LocBiometrics: Mobile phone based multi-factor biometric authentication with time and location assurance

Ihsan A. Lami, Torben Kuseler, Hisham Al-Assam, Sabah Jassim*

***Abstract* — The continuing growth of Smartphones and Superphones has significantly increased mCommerce. The security of personal information on the phone and lack of the face-to-face identification has made the authentication process prone to identity theft and false impersonation. Biometric authentication offers personal identification but is missing the real-time and precise-position associated with the person. This paper proposes the use of freshly-generated real-time personal-data and present-position to form a "one-time multi-factor biometric" representation. i.e. using GPS "time and location" to stamp the user's fresh biometric data on the phone side, and then, the authenticator will compare this information with the position of the phone obtained independently from the cellular network at that instant in time.**

***Keywords* — Authentication, Cellular Towers, GNSS, GPS, Location, Multi-Factor Biometrics, Time**

I. Introduction

Mobile commerce over Smartphones/Superphones are becoming part of everyday life, enabling financial transactions to be performed anywhere, anytime by anyone. From personal security and authentication side, this has eliminated the traditional face-to-face based business transactions, e.g. inside a bank where all involved parties have the "who, where and when" clearly defined.

Traditional authentication factors can be broadly categorised into three groups [1]. 1) knowledge-based, or something you know, which typically relies on a memorised password or a PIN. 2) object-based, or something you have, which relies on a physical possession such as tokens. 3) Identity-based, or something you are, i.e. biometrics, which relies on the uniqueness of physical or behaviour characteristics of a person such as fingerprint, facial features, iris, or voice. A random password can offer an extremely strong security mechanism for user authentication. However, in practice, secret passwords that humans can easily remember are often short and easy to guess [1]. On the other hand, the major security drawback of a physical token is that, if lost or stolen, an impostor can gain unauthorized access. In biometric-based authentication, a legitimate user does not need to remember or carry anything and it is known to be more reliable than traditional authentication schemes. However, the security of biometric systems can be undermined in a number of ways. For instance, a biometric template can be replaced by an impostor's template in a system database or it might be stolen and replayed [2].

Current and future generations of Smartphones and Superphones have enough gadgets and sensors that can be deployed to enable "secure data and authentications" for mCommerce. These sensors include camera, finger print sensor, and GPS receiver. For example, location applications can determine the phone position via the GPS data, via the cellular network base station/tower triangulation, via Wi-Fi by approximating the distance to a known Wi-Fi Access point, or via a combination of these. Equally, biometric data can be collected for the face, voice, palm vain, or finger print of the person.

For mCommerce, intelligent biometric-based authentication and verification will help identifying the person (the "who"), while the GPS data and wireless connectivity can identify the exact time (the "when") and location of person (the "where") as well as the "collected biometric data". This information, when coupled/compiled with secure data connection (using SSL for example) and data integrity checking algorithm (e.g. hashing) to form a one-time multi-factor biometric (OTMFB) representation, shall offer a novel and attractive authentication process for Smartphones and Superphones to increase security and to identify and defeat distance attacks from intruders.

Furthermore, this paper proposes a novel approach that uses the cellular towers as a second source of location information, which is completely independent from the first location source (GPS receiver on the device) to strengthen the security of the application. Cellular towers controlled by network operators continuously locate mobile phones during their normal operation, and most operators in the US, for example, uses this location method to comply with the FCC-9-1-1 requirements [3]. i.e. this cellular network based phone location information will be used to cross-check the phone position received from the GPS receiver on the device itself, independent of the phone-user.

The work presented in this paper complements the previously proposed enhanced multi-biometrics authentication technique [4] with the assurance of time and location. By conjunction of multi-modal biometric-

*Ihsan Alshahib Lami, Torben Kuseler, Hisham Al-Assam and Sabah Jassim are with the Applied Computing Department, University of Buckingham, Hunter Street, Buckingham, MK18 1EG, UK (phone: 44-1280-814080; email: first.last@buckingham.ac.uk).

based verification, a user password and two-way independent localisation of the mobile device user, the three issues of "who, where, and when" can now be clearly identified in any remote and mobile secure transaction.

The rest of the paper is organised as follows: Section II provides an overview of related work in multi-factor biometric authentication and GPS. Section III describes the proposed LocBiometrics algorithm. Section IV concludes the results and outlines future work.

II. Background & Related work

GPS location and time data has been used to derive a unique signature to discover ground distance and cyberspace attacks [5]. Such a generated signature can be added to documents or digital transactions to verify that the document was created or changed at this unambiguous defined place and moment in time. The idea is that, every bit value from the satellite signals, and accordingly the generated signatures, changes every 20 milliseconds. Therefore, an intercepted signature cannot be reused by an attacker to perform a replay attack with a faked location. However, the standard GPS receivers used in today's mobile devices are not suitable for the generation of such required unique signatures because they calculate latitude, altitude and longitude values directly from the GPS signals. This can enable attackers to generate their own set of coordinates to forge their real location. In consequence, the authenticator cannot be sure if the position was really calculated by a GPS receiver on the mobile device or was faked by an intruder.

Another proposed solution uses position and time as an additional factor of authentication to reduce identity theft [6]. A major problem in today's mobile business world is identity theft and impersonation. Around 10 million Americans were hit by identity theft in 2008, an increase of 22 percent compared to the previous year [7]. So, this solution compares the received current position of the mobile device with a database of pre-known positions of the points of business agreed / associated with the mobile phone user, e.g. an ATM machine. i.e. a continuous location tracking of the device, as well as a continuous online verification system is established to do this. However, continuous tracking of mobile devices to ensure that no anomalous behaviour has occurred at any point in time is very difficult. The devices could be switched off by the genuine user, run out of battery power, or monitoring range. Another drawback is that the point of sale must be pre-known by the verifying side which is not always the case in mobile business.

In the recent past, several publications have proposed the use of Multi-Factor Biometric Authentication (MFBA) to enhance both security and accuracy of biometric systems using different modalities such as fingerprints [8], facial features [9], iris [10] and palm features [11]. An example of a two-factor biometric authentication is the User-Based Transformation (UBT). Typically, UBTs employ transformation keys generated from passwords/PINs or retrieved from a token. Random orthonormal projection can be consider as a simple but effective UBTs [12]. This uses random orthonormal matrices to project biometric features into other (secure) spaces where the distances among the data points before and after the transform are preserved. Although MFBA systems offer better security when certain requirements are met [13], replay attack remains one of the challenges that current MFBA systems are unable to prevent.

III. LocBiometrics Algorithm

The LocBiometrics process ensures that the biometric features do belong to the genuine and physically-present user by stamping his/her real-time collected and generated biometric data. i.e. the tight combination of a real-time biometric generated key (who actually you are now), a password (something secure you only know), with location (where you are now) and real-time shall strengthens the security of the authentication process.

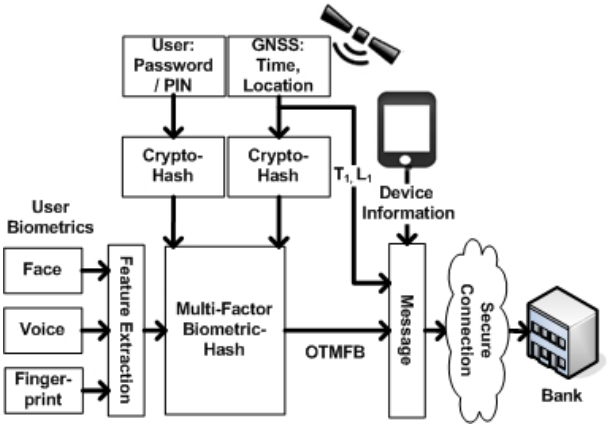

Fig. 1. OTMFB message generation process

To achieve this, genuine users need to enrol their biometrics (e.g. face, voice and/or fingerprint), a password/PIN and the locations where he/she is likely to operate with their business partner. i.e. a biometric template is generated out of the presented biometrics and stored together with a hashed value of the chosen user password/PIN and the area of user operation. Once the user needs to perform a secure transaction with the business partner, an authentication process is triggered as shown in Fig. 1. The proposed multi-factor biometric-hash algorithm combines the user fresh biometrics from the mobile phone sensors with the password, then uses the hashed GPS time and location values to produce a one-time permutation to be applied on the biometric features. A proprietary pseudo random permutation generation scheme is used. This scheme relies on DES-like S-boxes to produce a secure one-way permutation for any given seed. Then a user-based random orthonormal projection [12] is generated from the password/PIN to transform the biometric features to a secure domain. The generated One Time Multi-Factor Biometric (OTMFB) representation is sent together

with the actual GPS time, location, information about the used mobile device and the actual transaction message over a secure connection to the authenticator side (e.g. a bank).

The current time and position of the device are the critical one-time factors that will be employed every time to prevent the replay attacks .The time and position will be thereby extracted from the GGA (Global Positioning System Fix Data) message generated every second by the GPS receiver [14].

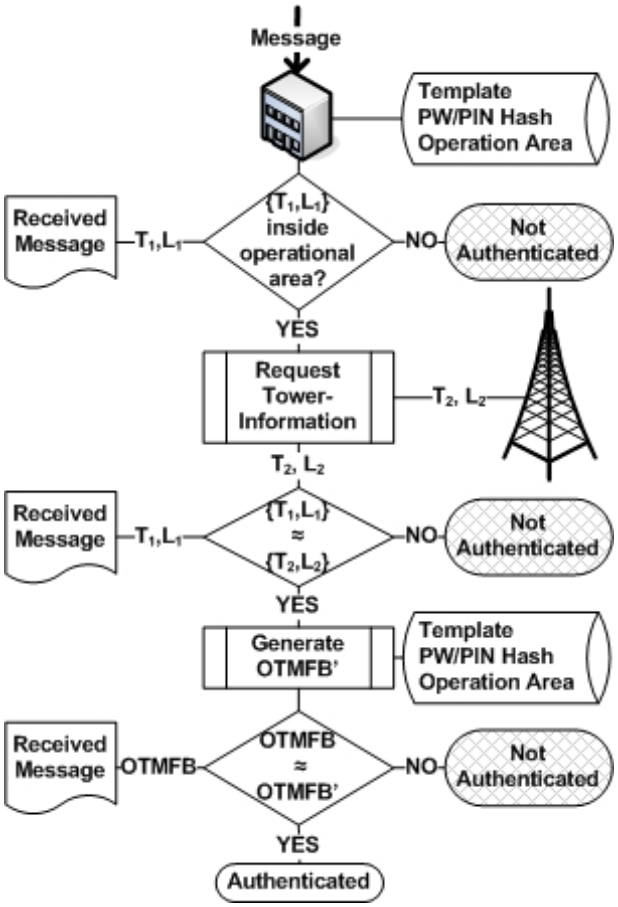

Fig. 2. User verification process

During the verification process (see Fig. 2.), the authenticator extracts the time, location, OTMFB and device information from the message and verifies, as a first step, that the transmitted location is inside the agreed area of operation of the particular device and user. It follows this by requesting the current position of the phone from the cellular network operator, using U-TDOA of signals from the serving and secondary base stations around that phone at that time, shown in Fig. 3. The U-TDOA user verification process of cellular signals reaching different network towers in range of the mobile device can achieve an accuracy of approximately 50 meters, depending on the area of operation [15].

So, the authenticator shall verify that the device is actually at the claimed location by comparing the transmitted GPS position from the phone and the position gained from the network operator. If the location difference is within a certain threshold, the device is confirmed to be at the claimed position at that point in time. The authenticator will then use the enrolled biometric template, the password/PIN hash value as well as the time and location information to generate a fresh local OTMFB'. This is compared with the received OTMFB from the user to verify the user is genuine and to ensure that replay attack has not occurred.

IV. Results

To test the viability of the proposed scheme, fingerprint and face biometrics are used in the way described in [12]. Let x_1, x_2 be two fixed size biometric feature vectors of a user extracted from a face or a fingerprint (say x1 is freshly extracted for authentication and x2 is saved during the enrolment stage in an enterprise database), the Euclidian distance that is used at the matching stage between the two vectors is given by:

$$\|x_1 - x_2\|^2 = \sum_{i=1}^{n}(x_{1i} - x_{2i})^2 = (x_1 - x_2)^T(x_1 - x_2) \quad (1)$$

Let y_1, y_2 be the two OTMFB representations of x_1, x_2 created by our proposed scheme, the Euclidean distance between y1, y2 will be as follows:

$$\begin{aligned} \|y_1 - y_2\|^2 &= (y_1 - y_2)^T(y_1 - y_2) \\ &= (PAx_1 - PAx_2)^T(PAx_1 - PAx_2 -) \\ &= (x_1 - x_2)^T PA^T PA(x_1 - x_2) \\ &= (x_1 - x_2)^T O^T O(x_1 - x_2) \\ &= (x_1 - x_2)^T I_n(x_1 - x_2) = (x_1 - x_2)^T(x_1 - x_2) \\ &= \|x_1 - x_2\|^2 \end{aligned} \quad (2)$$

Where O=PA is an orthonormal matrix.

The Euclidean distances between the two OTMFB representations of a user equals to the Euclidean distances between the two feature vectors of his biometric samples. However, experiments show that when x1, x2 belong to two different individuals (i.e. a user-based P and A are used), the Euclidean distances increase which results in better security and accuracy.

Several measurements of phone-GPS position at various locations and comparing these to positions obtained from the cellular network serving the phone at that location has concluded that an error of up to 300 meters can result. This is deemed to be OK for the purpose of this authentication process.

V. Conclusion and Future Work

In conclusion, this paper proposes a novel technique to verify the claimed position of a user within a remote business transaction. The combination of two independent positions obtained (GPS/GNSS receiver on the mobile device and cellular towers controlled by the network operators) to locate and verify the claimed

position of a mobile device will limit the fraud-attack possibilities and avoid certain distance attacks commonly existing in various identity theft scenarios. This is then combined with multi-model biometric verification to establish a multi-factor authentication based on various biometric data (e.g. face, voice or fingerprint), a user password as well as location and time information. Integration of time and location into the authentication process ensures that it is a secure-live communication and thus reduces the possibility of replay attacks.

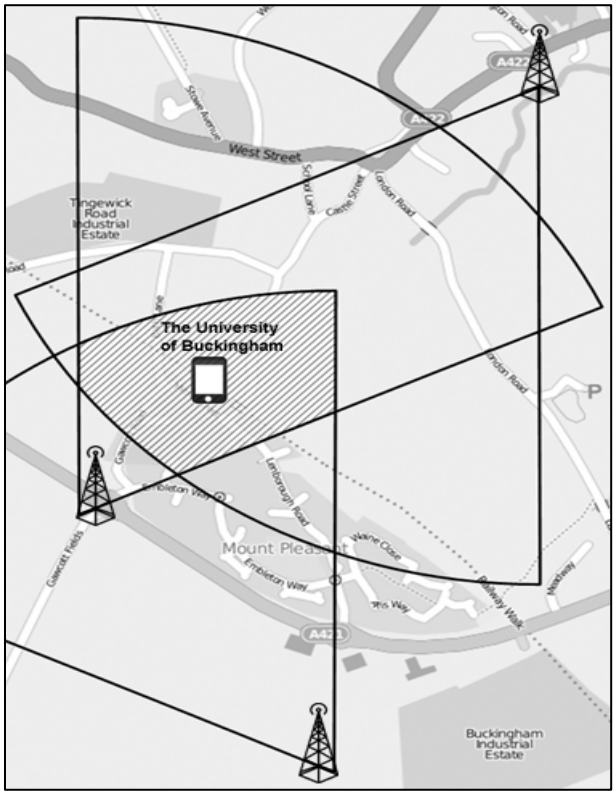

Fig. 3. Accuracy range of towers vs. GPS

Work on this LocBiometrics algorithm is ongoing to further combine the real-time and location information coming from the GPS receiver to become an essential and completely integrated part of the generated One Time Multi-Factor Biometric on the device. i.e. only one hashed version of the information is sent over the secure connection. Also, the verifying side will use the time and location information received from the second independent source (the cellular towers) together with the pre-enrolled biometric template and user password to securely identify the user and to verify the claimed position of the device.

REFERENCES

[1] S. Z. Li and A. K. Jain, Eds., *Encyclopedia of Biometrics*. Springer US, 2009.

[2] K. Nandakumar, "Multibiometric systems: fusion strategies and template security," Ph.D. dissertation, East Lansing, MI, USA, 2008, adviser-Jain, Anil K. [Online]. Available: http://-www.cse.msu.edu/biometrics/Publications/Thesis/-KarthikNandakumar_MultibiometricSystems_PhD08.pdf

[3] U.S. Federal Communications Commission, 9-1-1 Service. [Online]. Available: http://www.fcc.gov/pshs/services/911-services/

[4] T. Kuseler, I. Lami, S. Jassim, and H. Sellahewa, "ebiometrics: an enhanced multi-biometrics authentication technique for real-time remote applications on mobile devices," in *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, ser. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, S. S. Agaian and S. A. Jassim, Eds., vol. 7708. SPIE, apr 2010, pp. 77080E.1–77080E.9. [Online]. Available: http://link.aip.org/link/?PSI/7708/77080E/1

[5] D. Denning and P. MacDoran, "Location-based authentication: Grounding cyperspace for better security," *Computer Fraud and Security Bulletin*, Feb 1996.

[6] P. C. van Oorschot and S. G. Stubblebine, "Countering identity theft through digital uniqueness, location cross-checking, and funneling," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, A. S. Patrick and M. Yung, Eds., vol. 3570. Springer, 2005, pp. 31–43.

[7] K. M. Finklea, "Identity theft: Trends and issues," Congressional Research Service, CRS Report for Congress, 2010. [Online]. Available: http://www.fas.org/sgp/crs/misc/-R40599.pdf

[8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 1–17, 2008.

[9] H. Al-Assam, H. Sellahewa, and S. Jassim, "A lightweight approach for biometric template protection," in *Proceedings of SPIE*, vol. 7351, March 2009, pp. 73510P.1–73510P.12.

[10] L. Nanni and A. Lumini, "Empirical tests on biohashing," *Neurocomputing*, vol. 69, no. 16-18, pp. 2390–2395, 2006.

[11] T. Connie, A. T. B. Jin, M. G. K. Ong, and D. N. C. Ling, "Palmhashing: a novel approach for dual-factor authentication," *Pattern Anal. Appl.*, vol. 7, no. 3, pp. 255–268, 2004.

[12] S. A. Jassim, H. Al-Assam, and H. Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," in *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis (ISPA)*, 2009, pp. 556 – 561.

[13] H. Al-Assam, H. Sellahewa, and S. A. Jassim, "Multi-factor biometrics for authentication: A false sense of security," in *Proceedings of the 12th ACM Workshop on Multimedia and Security*, 2010, pp. 81–88.

[14] *NMEA 0183 - Standard for interfacing marine electronic devices, Version 4.00*, National Marine Electronics Association Std., 2008.

[15] TruePosition, "U-tdoa: Enabling new location-based safety and security solutions," White paper, October 2008.