Chapter 44
Biometric Authentication in Broadband Networks for Location-Based Services

Stelios C. A. Thomopoulos
National Center of Scientific Research "Demokritos," Greece

Nikolaos Argyreas
National Center of Scientific Research "Demokritos," Greece

ABSTRACT

Broadband communication networks have begun to spread rapidly over fixed networks, with wireless networks following at close distance. The excess capacity allows the offering of broadband services at competitive rates. Location-based services (LBS) over wireless broadband networks are becoming mainstream in an emerging ambient intelligence society. For LBS over broadband and, in particular, peer-to-peer networks, such as ad hoc networks, unambiguous user authentication is of paramount importance to user trust and safety, thus ultimately to the success of such service. Biometric authentication is an approach to providing irrefutable identity verification of a user, thus providing the highest level of security. This chapter addresses some of the issues associated with the use of biometric ID for user and apparatus authentication over broadband wireless networks (e.g., GPRS, UMTS, WiFi, LANs) and narrow band local networks (e.g., bluetooth, Zigbee, PANs, BANs).

INTRODUCTION

The spreading of broadband networks stimulates a wealth of Internet services over fixed and wireless networks with stationary and mobile devices. Combining accurate location information from enhanced GPS infrastructures, such as EGNOS, Galileo …, with broadband wireless networks, provide the necessary infrastructure for delivering high quality and versatile location-based services (LBSs) ranging from travel information to entertainment, to crisis and incident management, to services on demand, to health care and peer-to-peer communications, to mention just a few.

DOI: 10.4018/978-1-4666-2038-4.ch044

In all these services, the common thread is the ability to unambiguously identify and authenticate the mobile user and customer to the LBS provider. Different LB services may have different authentication requirements. However, no matter what the application is all such services, the unambiguous authentication of the user is paramount to gaining the trust of the end user and thus achieving the success of the services. Unambiguous user authentication is paramount to the parties involved in an LB service and the trust upon which the service is built. If for example the LBS refers to the provision of transport services on demand, the ability to correctly identify and authenticate both parties involved in the transaction, that is the passenger (i.e., the user) and the driver (i.e., the service provider) build mutual trust and can be proved life-saving in the case of a car-jacking, criminal activity, or fraud.

User identification and authentication can be performed by a variety of means, ranging from a simple alphanumerical password to a more secure digital signature, to the ultimate in security biometric ID. Although a digital signature produced by an electronic device provides the convenience of a self-contained identification instrument, it does not prevent fraudulent use of a user ID. Since there is no unique and inherited connection between the user and the digital ID, any holder of the electronic device that produces the digital ID can produce a fraudulent authentication. The only means to eliminate such possibility is the use of biometric ID.

Biometric ID is a digital signature generated from the measurement of some bodily human characteristics that are unique, or different enough to be considered unique, from user to user. This Biometric ID, encoded properly, constitutes a unique signature for each user that cannot replicated by an impostor. This biometric ID can be used to meet the stringent requirements imposed by LB services and the necessary trust required by users and operators of such services alike. Examples of biometrics commonly used for user identification and verification include fingerprint identification, iris scan, face and voice recognition, signature recognition, hand geometry, and combinations thereof (Reisman & Thomopoulos, 1998; Thomopoulos & Reisman, 1993).

The use of biometric ID imposes certain restrictions and technological challenges that need to be addressed before biometric authentication becomes widely used as an enabling technology for irrefutable user authentication in LBS and other broadband services.

BIOMETRIC ID

A. Requirements for Biometric ID Usage

Biometric ID is the mathematical encoding of certain bodily features that are considered unique for each human being and differ enough from person to person so that this difference can be used safely enough to tell apart one person from another. For example, in the case of fingerprints, biometric features are the characteristic points that are formed from the endings or bifurcations of the finger ridges and/or the pattern of the ridges themselves. In the case of the iris scan, biometric features are the radial patterns of the iris. In the case of the face, biometric features are the relative location of the eyes, mouth, nose, and so forth.

The mathematical encoding of the biometric features constitutes what is referred to as biometric "template" or biometric ID (Thomopoulos, Reisman, & Papelis, 1996). No matter which biometric is used, the biometric features constitute unique and personal human characteristic and as such, they are protected by the Personal Information Protection Act (PIPA) (Personal Information Protection Act, S.A. 2003, c. P-6.5). This protection imposes a number of issues, concerns, and restrictions with the extraction (or capturing) of biometric features, their (electronic) storage, encoding into a biometric template and the