration, public identities are not authenticated by the network. Each ISIM application has to store at least one public identity, which might be used to identify the stored user information in the HSS of the operator.

The relationship between a subscription, private identities and public identities is shown in Figure 4.2 [70]. Every private identity is stored in a separated ISIM application. However, it is possible to provide two different smart cards, containing two different ISIM applications and thus two different private identities, to a single user (subscription). Moreover, a single public identity can be connected to two different private identities. Therefore, a single public identity can be used simultaneously from two different devices using two different smartcards. Every public identity is connected with one specific service profile.

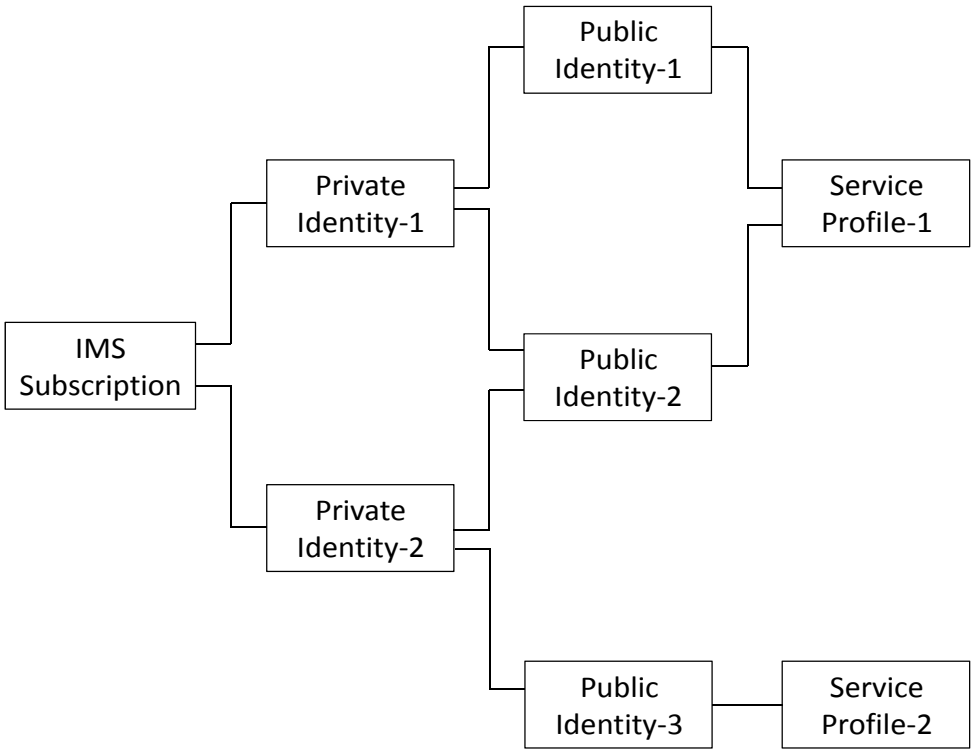

Figure 4.2 Relationship between identities

4.2.3 Storage of Identities

On the network side, the HSS of the mobile operator's network stores the identities of every subscribed client. Identification and authentication of subscribers in IMS is based on the presence of a UICC card in every connected terminal. The UICC is a removable smart card with limited storage space and processing power that can contain several logical applications. Storage of identities, identification and authentication procedures are handled by the following three applications.

SIM (Subscriber Identity Module): The terms UICC and SIM are often confused, but UICC refers to the physical entity of the smart card while SIM is just an application inside the UICC. SIM is the application containing the GSM identification information. Terms were standardized in the early development phase of GSM and the same specifications are followed in 3GPP.

USIM (Universal Subscriber Identity Module): This application is standardized by 3GPP in [73]. USIM provides the storage of information and procedures that are used for identification and authentication when accessing UTMS networks.

ISIM (IP Multimedia Services Identity Module): This application is standardized by 3GPP in [74], targeting specifically, identification and authentication in accessing the IMS. The main stored parameters are:

- **Private User Identity**: One private identity of the subscribed user. Only one private identity is allowed per ISIM.
- **Public User Identity**: One or more of the public identities connected with the private identity.
- **Home Network Domain URI**: The SIP URI of the home network domain to be used in the registration.
- **Long-term Secret**: This secret is created by the operator; one copy is stored in the ISIM and the other one in the operator's HSS. Authentication is based on this key, which is used to derive a cipher key and an integrity key. The cipher key is used for encryption and the integrity key for integrity protection of SIP messages between the terminal and the S-CSCF. Moreover, they are used for authentication to services in the procedures of GBA, as it will be described in section 4.3.

All of the aforementioned applications can reside simultaneously on the same physical UICC card inserted in a mobile terminal. Although ISIM is designed and preferred for access to the IMS system, there is support for access by deriving the necessary parameters out of the existing USIM [70].

4.2.4 Authentication in the IMS

Authentication of a subscriber in IMS is done by using the IMS Authentication and Key Agreement Procedure (IMS AKA) [75]. It is based on the IP Multimedia Private Identity (IMPI) and the shared key between the subscriber and the network operator, which is stored in the UICC smart card. In case that an ISIM is not available, but there is an USIM application in the UICC of the terminal, the same procedure that will be described here is followed. However, in this case the necessary initial parameters are derived by the parameters stored in USIM with a procedure described in [70]. In order for the subscriber to be authenticated it is required to have in the ISIM of the terminal one IMPI and at least one or more IP Multimedia Public Identity (IMPU). The exchanged messages use the SIP protocol except the communication to and from the HSS, which uses the DIAMETER [76] protocol. The messages' flow and the participating entities are shown in Fig. 4.3.

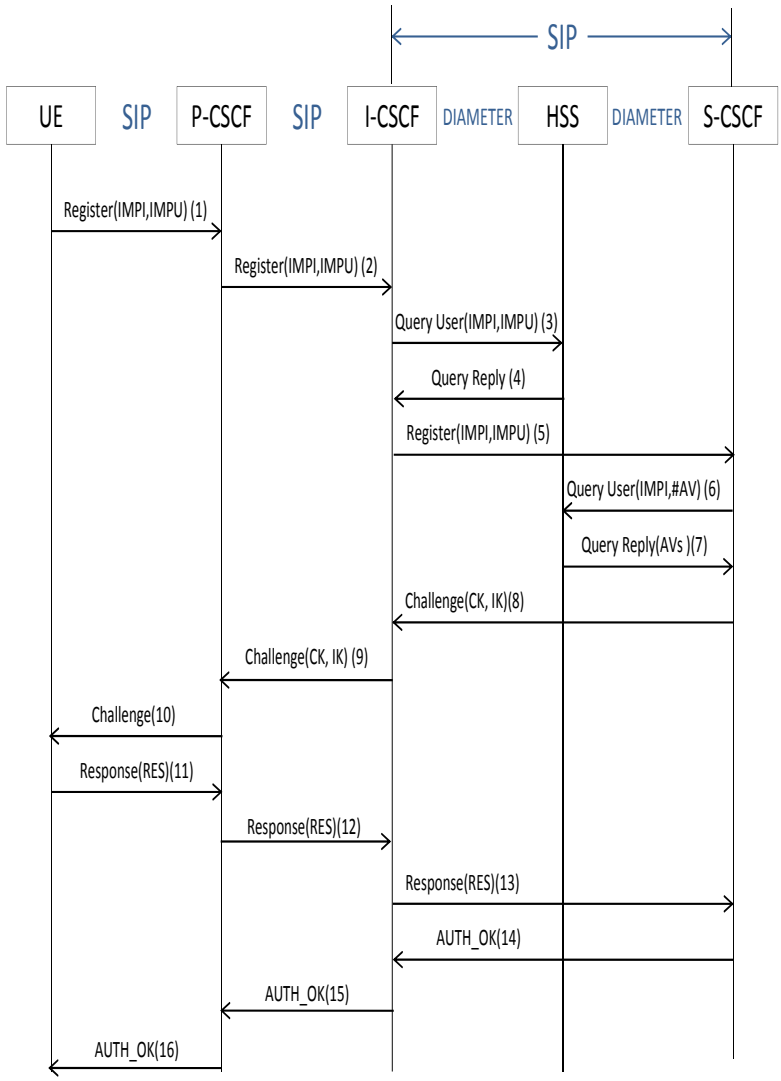

Figure 4.3 IMS AKA Message Flow

In message 1, the UE sends a SIP REGISTER message containing also its IMPU and IMPI towards the P-CSCF.

In message 2, the P-CSCF processes the attached home network domain URI, performs a DNS request and finally forwards the message to the I-CSCF.

In message 3, the I-CSCF contacts the HSS, using the DIAMETER protocol, in order to obtain the user related information already stored by the network operator.

Based on the response from the HSS, in message 4, the I-CSCF selects the appropriate S-CSCF to serve the subscriber.

Then, in message 5, it forwards the initial SIP REQUEST message from the UE to the selected S-CSCF. When receiving this message, the S-CSCF will use an Authentication Vector (AV) for proceeding with the authentication of the subscriber. If the S-CSCF does not have already an AV stored for the specific subscriber, it contacts the HSS to obtain one.

In message 6, the S-CSCF sends a DIAMETER message containing the IMPI and a number of the AVs.

The HSS, in message 7, replies with an array of AVs sorted according to their sequence number. Each AV contains:

- RAND: a random challenge.
- XRES: the expected result.
- AUTN: a network authentication token. This token is created using the shared secret key stored in the IMSI. It includes a sequence number (SQN), which is kept always in sync between the IMSI and the HSS, and a Message Authentication Code (MAC). The exact mechanism for the synchronization of SQN and the derivation of AUTN is described in [58].
- IK: an Integrity Key.
- CK: a Ciphering Key.

Each of these AVs can be used only once for the authentication of the terminal. Based on the first AV, the S-CSCF creates an authentication challenge to be sent to the UE using the HTTP Digest AKA, described in RFC3310 [77]. It contains a WWW-Authenticate header with a nonce value calculated using RAND and AUTN.

This challenge plus the CK and IK are forwarded to the P-CSCF through the I-CSCF, in messages 8 and 9.

In message 10, the P-CSCF removes the CK and IK and passes the authentication challenge to the UE. The UE from the nonce value deduces the RAND and the AUTN. The AUTN consists of the SQN and a MAC. The UE uses the secret

shared key to compute an XMAC value and compares it against MAC. It also checks SQN for being in the correct range. The procedure for these checks and the use of the secret shared key is the same as in 3GPP AKA [58]. When these checks are passed, the ISIM is able to compute a response RES, CK and IK.

Using RES, in message 11, the UE sends a respond to the P-CSCF inside a SIP REGISTER message. This response is forwarded to the S-CSCF, in messages 12 and 13.The S-CSCF compares the received RES value against the XRES value that has been obtained initially, in message 7. If it is successful, the authentication is completed and the IMPU is registered for the specific terminal.

The procedure concludes with messages 13-15 when the S-CSCF forwards a SIP 2xx AUTH_OK message to UE and registering the IMPU to the HSS, in case it was not already registered.

4.3 Generic Bootstrapping Architecture (GBA)

GBA was proposed by the 3GPP in order to enable secure access and bootstrap authentication to third-party applications, which are not standardized under the IMS. The vision behind this architecture is to provide a common frame that can be utilized by all different kind of digital services, which might need to authenticate their users. The authentication solution should be general and access independent, following the design principles of the IMS. The access to IMS networks is controlled by the AKA mechanism described in the previous section. This mechanism is extended by the GBA in order to bootstrap authentication to various services. The GBA's design ensures that authentication is completely separated between different services and the original infrastructure is not jeopardized. This is achieved by protecting the initial keys from the AKA procedure. For each new service that the subscriber wants to access, new different key material is derived. Two slightly different versions of GBA are proposed by 3GPP in [59]. The first version does not require a GBA-aware UICC while the second one provides UICC security enhancements.

- **GBA_ME**: All functions, for bootstrapping authentication on the client side, are executed on the ME, the hardware of the subscriber's terminal. Thus, the UICC and its ISIM application have no participation in executing the GBA specific procedures.
- **GBA_U**: In order to provide enhanced security features for applications, it is necessary to physically protect the derived keys. This version uses the UICC in order to store derived keys and splits functions between the ME and the UICC.

In GBA, there are four entities participating in the procedure for authentication.

- **UE** (User Equipment): the client.
- **NAF** (Network Application Function): the service application.
- **BSF** (Bootstrapping Server Function): the entity implementing the bootstrapping procedure on the network side.
- **HSS** (Home Subscriber System): the main registration database of the operator.

In the next paragraphs the requirements for the entities and their interfaces will be described. The architecture, the entities participating and the interfaces between them are shown in Fig. 4.4.

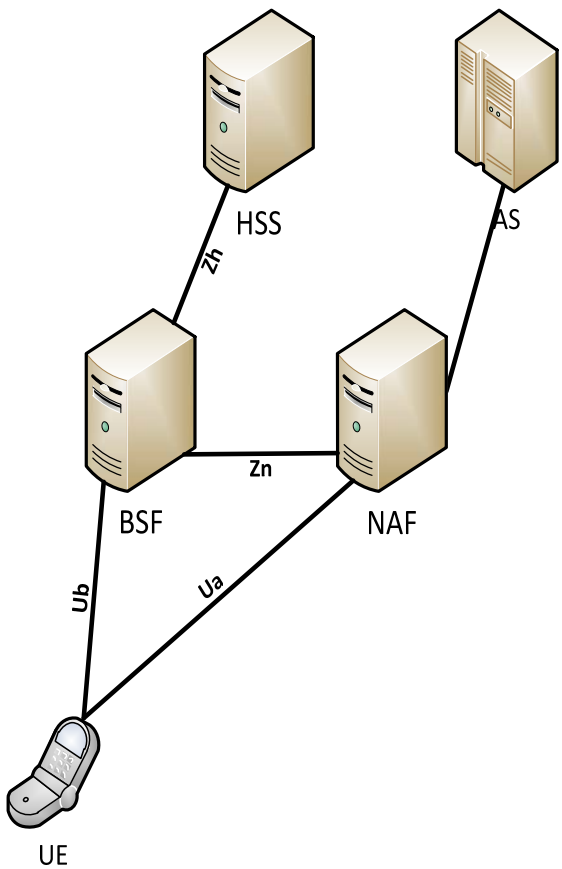

Figure 4.4 Generic Bootstrapping Architecture

4.3.1 UE

The term User Equipment (UE) implies both the UICC, with ISIM or USIM application and the ME. The main requirements, related to GBA, are the following:

- Support of the HTTP Digest AKA protocol [77].
- Select and use one of the USIM or ISIM applications to derive the needed key material, based on the CK and IK that were described in the previous section.
- Support both GBA_U and GBA_ME, and the NAF specific protocol.

The interfaces to the other entities are:

- **Ub**: The interface between the UE and the BSF. It uses the HTTP Digest AKA protocol. It offers mutual authentication between BSF and UE and bootstrapping of the session keys.
- **Ua**: The interface between the UE and the NAF. The used protocol is application specific and it is secured by using the key material derived after the GBA procedure.

4.3.2 BSF

BSF is the basic entity for the bootstrapping procedure. The main requirements are:

- Support mutual authentication between UE.
- Agree on the session keys to be used later with one specific NAF and restrict the use of these keys to that particular NAF.
- Obtain the GBA User Security Settings (GUSS) from the HSS and keep track between these GUSS and the NAF that should be used.

The interfaces to other entities are:

- **Zh**: It is the interface between the BSF and the HSS. It uses the DIAMETER protocol and it should provide confidentiality, mutual authentication and integrity. It is used by the BSF in order to request and obtain an AV and the GUSS from the HSS.
- **Zn**: This interface is between the BSF and the NAF. The DIAMETER protocol is also used in this interface, which should provide confidentiality, mutual authentication and integrity. It is used for the NAF

to request the key material from the BSF and application specific user security settings.

4.3.3 HSS

The HSS, in the GBA context, provides the storage of all the user related information. The main requirements are:

- Provide storage of GUSS and mapping to one or more IMPIs of a subscriber.
- Specify the lifetime of the key to be derived for each user.
- Specify which type of UICC will be used by the user and thus if GBA_U is supported or not.
- It must also implement the **Zh** interface to BSF as already described.

4.3.4 NAF

NAF is the entity that the UE is authorized to. It does not need to have any security association with the BSF before the execution of the protocol. The main requirements are:

- Locate and communicate in a secure manner with the correct BSF. That is the BSF, which handles the authentication and the GBA procedures of the user requesting access.
- Acquire the key material from the BSF and the User Security Settings stored in HSS through the BSF entity.
- Check the validity and the lifetime of the key material.
- In the case of GBA_U, it should be able to determine and indicate the right key to be used.
- Implement the **Zn** interface, as described before.
- Implement the **Ua** application specific interface for communication with the UE.

4.3.5 GBA_ME

This section describes the basic GBA procedure without the UICC enhancements. Communication between entities is based on the HTTP Digest AKA [77] and the 3GPP AKA [58]. The messages' flow and the participating entities are shown in Fig. 4.5.

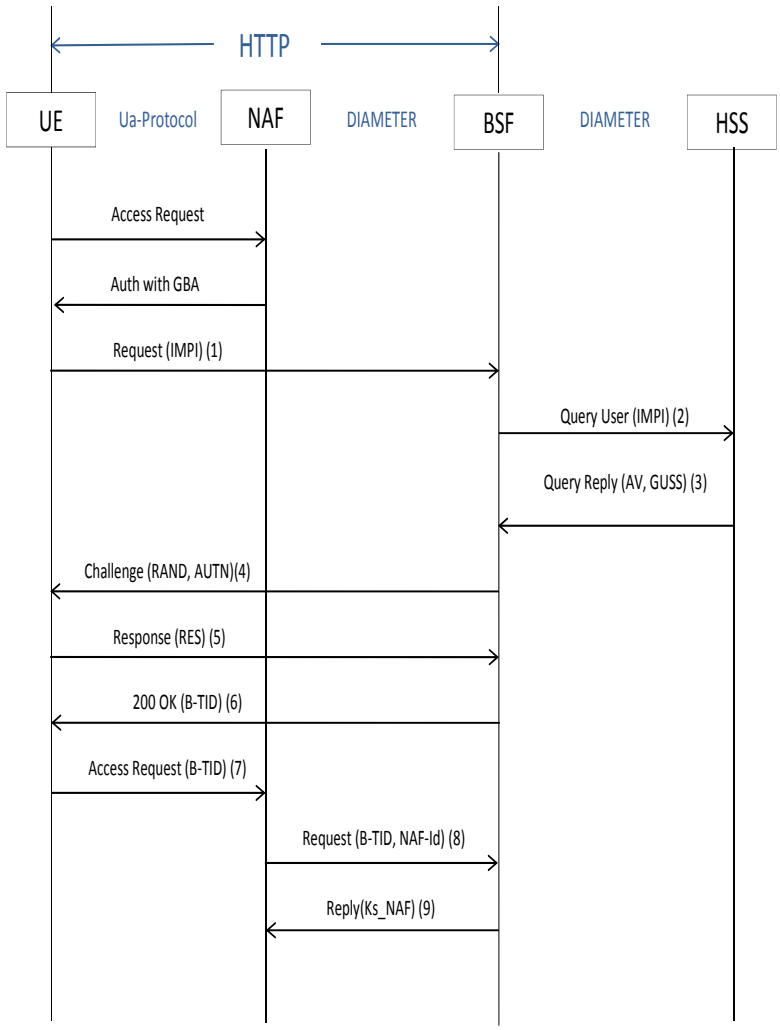

Figure 4.5 GBA Message Flow

First, the UE contacts the NAF and issues a request for accessing the service by using the specific protocol of the **Ua** interface. If authentication is needed, the NAF replies with an indication that the UE should initiate the GBA procedure.

In message 1, the UE using the **Ub** interface sends a HTTP request to the BSF, using the IMPI as username. The BSF looks up this IMPI in its local database. If

this is the first time that this particular user contacts the BSF, the BSF has to contact the HSS in order to receive the GUSS.

In messages 2 and 3, the BSF sends, through the **Zh** interface, a Multimedia-Auth-Request (MAR) according to the DIAMETER protocol, using the IMPI of the UE. The HSS replies with a Multimedia-Auth-Answer (MAA) containing the GUSS and one AV. The AV contains the RAND, AUTN, XRES, CK and IK, as specified in the previous section regarding the IMS Authentication.

In message 4, the BSF replies to the UE with a challenge in a “401 Unauthorized” response, as specified in [77]. This challenge contains the RAND and AUTN values. The keys CK, IK and the XRES value are excluded from the AUTN. The UE proceeds with the verification of the AUTN value to conclude if the challenge comes from an authorized network or not. Then, it calculates CK, IK and RES. The procedure for the verification of AUTN and the key derivation is the same as it was described in the IMS Authentication, and it is based on the secret key stored in the IMSI application. When this step is concluded, both UE and BSF share the same keys CK and IK.

In message 5, the UE send a HTTP AKA Digest response to the BSF, which is calculated using the RES value. Then, the BSF verifies the Digest response against the XRES value obtained previously by the HSS. If the response to the challenge of message 4 is correct, then the BSF proceeds in creating a Bootstrapping Temporary Identifier (B-TID). The B-TID is in the NAI format and it is created using the base64 encoded value RAND and the BSF’s server name. The BSF calculates the key Ks by concatenating the values of the keys CK and IK.

In message 6, the B-TID is sent to the UE in a HTTP 200 OK response together with the key lifetime value, indicating the success of the authentication procedure. The UE also calculates the key Ks by concatenating the values of the keys CK and IK.

Afterwards, both the UE and the BSF use the key Ks to derive the key material Ks_NAF. The derivation procedure is described in [59] and uses the following parameters:

- Ks : The key bootstrapped at the beginning of the process.
- “gba-me” : A string indicating the GBA mode that will be used .
- RAND : The random number sent from the HSS.
- IMPI : The user’s private identity.

- NAF_Id : The id of the NAF constructed by concatenating the Fully Qualified Domain Name (FQDN) of the NAF and an identifier for the Ua interface security protocol specified in [59].

In message 7, the UE sends the B-TID to the NAF, through the **Ua** interface, in order to allow the NAF to retrieve the corresponding key material from the BSF.

In message 8, the NAF contacts the BSF sending the B-TID and its NAF-Id, through the **Zn** interface.

In message 9, the BSF, after verifying the NAF-Id, replies with the Ks_NAF corresponding to the B-TID received. In case the NAF has requested User Security Settings and has the authorization to receive them, the BSF includes them in its reply.

After these steps, the NAF and the UE share a common key, the Ks_NAF, which can be used as a security association for the rest of the protocol used in the Ua interface. The NAF can implement an access control for UE using any application specific protocol. A use case scenario using HTTP Digest Authentication inside a TLS channel, is described in [78].

4.3.6 GBA_U

This mode of the GBA procedure was proposed in order to offer secure storage of the bootstrapped keys using the UICC card of the terminal. Messages exchanged between UE and BSF through the Ub interface are identical to the GBA_ME version. The main difference is that the Ks key is stored inside the UICC and only the derived Ks_ext_NAF key is passed to the GBA application on the ME.
After the message 4, as it is shown in Fig. 4.4, the UE passes the received parameters to the UICC. Identical to the GBA_ME mode, the UICC, using the shared secret key and the 3GPP AKA procedures, verifies the AUTN and computes the keys CK, IK and the value RES. The difference to the GBA_ME is that only the RES value is returned to the ME and sent back to the BSF. After the verification of the RES in the BSF, both UICC and BSF proceed on deriving two keys: the Ks_ext_NAF and the Ks_int_NAF. The Ks_ext_NAF is computed in the same way as the Ks_NAF key in GBA_ME. In order to differentiate the Ks_int_NAF the string "*gba-u*" replaces the string "*gba-me*" in the input parameters of the key generation procedure. Finally, the key Ks_ext_NAF is passed to the ME and the Ks_int_NAF is stored in the UICC.
A NAF can indicate to the UE if access to its services requires the use of GBA_ME or GBA_U. Furthermore, for security critical applications a NAF can indicate if the use of the Ks_int_NAF is needed. In such case, a challenge value is passed in the UICC, which uses the Ks_int_NAF key and produces a response.

The Ks_int_NAF remains always inside the UICC and only the computed response is passed to the UE. Then, it is sent to the NAF.

4.4 Group Signatures

Group signatures originally proposed in [50] can provide anonymity for a user inside a group. Group signatures were proposed to address the problem of showing membership in a group of users, which share some specified attributes. The goal is for a member to be able to convince a third party for his/her participation in the group. However, the third party should be able to induce nothing more (i.e. identity) than the user's membership. The basic properties, which a group signature should have, are the following:

i. Only members of the group are able to sign messages.
ii. The receiver of a message can verify the integrity of the message and if it is originated from a legitimate member. However, the receiver cannot link together signatures computed by the same user or identify the signer within the group.
iii. An authorized authority can open a given signature and disclose the signer under special circumstances (e.g., criminal investigation).
iv. An authorized authority can revoke a signer's ability to sign legitimate signatures.

Due to these properties, group signatures are suitable for offering authentication while also preserving location privacy. Namely, three major requirements for location privacy, anonymity, unlinkability and accountability are achieved. A group signature on a location sample proves to the receiver that the sample is created by a legitimate user, who is member of the authorized group. However, the user can be anyone of the group members. Moreover, the next signature from the same user is unlinkable to the previous one. The receiver cannot induce that the two signatures were signed with the same private key. Accountability is enforced because, when it is demanded by an authority, the entity, which manages the members of the group, can open a signature and identify the user.

In a group signature scheme there are three different types of actors, which are involved in creating the keys, signing and verifying the signatures.

- **Group Manager**: It is the entity administering the group. It can add new members in the group, revoke misbehaved members and open a signature to identify the signer. It is also responsible for creating the needed keys and administrating their distribution. The keys produced by the group manager are: 1) one group public key (*gpk*) 2) several private group secret keys (*gsk[i]*) for every user, member of the group and 3) a group manager secret key (*gmsk*). The group manager is the only entity that holds the mapping between the key of a user and its actual identity.

- **Group Members**: Entities that are given a valid secret group member key to sign legitimate signatures. Group members also have access to the group public key.
- **Verifiers**: Entities that receive the signed messages from the group members. Verifiers have access only to the group public key and they use it to verify a signature. In case that the scheme supports revocation, they might also have access to a Revocation List in order to discard signatures coming from revoked members.

The group manager has to implement the **Keygen, Open** and **Revoke** functions, group members the **Sign** function and verifiers the **Verify** function. Depending on the scheme the **Revoke** function might entail actions to be taken, either by both verifiers and group members or just by verifiers. The details of these functions are described below:

- **Keygen**: A randomized algorithm, which produces the keys needed for the system, namely the users' private keys *gsk[i]*, group manager's private key *gmsk* and the group's public key *gpk*.
- **Sign**: Takes as inputs a message *m*, the *gpk* and a user's *gsk*, then produces a signature σ.
- **Verify**: Takes as inputs a message *m*, the *gpk* and a signature σ, then it verifies if σ is a valid signature for *m*.
- **Open**: Takes as inputs a message *m*, the *gpk*, a signature σ and *gmsk*, then it can identify the user which issued the signature σ.
- **Revoke**: This function varies according to the given scheme. Two variations exist. In the first approach the group manager publishes periodically a revocation list and accordingly, the legitimate group members update their keys (private and public) while verifiers update the public key. In the second approach, for schemes supporting verifier local revocation, the group manager publishes a list of revocation tokens which only verifiers use when validating a signature. Group members do not need to change their keys.

Among the various group signatures schemes in literature, a scheme running on smartphones has to be efficient and to produce short length signatures in order to keep the computational and communication overhead low. Based on these requirements, two different schemes proposed in literature have been investigated and implemented in this research. The first scheme produces short signatures and is computationally efficient, since it does not require pairing-based computations for signing. However, the disadvantage is that unrevoked users must compute new keys every time a new revocation list is published. This problem is addressed by

the second scheme, which supports verifier local revocation. However, this comes with some additional computational cost.
The BBS scheme proposed in [79] is based on the Strong Diffie-Hellman assumption (SDH) and the Decision Linear assumption in bilinear groups. It generates signatures with short size and it does not require any bilinear pair computations for the signing operation (in other words, it keeps the computation cost on the smartphone lower). An interesting feature of the BBS scheme concerning signing, that is critical for a mobile application, is that several values for the computation of a signature can be pre-computed once and thus reduce the time needed for each separate signature. Signing a signature requires 8 multi-exponentiations and verifying requires 6 multi-exponentiations and one pairing computation. Furthermore, batch verification technics proposed in [80] can be applied to minimize the computational time of the verification. However, one drawback of this scheme is that it does not support verifier local revocation.
The second implemented scheme, is the BS scheme proposed in [81], which supports verifier local revocation. It is based on the same assumptions as the BBS scheme and revocation is implemented using an additional argument in the verification algorithm. In the BBS scheme the group manager publishes a Revocation List (RL) with the private keys of the revoked users, whenever some users need to be revoked. Using this RL, both signers and the verifier update their keys (both the private keys and the public key) according to an algorithm. After this step, signatures produced by valid signers can be successfully verified, whereas signatures by revoked users fail. The advantage of the BS scheme is that the RL is used as a parameter in the verification algorithm and thus, signers do not need to take any action in order to update their keys. Group members continue to use their old keys but the verifier can identify signatures that were computed with revoked keys. The signing operation of this scheme requires 8 multi-exponentiations and 2 bilinear map computations. Verification requires 6 multi-exponentiations and 3+2|RL| computations of the bilinear map. Thus the verification time is linear to the length of the RL. An optimization of the verification algorithm is also proposed, but in that case the drawback is that partial linkability is introduced.

4.5 GBA with Group Signatures

Our proposed architecture is shown in Fig. 4.6. The proposed improvement to the GBA architecture is the integration of a Group Signatures Center (GSC) with the NAF. The two entities (the NAF and the GSC) could reside on different physical servers; in this case, they communicate via a standard secure channel (e.g. using TLS [82]). Nonetheless, as they are both controlled by the mobile operator and reside in its network, we assume for the rest of the discussion that they reside on

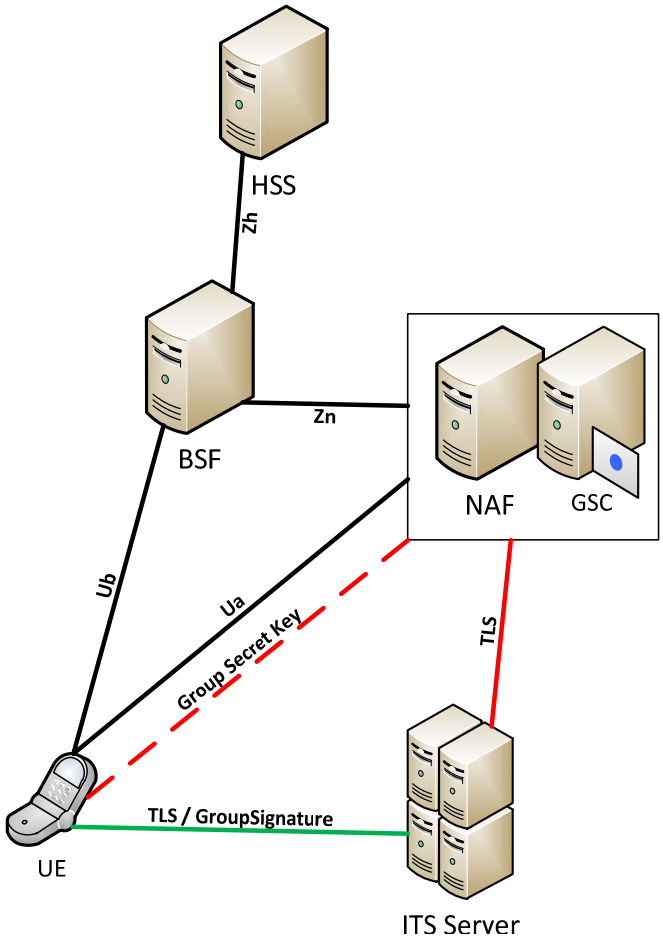

Figure 4.6 Proposed Architecture

the same physical machine. Regarding the group signatures in our system, the GSC is the group manager administrating the group whose members are all the participating smartphones. The ITS server is the verifier. The used GBA procedure could be the GBA_ME or the GBA_U, since this does not affect the functionality of our proposal. For simplicity, for the rest of the discussion in this chapter, the GBA_ME protocol is assumed. The messages' flow between the entities of the system is shown in Fig. 4.7.

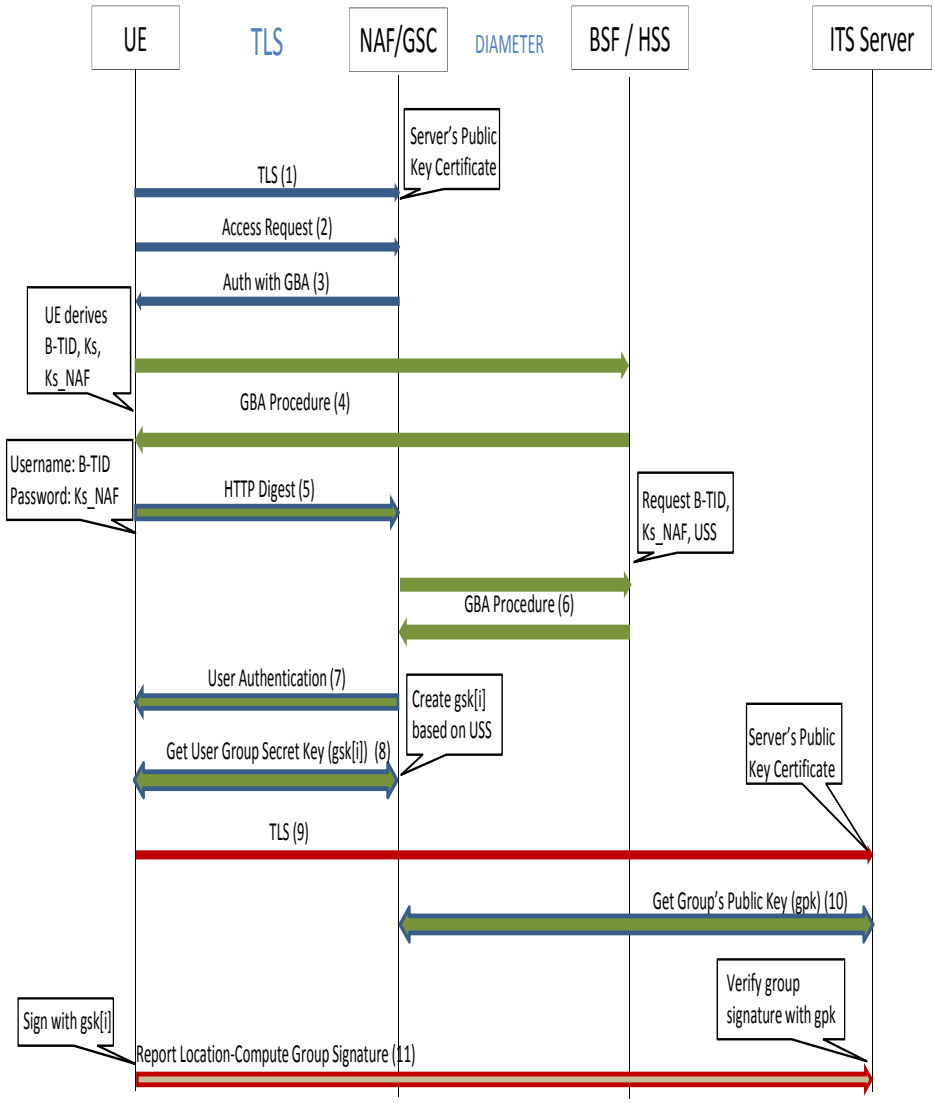

Figure 4.7 Message Flow

In steps 1-3, the UE contacts the NAF/GSC server for obtaining the private group secret key *gsk[i]*. The server's authentication to the client is implemented using TLS and a public key certificate installed on the server. The UE validates the certificate, with a preinstalled public certificate of a trusted authority, and proceeds in establishing a TLS channel with the server. The NAF/GSC server indicates to the UE that user authentication, by means of GBA, is required.

In step 4, the UE runs the GBA procedure with the BSF server, as described in the previous section. Finally, the UE obtains the B-TID and derives the Ks_NAF.

In step 5, the UE authenticates to the NAF/GSC using the HTTP Digest Authentication [83] inside the TLS channel. The authentication is based on the previously bootstrapped credentials as specified in [78]. The UE sends a HTTP request inside the TLS channel to the NAF/GSC, containing an Authorization header with the B-TID as username and the Ks_NAF as password for calculating the digest.

In step 6, the NAF/GSC runs the GBA procedure, described in the previous section, between the NAF and the HSS. Using the B-TID of the UE, it acquires the Ks_NAF and GUSS related to the user requesting access. The communication between the two parties is implemented using the **Zn** interface of GBA and the DIAMETER protocol. Both entities are supposed to be operated by the mobile operator, and security and privacy are provided by using standard TLS with public certificates. Then, the NAF/GSC proceeds with the authentication of the user, using the Ks_NAF and comparing it with the digest value.

In step 7, if the authentication was successful and the GUSS parameters supplied from the HSS indicate that the user is subscribed for accessing the ITS server, the NAF/GCS replies to UE with an authentication success message.

Then, in step 8, the NAF/GSC proceeds on creating the *gsk[i]* and sends it, together with the group's public key (*gpk*), to UE using the already established TLS channel. After this phase, the user is ready to start reporting location samples to the ITS server.

In step 9, the UE initiates a TLS connection to the ITS server. The ITS server's public key certificate is used to authenticate the server to the UE. This certificate should be signed by a trusted authority, providing PKI services. Its validity is checked in the UE using the preinstalled public certificate of the authority.

In step 10, the ITS server, in case it has not contacted the NAF/GSC server so far, contacts it and gets the *gpk* that will be used for the verification of the group signatures. There are no special security or privacy considerations for this part, besides the authentication of the NAF to the ITS server and the encryption of the

communication channel. This is required for the ITS server to be sure that it uses the correct *gpk*. Security for this part can be provided by means of standard TLS.

Finally, in step 11, for the UE to be authenticated to the ITS server, a hash of the message to be sent is produced and then the digital signature σ is computed, using the *gpk* and the *gsk[i]*. Finally, the message and the signature σ are submitted to the ITS server through the TLS channel established earlier. The server verifies the signature using the *gpk* that has been acquired from the NAF. Then, it accepts the message and authenticates the user or terminates the connection if the signature was not valid.

For a user to be identified, in case of misbehavior or at the authorities' request, the mobile operator and the traffic service provider must cooperate. Using the group manager's secret key (*gmsk*), the mobile operator can open the signatures in question and the user can be identified.

4.5.1 Revocation

When using the BBS scheme, for the misbehaving user to be revoked from the system, the *gpk* and each unrevoked user's *gsk[i]* must be changed. In this case, the GSC publishes a RL with the private keys of the revoked users and notifies the ITS server and the users that a new RL is available. The ITS server contacts the GSC directly to get the required parameters, while the users have to execute the authentication procedure from the beginning for assuring that only the unrevoked users will be authorized. Then, they proceed on calculating the new keys using the procedure specified in [79]. When using the BS scheme, the ITS Server contacts periodically the GSC to obtain the updated RL. Then, it proceeds with the verification of the signatures. Signatures originating from revoked users can be identified from the verification algorithm.

4.5.2 Security Analysis

4.5.2.1 Adversary Model

In order to examine the security of the proposed solution an adversary model is defined in this section. Adversaries, their position in the system and the possible threats that they can impose are defined here. In the following section, the detailed analysis for each type of threat is presented. Four different types of adversaries can pose threats in the targeted system. 1) outsiders, 2) the mobile operator, 3) the ITS server, 4) misbehaving users.

Outsiders: We suppose that an outsider can eavesdrop, remove, add and change a message on every link of the communications architecture except the interfaces **Zh**

and **Zn,** which belong to the mobile operator's internal network and thus, can be considered secured. Practically, the communication between the interfaces **Ua** and **Ub** is conducted using the mobile operator's cellular network and thus communication is protected through encryption in the physical layer. However, since access to IMS can be provided also through fixed internet providers, for analysis, we suppose that an outsider can interfere with these interfaces too.

The threats from an outsider can be the following:

- Impersonate an authorized user and acquire a valid group secret key.
- Impersonation of a legitimate user to the ITS server.
- Impersonation of the ITS server to a user.
- Access to location information sent to the ITS server.

Mobile operator: Since the mobile operator has already access to identity information of users, the requirement for users' privacy is to deprive access to the submitted location samples.

ITS Server: According to the privacy requirements for users, the ITS server can pose the following threats:

- Access any kind of identity information related to a user.
- Link subsequent location samples to a single source.

Misbehaving User: A misbehaving user can pose threats against the ITS server and its functionality. These threats can be the following:

- Report incorrect location information.
- Report multiple location information simultaneously.

4.5.2.2 Analysis

This section presents the security analysis, based on the adversary model defined before. Analysis is categorized according to each adversary and the threats that it can impose. For the rest of the discussion here, we assume that the adversaries, mobile operator and ITS server cannot cooperate against users in order to disclose his/her identity.

Outsider: A legitimate user is authenticated in the system using a group secret key *gsk[i]*. This key is transmitted from the NAF/GSC inside a TLS channel and user authentication is implemented by means of the GBA procedure. Messages 1-3, 5 and 7-8 are protected using TLS and the NAF/GSC public key certificate. An outsider residing in the link between UE and BSF, in step 4, could possibly get the

B-TID of the user, but not the key Ks_NAF, required for the rest of the GBA procedure. The procedure is based on a challenge-response scheme with a random number and no keys are exchanged between the two entities. So, even in possession of the B-TID, the outsider cannot be authenticated to the NAF/GSC in order to get a group private key. However, this can lead to possible Denial Of Service (DoS) attacks on the NAF/GSC and BSF. An adversary in possession of a valid B-TID or even with a random spoofed B-TID can use it to initiate the authentication towards the NAF/GSC. Even though the procedure will fail, the NAF/GSC would have to waste resources in order to contact BSF and run the procedure in order to derive the needed key material and finally to identify the unauthorized user. Another possible DoS attack can be applied if, for some reason an adversary is in position to produce valid RAND, AUTN pairs. Then, it can impersonate a BSF to the UE and force it into storing a fake B-TID. The UE will be able to realize that this B-TID is not from a valid BSF, only when trying to contact the NAF/GSC.

The signature computed on the submitted location sample is sent through a TLS channel encrypted using the ITS server's public key certificate. Thus, an outsider residing in the link between UE and ITS server cannot acquire a pair of message-valid signature and reuse it for reporting to the server.

Impersonation of the ITS server to the user is prevented by using a public key certificate. This certificate is signed from a trusted certification authority and its validity is checked by the UE.

Access to location information sent to the ITS server, in step 11, is prevented by using TLS and encryption using the server's public key in the link between UE and the ITS server. Moreover, the TLS channel provides integrity protection for data exchanged between the two parties. In this way, the integrity of the location samples reported by users and the integrity of the feedback provided by the server is protected.

Mobile Operator: Location samples, protected with the server's public key, are sent directly to the ITS server through the TLS channel, in step 11. The mobile operator cannot decrypt the location information sent to the ITS server inside the established TLS connection. Establishment of the TLS channel is based on the ITS's public key certificate and end-to-end encryption (i.e. between each user and the ITS server) is provided.

The mobile operator also acts as the group manager, since it is controlling the GSC entity. Thus, it knows the key *gsk[i]* that each user has obtained, it has access to the user's identity information (i.e. the operator controls the HSS entity) and furthermore the mobile operator can open a group signature, identify the *gsk[i]* key that was used and therefore disclose the identity of a user. However, because of the

use of TLS connection the mobile operator can not access the group signatures submitted by users. If the disclosure of a user's identity is needed then the ITS server must cooperate with the mobile operator. The location samples in question and the user's group signature are sent to the mobile operator and then using the *gmsk* key the signer can be identified.

It should be mentioned that location tracking of a subscriber's smartphone from the mobile operator is possible using network-based techniques. Also, linking this location with the user's identity is trivial since the operator controls the user's subscription in the network. Furthermore, in some countries it is mandatory for the operator to be able to locate a terminal with a given accuracy for emergency reasons. For example, in USA the E911 Phase II [84] requirements indicate that providers should be able to locate an emergency call in a range from 50m to 300m, depending on the type of location method used. However, these network-based methods used by the mobile operator depend highly on the environment and the network infrastructure topology and cannot provide the same accuracy as mobile-based methods, such as A-GPS. Disclosure of this information to third parties is allowed only if legally requested by a state authority or with the consensus of the subscriber.

Considering the previous observations and based on the existing trust of subscribers to the mobile operator, the proposed architecture leverages the operator as a trusted authority. On the other hand, continuously and more accurate location information, reported from smartphones to the ITS server, are protected. In this way, the mobile operator cannot access any additional information than it already knows.

ITS Server: As mentioned earlier, even the storage of anonymous sequential location samples can pose a privacy threat by allowing location tracking. However, in this proposal, the focus is on preventing the linking of samples based on some identifier. A misbehaving ITS server or an outsider getting access to the accumulated data cannot connect the location information with a specific user, since not identity information is transferred to the ITS server besides the group signature. The connection between sequential location data exists only as long as the UE is using the same TLS connection to the server. However, in a real case scenario, every time the application is started, a new connection will be established with the ITS server. These sequential connections, due to the properties of group signatures, cannot be linked together even when the UE is using the *gsk[i]*.

Another way for the ITS server to link sequential connections originating from the same user, is the IP address of the connection's source. Although, this type of network privacy wasn't the focus of this thesis, it should be noted that allocation of IP addresses depends on the mobile operator's network settings. Most of the

operators use dynamic allocation and thus the IP address of a device is changing frequently. For example, a study on the feasibility of locating smartphones based on their IP addresses [85] shows that IP addresses in 3G networks change frequently for most operators. Moreover, IP addresses don't embed fine-grained locality information that could be used in order to induce a smartphone's location from its IP address. However, in order to completely exclude this type of threat, other solutions, complementary to anonymous authentication, can be applied. For example, on the network operator's side an IP-Proxy server could be integrated, acting as an IP anonymizer.

Misbehaving User: The accuracy of the provided traffic information to the users of the ITS depends on the information provided by the participating users. Thus, even legitimate users when reporting erroneous data to the ITS server, can be the cause of malfunctioning and finally inaccurate traffic information. The accuracy of the supplied information depends on the location technique used on the smartphone and varies depending on whether network-based technique is used or A-GPS. Also, the environment (i.e. dense and high buildings in urban areas) can affect the accuracy of the provided location. Moreover, it should be assured that the smartphone does not fake its location. However, this is orthogonal to the topic of this thesis and also depended on the smartphone's software platform. For the rest of the discussion, it is assumed that the user cannot trick the mobile application into reporting a fake location. On the other hand, even without faking his/her location, a misbehaving user might be able to threaten the system's functionality.

In general, anonymous authentication introduces the problem of Sybil attacks against the ITS server. A misbehaving user could produce and sign multiple spurious location updates. These updates are reported to the server, impersonating in this way multiple legitimate users. Due to the property of unlinkability, the server can not link these updates to the same user and detect the abuse. In order to implement such kind of attack, a user has to extract the valid *gsk[i]* from the application, transfer it to another device and then connect it to the ITS server. The user initiates a TLS connection to the ITS server and then reports his/her location. The ITS server will verify the signature with the *gpk*, which was provided by the user. However, due to the properties of group signatures, as explained before, this signature originating from the second device and the signature from the first device, cannot be linked together. The ITS server obtains two different location samples coming from different devices (with different IP addresses) and considers them as coming from two different legitimate users. Using this attack, a misbehaving user can impersonate multiple users (i.e. vehicles) traveling on a particular street. One possible scenario is the ITS server to falsely estimate a traffic congestion on that street and accordingly, to send erroneous feedback to the other users traveling in the nearby area.

Traditional approaches with pseudonyms overcome these threats with time limited certificates without overlapping validity with each pseudonym used for one update [46]. This solution puts extra burden on management (e.g. for preloading sufficient pseudonyms), but it may very well be practical due to low computational costs and the low rates of updates (e.g., compared to safety applications). For approaches based on group signatures two different solutions can be applied.

The first solution requires the signing procedure and the storage of the secret key (*gsk[i]*) to be moderated by a secure hardware module (i.e. UICC card). A possible approach would be to utilize the GBA_U variation. As described in a previous section, with the GBA_U variation of GBA, a key Ks_int_NAF is derived and shared between the NAF entity and the UICC of the smartphone. However, this key is derived inside the UICC and furthermore never leaves the UICC card. This key could be used to encrypt the group signature key transferred from the NAF/GSC to the UE. The smartphone could not access it since it cannot access the Ks_int_NAF key. In this scenario, signing of a group signature would require the application to pass the location data to the UICC card. The responsible application inside the UICC would use the Ks_int_NAF to decrypt the gsk[i] key, then sign the signature and finally, pass the outcome to the ITS application. Nevertheless, implementation of this approach requires further investigation, mainly on the efficiency of group signatures implementation inside a UICC card.

The second approach, in order to avoid Sybil attack could be the enforcement of e-tokens schemes with limited number of valid authentication actions [54]. In this scheme, the client obtains, after authentication to the issuing entity (i.e. the NAF/GSC), a dispenser with *n* e-tokens. These e-tokens can be used for *n* number of anonymous and unlinkable authentications. The verifier (i.e. the ITS server) can verify the authenticity of the user by checking the submitted e-token. When the dispenser is expensed, the client requests another dispenser from the NAF/GSC. However, this scheme introduces higher computational cost comparing with normal group signatures.

4.5.3 Implementation

To evaluate our proposed solution, a full working testbed of the IMS architecture is needed in order to assess its scalability and performance. There is one open source implementation of the IMS [86], but unfortunately it does not support the GBA architecture. Therefore, the Mobile Web Security Bootstrap [87] library provided by Ericsson Labs, which offers an implementation of the GBA, was used. The library provides a GBA client running on the Android platform and a NAF server implemented in Java. The rest of the entities in the GBA (BSF and HSS) are run

and controlled by Ericsson Labs. A software emulated ISIM card holding the values is used:

- IMPI : Emulated private identity.
- IMPU : Emulated public identity.
- K : Emulated shared key.

For a user to be able to use the library, first his/her ISIM card must be registered in the Ericsson Labs system. Using the library's functions, which implement the GBA procedures, the client application bootstraps the B-TID and the Ks_Naf. These values are used for the client's authentication to the NAF/GSC entity. The NAF/GSC was implemented using Java Servlets and the client application on the smartphone was implemented in the Android platform.

The efficiency of our proposed approach can be affected by the following factors: 1) the efficiency of running the authentication protocol in the GBA 2) the efficiency of verifying each signature on the ITS server and 3) the efficiency of signing the signatures on the smartphones. The first factor can not be considered critical, since this procedure is executed only once by the smartphone's application in order for the user to be authenticated and to acquire the singing key (*gsk[i]*). Verification on the server side could be an issue, depending on the volume of signatures to be verified (number of simultaneous users). However, the ITS server is assumed to have enough hardware resources and moreover, batch verification solutions can be applied to optimize the performance of the verification algorithm [80].

The most critical factor is the computational effort needed to produce a group signature. Comparing with standard digital signatures, group signatures require more complex computations, based on bilinear pairings and thus, their feasibility on smartphones needs to be evaluated. Moreover, to the best of our knowledge, there are no public available implementations of group signature schemes for the Android platform that could be used in order to estimate the computational overhead to the proposed solution. As mentioned earlier, location samples submitted to the ITS server inside the same TLS channel can be trivially linked together. In every established TLS connection, the application on the smartphone needs to authenticate the user only once. This is implemented by submitting one group signature to the ITS server. Therefore the number of signing operations on the user's smartphone is equal to the number of different TLS connection to the ITS server in a time frame. Privacy-wise, the optimal choice is to establish a new connection for every new location sample to be submitted to the ITS server. However, this choice poses the maximum computational load on both the users'

smartphones and the ITS server. Further experiments, on a complete implementation of the system are required, before deploying, in order to find the optimum solution achieving balance between privacy and efficiency.

The sampling rate of smartphones' locations depends on two factors. The first one is the traffic estimation algorithm and the number of samples that are required to produce accurate traffic estimations. The second factor is the required privacy of users in relation with route tracking algorithms. Since the estimation of both these factors falls out of the scope of this thesis, we chose to compare it against two representative sampling techniques in order to evaluate the feasibility of group signatures on smartphones. The first technique uses sampling in a simple periodical manner. According to the analytical evaluation described in [88] for penetration rates between 3% and 5% (depending on the type of road) of vehicles reporting their location, a periodical sampling of 10sec is sufficient for providing adequate traffic information. The second technique uses a privacy preserving spatial sampling with VTLs. In this technique, reporting is done every time a vehicle crosses a VTL. The placement of VTLs is not fixed but determined by an algorithm which takes into account the penetration rate, the expected average speed of vehicles, and excludes sensitive, regarding location privacy, areas. We use as comparison margin the densest case. Based on the numerical results provided in [89], this is 8.6 VTLs per mile with 1%-2% penetration rate while vehicles' speed is expected to be 0-97 km/h. When using these parameters, the achieved mean travel time error is 5%. In such a scenario, the most demanding case for a vehicle would be to submit a sample and thus compute a signature about every 7.05 sec.

In order to have an estimation on the feasibility of group signatures, two different group signatures schemes, as described in section 4.4, were implemented. For the implementation, the Java Pairing-Based Cryptography Library (jPBC) was used [90], which is a Java port of the PBC library [91] that provides the mathematical

	X10i	**HTC Google Nexus One**	**X10i mini**	**HTC Legend**
BBS sign	4.107	4.103	8.736	9.545
BBS verify	6.635	7.787	15.905	15.808
BS sign	5.710	6.216	12.209	11.967
BS verify	8.335	8.953	17.793	17.033

Table 4.1 Sign/Verify Delays (Sec)

tools for pairing-based operations. To initialize the schemes, we used the Type A curve generator of the library with the default parameters (160 bits long group order r and 512 bits long base field q) offering 80 bits level of security according to [92]. The size of the final signature is 510 bytes for the BBS scheme and 360 bytes for the BS scheme. To optimize the execution time for the BBS scheme, the precomputation of variables suggested in [79], was used. Table 4.1 presents the time (in sec) needed for one successful signing/verifying operation, on different Android phones we experimented with. We should note that verification on the client side is not needed, but is presented here for completeness. As expected, the time varies mainly depending on the CPU of each model. The X10i and HTC Google Nexus One have a 1 GHz Scorpion processor while the two others a 600 MHz ARM 11 processor.

According to the margins described earlier, the efficiency of both schemes is acceptable, for both types of sampling techniques when using the first two smartphones with 1GHz processors (X10i and HTC Nexus One). For the rest of the tested smartphones, the BBS scheme requires acceptable time for the periodical sampling technique, but both schemes fall short for the VTL technique, since they require singing times over the 7.05 sec margin. Although the signing times appear relatively high in this implementation, they are not far from the demands for the specific type of the traffic management application. Further optimization of the cryptographic implementation or experimenting with different group signature schemes is possible to provide improved results. Finally, in order to draw a final conclusion on the scheme to be used, the whole system implementation must be taken into account. As already indicated, the frequency of location sampling depends on various factors that need to be precisely defined. Then, it would be possible to suggest a time frame for a smartphone to determine its position, sign a group signature and report it to the ITS server. This time frame would be used as margin for choosing the most suitable cryptographic primitive.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

Smartphones present great opportunities as traffic probes in future ITSs. However, one of the major challenges, until reaching smartphone-based ITS deployment, concerns the security of the system and the privacy of participating individuals. ITS's security is essential for guaranteeing the proper operation of the system and the trustworthiness of the provided feedback. Meanwhile, privacy concerns could be an important factor of users' reluctance to join an ITS. Therefore, in order to attract enough number of users it is of paramount importance to assure them about the privacy of their whereabouts. The focus of this thesis was the security and privacy of communications in a smartphone-based ITS. The goal was to identify the security and privacy requirements and to propose a solution fulfilling these requirements.

In order to secure the system's operations, it is necessary to implement an authentication and access control mechanism on the ITS server. In this way, only legitimate users will be able to report their location to the ITS. Moreover, misbehaving users must be excluded from the system and deprived the authorization to report their location and get feedback from the IST server. In order to identify misbehaving users, accountability must be enforced and the integrity of the exchanged messages between system's entities must be guaranteed. Regarding the privacy of the users in the ITS, three requirements have to be fulfilled. First, the user should be anonymous to other entities of the ITS, as well as to outsiders. The second requirement is unlinkability. Sequential location

samples submitted by a user should not be identified as originating from the same source. The last requirement regarding users' privacy is the confidentiality of messages. Only the authorized ITS server should be able to have access on the location information submitted by users.

Obviously, there is a conflict between security requirements for the ITS and privacy requirements for the users. Whereas the ITS demands every user to be authenticated in the system, this would directly violate the privacy of users inside the ITS. In such a case, the ITS server would have always a mapping between the identity of a user and his/her location. In order to mitigate this conflict we chose to split the two roles to different entities in the system, by applying the principle of separation of concerns. One entity is responsible for the authentication of users and the other one is responsible for handling location information and offering ITS services.

Chapter 4 of this thesis presented the proposed solution offering security and privacy in smartphone-based ITSs, which fulfills the aforementioned requirements. The proposed architecture provides privacy by design, separating authentication from location gathering and processing. For authenticating the users in the ITS, the GBA of the IMS is leveraged and further enhanced with the integration of anonymous authentication based on group signatures. Using GBA, a subscribed user acquires a private group signature key. Then, location samples are submitted to the ITS server in an end-to-end encrypted channel using TLS. Authentication of the ITS server to users is implemented with a public key certificate, while authentication of a user to the ITS server is implemented by computing a group signature on the submitted data. The ITS server is able to authenticate a legitimate user in order to grant access to the system. On the other hand, users remain anonymous to the ITS server and data sent is kept unlinkable and confidential. Even a misbehaving ITS server or an outsider getting access to the server's data, cannot trace and deduce the identity of a participating user. Data sent by the users are protected not only from outsiders, but also from the mobile operator. The mobile operator already knows roughly the location of a user through the network, but it cannot access additional and more detailed location information submitted by users. Finally, accountability with revocation of misbehaving users is achieved by the properties of group signatures. The ITS should send the suspicious location samples to the mobile operator in order for the group signatures to be opened. Then, the mobile operator can resolve the identity of the user who sent the sample.

The proposed approach enables the integration of various cryptographic primitives offering anonymous authentication. Two different group signatures schemes were implemented on smartphones. The BBS scheme and the BS scheme supporting

verifier local revocation. Results show the feasibility of this approach even though further optimizations could be applied in order to address the efficiency of these schemes on devices with low processing capabilities, such as smartphones.

Future work should investigate the exact time constraints requirements, taking also into account the location sampling algorithm used in the envisioned ITS. Based on this, the optimal cryptographic primitive should be chosen to be implemented. Another aspect to be further investigated is the protection of the derived anonymous credentials in the user's smartphone.

REFERENCES

[1] "Intelligent Transportation Systems Society." [Online]. Available: http://ewh.ieee.org/tc/its/. [Accessed: 25-Nov-2011].

[2] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84-95, Nov. 2009.

[3] "ITU Key Global Telecom Indicators for the World Telecommunication Service Sector." [Online]. Available: http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html. [Accessed: 25-Nov-2011].

[4] Y. Yim, "The state of cellular probes," 2003. [Online]. Available: http://escholarship.org/uc/item/8g90p0vw.pdf. [Accessed: 11-Oct-2011].

[5] D. Valerio, A. D'Alconzo, F. Ricciato, and W. Wiedermann, "Exploiting Cellular Networks for Road Traffic Estimation: A Survey and a Research Roadmap," *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*, pp. 1-5, Apr. 2009.

[6] H. Bar-Gera, "Evaluation of a cellular phone-based system for measurements of traffic speeds and travel times: A case study from Israel," *Transportation Research Part C: Emerging Technologies*, vol. 15, no. 6, pp. 380-391, Dec. 2007.

[7] 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," *Transportation Research Record*, vol. 1993, no. 1, pp. 51-58, Jan. 2007.

[8] "White Paper: How TomToms HDTraffic And IQRoutes Data Provides The Very Best Routing." [Online]. Available: http://www.tomtom.com/lib/doc/download/HDT_White_Paper.pdf. [Accessed: 25-Oct-2011].

[9] "Global mobile statistics." [Online]. Available: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats#smartphone-shipments. [Accessed: 20-Nov-2011].

[10] Globis Data Inc., B. Kirk, K. Fagan, and R. Renner, "Report: Development and demonstration of a system using cell phones as traffic probes," 2005. [Online]. Available: http://www.tc.gc.ca/eng/innovation/tdc-projects-its-d-its10-1140.htm. [Accessed: 13-Oct-2011].

[11] D. Work and A. Bayen, "Impacts of the mobile internet on transportation cyber-physical systems: Traffic monitoring using smartphones," in *National Workshop for Research on High-Confidence Transportation Cyber-Physical Systems: Automotive, Aviation, \& Rail, Washington, DC*, 2008, pp. 18-20.

[12] J. C. Herrera, D. B. Work, R. Herring, X. (Jeff) Ban, Q. Jacobson, and A. M. Bayen, "Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment," *Transportation Research Part C: Emerging Technologies*, vol. 18, no. 4, pp. 568-583, Aug. 2010.

[13] "Ford Sync." [Online]. Available: http://www.ford.com/technology/sync/. [Accessed: 13-Oct-2011].

[14] "BMW Connected." [Online]. Available: http://www.bmw.com/com/en/owners/bmw_apps/app_bmw_connected.html. [Accessed: 13-Oct-2011].

[15] V. Manolopoulos, S. Tao, S. Rodriguez, M. Ismail, and A. Rusu, "MobiTraS: A mobile application for a Smart Traffic System," in *Proceedings of the 8th IEEE International NEWCAS Conference 2010*, 2010, pp. 365-368.

[16] "Please Rob Me." [Online]. Available: http://pleaserobme.com. [Accessed: 13-Oct-2011].

[17] "Got an iPhone or 3G iPad? Apple is recording your moves." [Online]. Available: http://www.wired.com/gadgetlab/2011/04/iphone-tracks/. [Accessed: 13-Oct-2011].

[18] A. Brush, J. Krumm, and J. Scott, "Exploring end user preferences for location obfuscation, location-based services, and the value of location," in *Proceedings of the 12th ACM international conference on Ubiquitous computing*, 2010, pp. 95–104.

[19] J. Krumm, "Inference attacks on location tracks," in *Proceedings of the 5th international conference on Pervasive computing*, 2007, pp. 127-143.

[20] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: Why simple pseudonym change is not enough,” in *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, 2010, pp. 176-183.

[21] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Preserving privacy in gps traces via uncertainty-aware path cloaking,” in *Proceedings of the 14th ACM conference on Computer and communications security - CCS ’07*, 2007, pp. 161-171.

[22] B. Hoh et al., “Virtual trip lines for distributed privacy-preserving traffic monitoring,” in *Proceeding of the 6th international conference on Mobile systems, applications, and services, June*, 2008, pp. 17–20.

[23] “Foursquare.” [Online]. Available: https://foursquare.com/. [Accessed: 13-Oct-2011].

[24] “Apple Q&A on Location Data.” [Online]. Available: http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html. [Accessed: 13-Oct-2011].

[25] S. Amin et al., “Mobile century-using GPS mobile phones as traffic sensors: a field experiment,” in *Proceedings of the 15th World congress on ITS*, 2008, pp. 8-11.

[26] M. Gruteser and D. Grunwald, “Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking,” in *Proceedings of the 1st international conference on Mobile systems, applications and services - MobiSys ’03*, 2003, pp. 31-42.

[27] B. Gedik, “Location Privacy in Mobile Systems: A Personalized Anonymization Model,” in *25th IEEE International Conference on Distributed Computing Systems (ICDCS’05)*, 2005, pp. 620-629.

[28] B. Bamba, L. Liu, P. Pesti, and T. Wang, “Supporting anonymous location queries in mobile environments with privacygrid,” in *Proceeding of the 17th international conference on World Wide Web*, 2008, pp. 237–246.

[29] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, “Preventing Location-Based Identity Inference in Anonymous Spatial Queries,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719-1733, 2007.

[30] B. Gedik, “Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms,” *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1-18, Jan. 2008.

[31] H. Pagey, K. Hua, and C.-S. Lin, “Caching as Privacy Enhancing Mechanism in Location-Based Services,” *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, pp. 238-243, 2009.

[32] F. Liu, K. A. Hua, and Y. Cai, “Query l-diversity in Location-Based Services,” *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, pp. 436-442, 2009.

[33] F. Olumofin, P. K. Tysowski, I. Goldberg, and U. Hengartner, “Achieving Efficient Query Privacy for Location Based Services,” in *Privacy Enhancing Technologies*, vol. 6205, M. J. Atallah and N. J. Hopper, Eds. Springer Berlin Heidelberg, 2010, pp. 93-110.

[34] C.-Y. Chow, M. F. Mokbel, and X. Liu, “A peer-to-peer spatial cloaking algorithm for anonymous location-based service,” in *Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems - GIS ’06*, 2006, pp. 171-178.

[35] Y. Sun, T. F. La Porta, and P. Kermani, “A Flexible Privacy-Enhanced Location-Based Services System Framework and Practice,” *IEEE Transactions on Mobile Computing*, vol. 8, no. 3, pp. 304-321, Mar. 2009.

[36] M. Gruteser and H. Baik, “Protecting Location Privacy Through Path Confusion,” in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM’05)*, 2005, pp. 194-205.

[37] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Enhancing security and privacy in traffic-monitoring systems,” *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 38–46, 2006.

[38] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” in *2009 International Conference on Computational Science and Engineering*, 2009, no. March, pp. 139–145.

[39] “802.11p Standard.” [Online]. Available: http://standards.ieee.org/getieee802/download/802.11p-2010.pdf. [Accessed: 19-Oct-2011].

[40] “IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE).” [Online]. Available: http://www.standards.its.dot.gov/fact_sheet.asp?f=80. [Accessed: 15-May-2010].

[41] “1609.2-2006 IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages.” .

[42] “NOW: Network on Wheels.” [Online]. Available: http://www.network-on-wheels.de. [Accessed: 19-Oct-2011].

[43] H. Stübing et al., “simTD: a car-to-X system architecture for field operational tests,” *IEEE Communications Magazine*, vol. 48, no. 5, pp. 148-154, May 2010.

[44] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for Secure and Private Vehicular Communications,” in *2007 7th International Conference on ITS Telecommunications*, 2007, pp. 1-6.

[45] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening Privacy Protection in VANETs,” *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 508-513, 2008.

[46] P. Papadimitratos et al., “Secure vehicular communication systems: design and architecture,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[47] “Preciosa Project.” [Online]. Available: http://www.preciosa-project.org/. [Accessed: 20-Oct-2011].

[48] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, “Cross-layer privacy enhancement and non-repudiation in vehicular communication,” in *Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference*, 2007, pp. 1-12.

[49] K. Zeng, “Pseudonymous PKI for Ubiquitous Computing,” in *Public Key Infrastructure*, vol. 4043, A. S. Atzeni and A. Lioy, Eds. Springer Berlin Heidelberg, 2006, pp. 207–222.

[50] D. Chaum and E. Van Heyst, “Group signatures,” in *Advances in Cryptology—EUROCRYPT’91*, 1991, pp. 257–265.

[51] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks - VANET ’07*, 2007, pp. 19-28.

[52] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” in *Proceedings of the 3rd international symposium on Information processing in sensor networks*, 2004, pp. 259–268.

[53] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “On the Performance of Secure Vehicular Communication Systems,” *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 898 - 912, 2011.

[54] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, “How to win the clonewars: efficient periodic n-times anonymous authentication,” in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 201–210.

[55] A. Studer, E. Shi, F. Bai, and A. Perrig, “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs,” in *2009 6th Annual*

IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009, pp. 1-9.

[56] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[57] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in *2008 IEEE INFOCOM - The 27th Conference on Computer Communications*, 2008, vol. 8, pp. 1229-1237.

[58] 3GPP, "TS 33.102 V11.0.0 (2011-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 11)," no. 11. 2011.

[59] 3GPP, "TS 33.220 V11.0.0 (2011-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 11)," no. 11. 2011.

[60] G. Di Crescenzo, R. Morera, F. Vakil, and V. K. Varma, "A secure virtual point of service for purchasing digital media content over 3G wireless networks," *Security and Communication Networks*, vol. 1, no. 6, pp. 441–450, 2008.

[61] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic, and S. Khan, "Privacy in Mobile Web Services eHealth," in *2006 Pervasive Health Conference and Workshops*, 2006, pp. 1-6.

[62] J. A. MacDonald, "Authentication considerations for mobile e-health applications," in *2008 Second International Conference on Pervasive Computing Technologies for Healthcare*, 2008, pp. 64-67.

[63] V. Manolopoulos, S. Rodriguez, M. Ismail, and A. Rusu, "Security and Privacy Issues in a GPS-enabled Mobile Application for Smart Traffic - Abstract & Presentation," in *Smart Event 2010 in Smart Mobility Conference*, 2010.

[64] V. Manolopoulos and A. Rusu, "Secure and Privacy Preserving Access to Location-Based Services in 3G/4G Mobile Devices - Extended Abstract & Presentation," in *The 1st Security Conference - Europe*, 2010.

[65] V. Manolopoulos, P. Papadimitratos, S. Tao, and A. Rusu, "Securing smartphone based ITS," in *2011 11th International Conference on ITS Telecommunications*, 2011, pp. 201-206.

[66] G. Camarillo and M. A. Garcia-Martin, *The 3G IP Multimedia Subsystem (IMS)*, 2nd ed. Wiley, 2006.

[67] J. Rosenberg et al., "RFC 3261 SIP: Session Initiation Protocol," 2002.

[68] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, “RFC 3588 Diameter Base Protocol,” 2003.
[69] M. Poikselka, G. Mayer, H. Khartabil, and A. Niemi, *The IMS: IP Multimedia Concepts and Services, 2nd Edition*. Wiley, 2006.
[70] 3GPP, “TS 23.228 V11.2.0 (2011-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 11),” no. 11. 2011.
[71] B. Aboba and M. Beadles, “RFC 2486 Network Access Identifier,” 1999.
[72] H. Schulzrinine, “RFC 3966 The tel URI for Telephone Numbers,” 2004.
[73] 3GPP, “TS 31.102 V11.0.0 (2011-10) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 11),” no. 11. 2011.
[74] 3GPP, “TS 31.103 V10.1.0 (2011-04) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application (Release 10),” no. 10. 2011.
[75] 3GPP, “TS 33.203 V11.0.0 (2010-12) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 11),” no. 11. 2010.
[76] 3GPP, “TS 29.229 Technical Specification Group Core Network and Terminals; Cx and Dx interfaces based on the Diameter protocol; Protocol details,” no. 10. 2011.
[77] V. Torvinen and N. W. Group, “RFC 3310: Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA),” 2002.
[78] 3GPP, “TS 33.222; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS),” no. 10. 2010.
[79] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” *Advances in Cryptology–CRYPTO 2004*, pp. 1-19, 2004.
[80] A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, “Practical short signature batch verification,” *Topics in Cryptology–CT-RSA 2009*, pp. 309–324, 2009.
[81] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *Proceedings of the 11th ACM conference on Computer and communications security - CCS ’04*, 2004, pp. 168-177.

[82] T. Dierks and E. Rescorla, “RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2,” 2008.
[83] J. Franks et al., “RFC 2069 HTTP Authentication: Basic and Digest Access Authentication,” 1999.
[84] “Wireless 911 services.” [Online]. Available: http://www.fcc.gov/guides/wireless-911-services. [Accessed: 04-Nov-2011].
[85] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, “Where’s that phone?: geolocating IP addresses on 3G networks,” in *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, 2009, pp. 294-300.
[86] “OpenIMSCore.” [Online]. Available: http://www.openimscore.org/. [Accessed: 20-Oct-2011].
[87] “Mobile Web Security Bootstrap.” [Online]. Available: https://labs.ericsson.com/apis/mobile-web-security-bootstrap/. [Accessed: 10-Nov-2011].
[88] M. Ferman, D. Blumenfeld, and X. Dai, “An Analytical Evaluation of a Real-Time Traffic Information System Using Probe Vehicles,” *Journal of Intelligent Transportation Systems*, vol. 9, no. 1, pp. 23-34, Mar. 2005.
[89] B. Hoh et al., “Enhancing Privacy and Accuracy in Probe Vehicle Based Traffic Monitoring via Virtual Trip Lines,” *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1-1, 2011.
[90] “Java Pairing-Based Cryptography Library (jPBC).” [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/index.html. [Accessed: 20-Nov-2011].
[91] “Pairing-Based Cryptography Library.” [Online]. Available: http://crypto.stanford.edu/pbc/. [Accessed: 20-Nov-2011].
[92] N. Koblitz and A. Menezes, “Pairing-Based Cryptography at High Security Levels,” in *Cryptography and coding*, vol. 3796, N. P. Smart, Ed. Springer Berlin Heidelberg, 2005, pp. 13–36.