Toward Long-Term Quality of Protection in Mobile Networks

1Juluru Mallesh, 2Mrs. G. Satya Prabha

1PG Scholar, Department of ECE, SLC's Institute of Engineering and Technology, Piglipur Village, Hayathnagar Mandal, Near Ramoji Film City, Ranga Reddy District, Hyderabad, Telangana

2Assistant Professor, Department of ECE, SLC's Institute of Engineering and Technology, Piglipur Village, Hayathnagar Mandal, Near Ramoji Film City, Ranga Reddy District, Hyderabad, Telangana

Abstract

Sensor-equipped smartphones as well as wearable devices have undoubtedly become the predominant source of user-generated data in mobile networks. The proliferation of user-generated data has created a plethora of opportunities for personalized services based on the states of users and their surrounding environments. Those personalized services, although improving users’ perceived quality of experience, have raised severe privacy concerns, as most of these applications aggressively collect users’ personal data without providing clear statements on the usage and disclosure policies of such sensitive information. In order to sustain personalized services with long-term privacy preservation, disruptive paradigms are required. We envision that context awareness is a key pillar to providing long-term quality of protection (QoP) for individual privacy. In particular, users transit between different contexts, including mobility modes and social activities, and these contexts are temporally or logically correlated, which can be leveraged by adversaries to compromise users’ privacy. In addition, users may have different QoP preferences in different contexts. With these salient features in mind, this article investigates context-aware QoP mechanism designs for personalized services in mobile networks. We discuss possible attacks and propose corresponding countermeasures. In particular, we develop a QoP framework that exploits context awareness to achieve better trade-offs between service quality and privacy protection in long-term services. Finally, we provide some implications for future context-aware QoP mechanism designs by conducting a case study on smartphone traces.

1.INTRODUCTION

Due to continuing advances in low-power sensors and actuators, we are entering an era of rapid expansion in wearable and pervasive computing. Nowadays, it is
common for people to carry smart devices, such as sensor-equipped smartphones, smart watches, and healthcare devices. Those devices periodically measure users’ physical activities (e.g., Fitbit) and physiology, such as Samsung Simband with electrocardiogram (ECG) and photoplethysmogram (PPG) sensors embedded, making it possible to continuously track users’ contexts including mobility modes, social activities, and health conditions. These devices are normally capable of wireless connectivity, which enables them to upload their sensor readings to their service providers. Examples of these service providers include healthcare providers that own electronic medical record systems for users’ data collection and analysis, activity trackers that keep track of users’ trajectories or mobility modes, and environment-based applications that offer personalized services based on the operating conditions of users and their surrounding environments. On one hand, these services provided along with smart devices truly reap the benefits of context awareness to improve users’ quality of experience (QoE) [2]. QoE measures a user’s experiences with a service focusing on the entire service experience.

Context-aware applications optimize QoE by providing services tailored to users’ contexts. On the other hand, these services require users to continuously upload their personal data, which has imposed wide privacy concerns. Such privacy threats come from the fact that many service providers aggressively collect users’ data without providing clear statements about how to use the data and with whom the data will be shared. A recent survey studied 30 popular Android applications that have access to a user’s location, camera, and microphone data, and found that 15 of them sent users’ information to remote advertisement or analytics servers. Being aware of such risks, users may be reluctant to upload their data to service providers. However, this would also prohibit personalized services based on users’ data. Consequently, novel privacy preservation paradigms for personalized services in mobile networks are

2 PRIVACY THREATS FROM THE CONTEXT-AWARE PERSPECTIVE

QoP Preferences in Long-Term Services
Nowadays, location privacy is already a wide-ranging concern of both users and governments, as location traces can be used to infer many individuals’ behavior and preferences that users do not want disclosed. Context information, which provides more profound implications about users’ behavior and preferences, enlarges the range of sensitive information exposed to service providers. Today, many service providers aggressively collect much more personal data than is required to support their functionalities. Users, on the other hand, are sensitive about some contexts and corresponding sensor data the disclosure of which is undesired by them. Users’ QoP preferences can be categorized into the following two levels.

**Context sensitivity.** A user normally has a sensitivity preference on contexts. First, a user is sensitive to a subset of contexts. As illustrated in Fig. 1, a user might not want the contexts “in meeting” and “in hospital” to be learned by service providers, but she is willing to disclose the contexts “in café” and “walking.” In addition, a user has different levels of sensitivity.

**Data sensitivity.** The sensitivity level of sensor data is context-specific. For instance, a user may consider call logs during meetings as private information, while the user is sensitive to location information when she is at home.

3 Context-Aware Adversaries and Attacking Strategies —  
Adversaries include untrusted service providers and other entities that are interested in users’ private information and acquire users’ data by trading with service providers. Context awareness is a double-edged sword: it enables service providers to offer personalized services that substantially improve a user’s perceived experience, while also adding extra chances for adversaries to compromise users’ privacy. Different from the “single-shot” scenarios considered in many location and participatory sensing privacy preservation studies, contexts are temporally and logically correlated. Adversaries that are aware of this unique feature can compromise the user’s privacy by exploiting such correlations. Specifically, adversaries can infer the presence of sensitive contexts based on their previous observations in non-
sensitive contexts. Context-aware adversaries can be categorized into passive and active adversaries, as elaborated below.

**Passive adversary.** The adversary aggressively collects the user’s sensing data for offline analysis. The target of a passive attack is to obtain the user’s personal information and preferences, which are considered to be of great value.

**Active adversary.** The adversary launches real-time attacks based on the user’s instant context information. The adversary may push unwanted advertisements or context-based spams/scams to the user, or even make the user a victim of blackmail or physical violence. Different from a passive attack, an active attack has instant impact on the user and thus is observable to the user. Both types of adversaries can launch the following two types of attacks.

**Static attack.** A static attack follows predefined rules to acquire a user’s data and infer a user’s private information. The adversary may adopt certain models, such as Bayesian networks (BNs) or the hidden Markov model (HMM), to make inferences about a user’s sensitive information. The major limitation of the static attack is that it largely depends on the adversary’s background knowledge, and cannot update strategies according to the user’s actions.

**Adaptive attack.** An adaptive attack evolves over time by continuously tuning attack strategies or parameters. The adaptation is made based on new observations during long-term services. The adversary learns more accurate patterns of the user based on newly acquired data released by the user, and adjusts its attack strategies accordingly.

4 PROVIDING QOP AGAINST A PASSIVE ADVERSARY

Different from active adversaries, attacks by passive adversaries are not observable to the user. Thus, we adopt differential privacy as the data transformation technique, which makes no assumptions about adversaries’ background knowledge. As discussed earlier, the user’s data sensitivity varies over time due to context transitions. In our framework, we jointly adjust the releasing period and data transformation to minimize the overall data quality loss incurred by data transformation. The core idea is to use the data quality loss to guide the releasing period selection and enforce differential privacy by injecting randomness into each
selection. As we consider passive services, the sensor data does not require to be uploaded in real time. We assume that the maximal delay for data uploading is \( T \) time slots, and the data within the \( T \) time slots can be divided into \( K \) consecutive periods for data transformation and uploading. To this end, the framework first lists all possible periods, and computes the minimal data quality loss in each period that is required to guarantee the user’s privacy requirements. Then the framework randomly selects each period to ensure differential privacy. In order to guarantee differential privacy, the framework conforms to the exponential mechanism by selecting periods of less quality loss with exponentially greater probabilities to ensure differential privacy. Interested readers can refer to for detailed information about the exponential mechanism.

5 CONCLUDING REMARKS

This article has envisioned the crucial role of context awareness in achieving QoP in long-term services. Instead of focusing on protecting the user-generated sensor data in each context independently, context awareness exploits the correlations among different contexts and facilitates adaptive QoP paradigms. Through careful investigation of possible adversaries in long-term services, we have presented a context-aware framework and demonstrated its merits using real smartphone traces. Some observations in the smartphone case study can provide some implications for future designs of context-aware QoP provisions.

REFERENCES


