Chapter 15

On the Use of Optimal Stopping Theory for Secret Sharing Scheme Update

Constantinos Delakouridis
Athens University of Economics and Business, Greece

Leonidas Kazatzopoulos
Athens University of Economics and Business, Greece

ABSTRACT

The location privacy issue has been addressed thoroughly so far. Cryptographic techniques, k-anonymity-based approaches, spatial obfuscation methods, mix-zones, pseudonyms, and dummy location signals have been proposed to enhance location privacy. In this chapter, the authors propose an approach, called STS (Share The Secret) that segments and distributes the location information to various, non-trusted, entities from where it will be reachable by authenticated location services. This secret sharing approach prevents location information disclosure even in situation where there is a direct observation of the target. The proposed approach facilitates end-users or location-based services to classify flexible privacy levels for different contexts of operation. The authors provide the optimal thresholds to alter the privacy policy levels when there is a need for relaxing or strengthening the required privacy. Additionally, they discuss the robustness of the proposed approach against various adversary models. Finally, the authors evaluate the approach in terms of computational and energy efficiency, using real mobile applications and location update scenarios over a cloud infrastructure, which is used to support storage and computational tasks.

INTRODUCTION

Location-based services are becoming more popular than ever, mainly motivated by the convenience and leisure that they provide to everyday leaving, as well as by the availability of smart mobile phones that are equipped with ambient location appliances. The Mobile users’ location is estimated based on GPS sensors, triangulation, or proximity techniques. Then, they are assisted with navigation instructions, whilst sometimes much more intelligence is provided to avoid traffic jams, receive
proximity discounts from retails shops, restaurants, or pubs, pay insurance services proportionally to their driving ranges, enjoy different toll prices depending the distance covered on high ways, or locate the nearest point of interest. Teenagers, on the other hand, post location-tagged pictures or videos on social networks, upload geo-coded comments, receive in real-time distance calculations when running, discover nearby friends and socialized using proximity criteria.

But all these euphoria for mobile phones’ smart applications, intelligent location services and modern gadgets comes with a penalty. Legitimate service provides use location information for profit but without the previous consent of end-users, or they reveal location information to unauthorized third parties. Additionally, the location information is subject of inference or target by malicious attackers, traders, or marketers. The location privacy scheme, called Share The Secret (STS), originally proposed in (Marias et al., 2005), supports privacy using non-trusted servers. In this paper, we (1) enhance the basic STS algorithm in (Marias et al., 2005) to optimize the use of the location information distribution scheme, (2) apply consistency on combining location segments, (3) evaluate the STS scheme using real mobile devices and an “Infrastructure as a Service” (IaaS) cloud, and (4) discuss the robustness of the STS scheme against various adversary models.

In comparison to related location privacy approaches, the STS scheme enhances privacy even if adversaries have direct observation of the position of the end-user. Additionally, STS achieves privacy in cases where the multiple servers that store location information are compromised or collude to reveal the position of the end-user. Thus, non-trustworthy entities can be used to store and provide the location information. In the first prototype implementation, a cloud service was used for location information storage. Furthermore, a time-optimized location updating policy have been designed, so the location segmentation and updating procedure is limited, and, thus, information leakage to opponents is minimised. Finally, different privacy levels can be defined through various users’ profiles, policies or mobile applications that the users are registered.

The structure of the paper is as follows: Section 1 reports related work on location privacy. In Section 2 and Section 3 we introduce the STS scheme and discuss the basic modules and mechanisms. Section 4 reports robustness issues for the proposed scheme while Section 5 we evaluate the scheme using an IaaS cloud. In Section 6 we conclude the paper and discuss on going work.

PRIOR WORK

Several approaches that enable location privacy focus on the secrecy of Medium Access Control (MAC) identifiers or IP-layer address. On the MAC layer, the problem of interface identifiers is discussed in (Gruteser & Grunwald, 2003) that uniquely identify each client, allowing tracking of her location over time. The authors in (Gruteser & Grunwald, 2003) introduce a location privacy scheme through the frequent disposal of a client’s interface identifier. In the IP layer, Mobile IP (Fasbender et al., 1996b) implicitly addresses location privacy by associating two different IPs to the same subject (e.g., mobile user); (1) the static one, corresponding to the home network of the user, and (2) the dynamic one, corresponding to the current access network of the user. The Non-Disclosure Method (Fasbender et al., 1996a) considers the existence of independent, security (software) agents that are distributed on the IP network. Each security agent holds a pair of keys and forwards messages in an encrypted format. The sender routes a message to a receiver through the path determined by the security agents. Moreover, the Mist System (Al-Muhtadi et al., 2002) handles the problem of routing a message through a mobile network by keeping the sender’s location private from intermediate routers, the receiver and possible eavesdroppers. The Mist System consists
Related Content

Map-Based LBSs for Hiking: A Review of Requirements, Existing Solutions, and Future Trends
www.igi-global.com/chapter/map-based-lbss-hiking/67047?camid=4v1a

Deep Analytics in Sport Community Forums
www.igi-global.com/article/deep-analytics-in-sport-community-forums/209370?camid=4v1a

X3D-based Virtual Prototype Robot Mechanism Simulation
www.igi-global.com/article/x3d-based-virtual-prototype-robot-mechanism-simulation/131457?camid=4v1a

Development of Intellectual Property of Communications Enterprise and Analysis of Current Situation of Patents in Emerging Technology Field
Wenjia Ding (2013). Global Applications of Pervasive and Ubiquitous Computing (pp. 89-96).
www.igi-global.com/chapter/development-intellectual-property-communications-enterprise/72932?camid=4v1a