COMMUNICATION SECURITY: BIOMETRICS OVER WIRELESS NETWORKS

Charu Sharma*

Kanika Aggarwal**

ABSTRACT

Biometrics is a technology for authenticating a person's unique identity with security, speed and ease of use. Biometric techniques relied on a person's fingerprint, palm, iris, voice recognition, and other features of a person. Biometrics authentication requires an encrypted mechanism to securely transmit data over a network. Various access networks today are the Global System for Mobile (GSM) wireless communication network which enables digital wireless duplex communication with security and data encryption algorithms build in, Fiber-to-the-premises (FTTP) network which provide a large bandwidth to the enterprise and the Wireless Biomedical Sensor Networks (WBSNs) which are used to gather real time and continuous medical data from different parts of the human beings. Biometrics approach is an efficient way to overcome the insecurity of the wireless biosensor networks. The technology will allow customers of wireless services and products to authenticate their identities when conducting electronic transactions. This paper also describes the advantages, disadvantages and defines how biometrics has helped securing data in wireless networks.

*RIMT, Mandi Gobindgarh, Punjab.

**SCDL, Pune, Maharashtra.

I. INTRODUCTION

Biometric technology refers to any technique that reliably uses measureable physiological or behavioral characteristics of distinguish one individual from another. The characteristics like fingerprint, facial, thumb expression, voice, signature varies from person to person and biometrics uses these characteristics for national security and identifies theft prevention.

Wireless communication may be used to transfer information over short distances or long distances. It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs).

By combining biometrics with wireless communications as an overlay to existing access control systems, entry and admission become more convenient for the user. This is the ultimate in security like universal hands-free access, validated by unique human characteristics. The combination of fingerprint recognition and wireless communication allows new areas of biometrics integration.

As biometrics systems improve, become smaller and require less power for operation, the potential to integrate into new application grows.

The biometrics is used in various wireless communications like GSM wireless network, Biosensor networks, FTTP network etc.

II. BIOMETRIC DATA OVER ACCESS COMMUNICATIONS NETWORK

ID verification and access authorization gives a comparison of features extracted from a biometric device and the restored features in a database. Figure 1. Shows Access/denial of the biometric communications network.

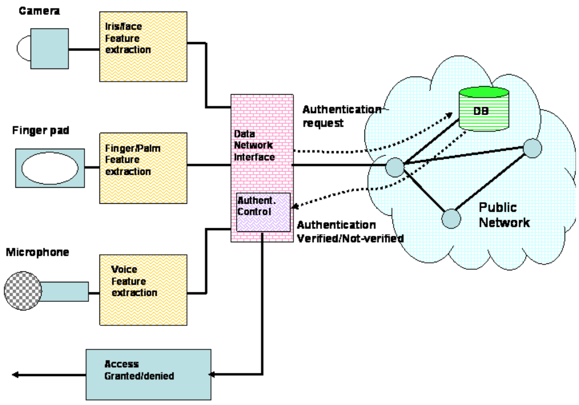

Figure 1. Access/denial of the biometric communications network

If the database is remote, there are two possibilities:

A. The biometric database may be centralized. The Biometric apparatus extract features and transmits them over the network to a remote central database for comparison and verification. Results are sent back to the authenticating apparatus over the network to grant or deny access.

B. The biometric database may be distributed. A biometric apparatus may maintain its own local database and it periodically updates a regional database, and so on. In this case, verification and authorization is fast and it does not risk unauthorized interception for each verification/authorization.

III. THE GSM WIRELESS NETWORK

The global system for mobile (GSM) wireless communications network enables digital wireless duplex communications with security and data encryption algorithms built in. The GSM network consists of four mfunctional components: the mobile station (MS), the network switching system (NSS), the Base Station System (BSS) and the Operation and Support System (OSS), Figure 2.

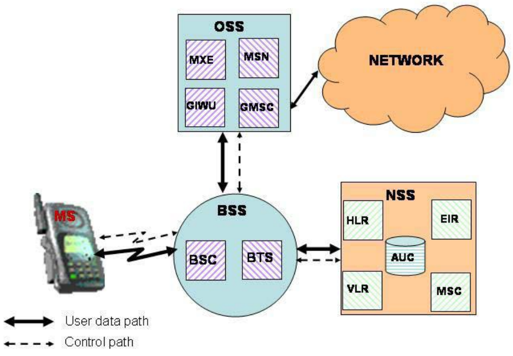

Figure2. Major functional components of GSM network

Among the major functional components of the GSM network, the network switching system (NSS) is more responsible for GSM security aspects. The NSS consists of the Home Location Register (HLR), the Equipment Identity Register (EIR), the Visitor Location Register (VLR), theMobile Services Switching Center (MSC), and the Authentication Center (AUC).

- The Home Location Register (HLR) stores data about GSM subscribers, including the Individual Subscriber Authentication Key for each Subscriber Identity Module.
- The Equipment Identity Register (EIR) contains information about the identity of mobile equipment preventing making calls from stolen, unauthorized, or defective mobile stations.

- The Visitor Location Register (VLR) temporarily stores information about roaming GSM subscribers.
- The Mobile Services Switching Center (MSC) performs telephony switching functions and is responsible for toll ticketing, network interfacing, and common channel signaling.

The Authentication Center (AUC) is a database that contains the International Mobile Subscriber Identity (IMSI), the Subscriber Authentication key and the algorithms that are defined for encryption. To provide system security and usability, multiple modes of biometrics can be used. There are three ways of doing this: sequential, optional and weighted. In sequential mode, the first biometric match must be made before the second is even attempted. For a successful identification, both matches must be matched. Either biometric must match for optional modes. In weighted, each biometric is given a weight. Authentication is based upon a weighted total. Also a combination of biometric and cryptographic authentication process can be applied.

The objective of GSM security is to make the GSM system as secure as the public Switched Telephone Network. Objectives of GSM security are:

– The operators of the GSM system wish that they can issue correct bills to the right people;

– The consumer requires privacy against traffic overhead.

In order to meet these objectives countermeasures are created to establish:

- Anonymity: So that it is not easy to identify the user of the system.
- Authentication. So the operator knows who is using the system for billing purposes.
- Signaling Protection. So that sensitive information on the signaling channel, such as telephone numbers, is protected over the radio path.
- User Data Protection. So that user data passing over the radio path is protected.

(a) Applications

GSM applications include GSM (Global System for Mobile Communication) modems, GSM terminals, GPRS amalgamation, GSM security, GSM remote monitoring. GSM channels are used in alarm security applications.

(b) Features

The Features of GSM are:

- PSTN line detection
- GSM voice channel functional test

- Event memory
- Remote Programming
- Lightning
- GSM network supervision

IV. WIRELESS BIOSENSOR NETWORKS

The tremendous improvement in a variety of technologies, such as micro-processing, sensing material, and most importantly wireless technology has resulted in development of the wireless sensor networks. Such networks are becoming indispensable in a large number of today's applications including real-time data gathering and monitoring for remote environments, medical applications, emergency assistance and alerts devices.

Combination of the low-powered biosensor devices, wireless communication, and network technologies resulted in appearance of the Wireless Biomedical Sensor Networks (WBSNs). A WBSN node consists of an embedded microprocessor, a radio transceiver (transmitter/receiver), a sensing component, a power unit, and a small amount of memory. These sensors, which are either implanted inside the human body or dressed on the surface of the human body, periodically gather medical data and relay it to an outside control node that is responsible for data collection and dissemination. The function of the control node is to analyze the collected data and to send periodical reports to a base station where data is stored for further analysis.

	Traditional Networks	Typical WSN	WBSN
Instance	WLAN	Smart Dust	Smart Ward
Coverage	LAN@50m	PAN@10m	PBAN@1m+PAN
Density	Sparsely	Densely	Densely
Data-centric	Address-centric	Data-centric	Data-centric
Large scale	N	Y	Y
Workloads	Unpredictable	Unpredictable	Partly predictable
Error rates	Medium	High	Must be very low
Energy constraint	No	Yes	For embedded node

Hops	Single	Multi-hop	Optional
Infrastructure	Y	N	N: Self-organizing
Node Failure	N	Y	Prohibited
Deployment	Random	Random	Planned

Table I. Feature Comparison Between Traditional Networks, Typical Wsn, And Wbsn

V. THE FTTP NETWORK

Fiber-to-the-Premises (FTTP) is a fiber-optic technology capable to deliver a very large bandwidth to the home and to the enterprise.

Because a good part of the deliverable bandwidth carries sensitive information, FTTP will attract the attention of eavesdroppers, identity thieves and network attackers.

Biometric data are unique to each person and therefore they constitute the personal key with which authorized access to buildings, accounts, terminals and more is granted. Consequently, network security and biometric data security should be carefully examined.

Currently, several PON architectures have been proposed. The WDM PON is based on multiple optical channels conforming to a coarse wavelength division multiplexing (CWDM) standard grid.

Regardless of which PON architecture is employed, user authentication remains critically important. Figure 3 shows the CWDM PON architecture where biometrics devices are located at the premises (residential or enterprise). Biometric data are transported over the public or private network where they are compared with pre-stored data in a database for ID authentication. It is this data transport that is vulnerable and requires data encryption and authentication protocols.

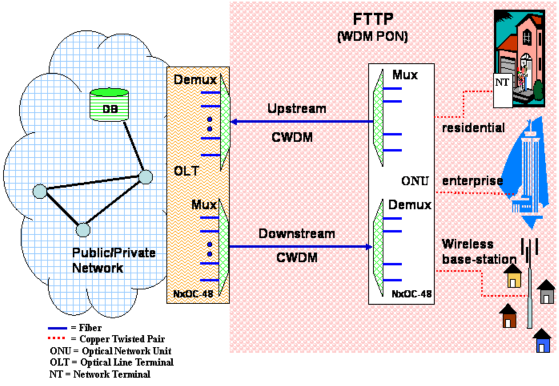

Figure 3. FTTP-PON

However, as shown in Figure 4, the link layer presents an opportunity for the eavesdropper to capture biometric data when they are transported over the network for identification.

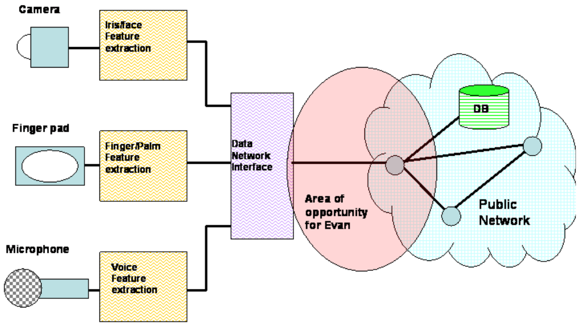

Figure 4. Eavesdropping opportunity for a biometric system over the FTTP network.

VI. APPLICATIONS OF BIOMETRICS IN WIRELESS COMMUNICATION

(a) Wireless biometrics for high end security and providing safer transactions from wireless devices like PDA's, etc.

(b) Biometrics is used in wireless home security camera for extra security on the checkout page and biometric data will protect against unauthorized access to cars and mobile phones.

(c) Biometrics technology and manufacturing of fingerprint security products & systems of Access control, time & attendance clock system and support applicable systems such as fingerprint readers, sensors, fingerprint module. Fingerprint locks are used for wireless communication industry based on the GPRS products development with fingerprint products.

(d) Experts have claimed that the user’s biometric profile is completely safe on handheld wireless devices, especially the Mobile Phones. The need of the hour is a biometrically enabled digital signature application for wireless devices that can guarantee complete security by preserving, storing and processing all sensitive data on a SIM card.

(e) Microlatch’s wireless fingerprint keyfob is one such product, using fingerprint identification for a range of security applications such as access to buildings, machines, specialist applications and as computer logons.

VII. ADVANTAGES OF BIOMETRICS IN WIRELESS COMMUNICATION

(a) High reliability

(b) Efficient and High performance

(c) Easy to use

(d) Easy to collect the data and to compare

(e) Provide a convenient and low-cost additional tier of security.

(f) Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.

VIII. DISADVANTAGES OF BIOMETRICS IN WIRELESS COMMUNICATION

(a) It can be easily manipulated.

(b) Someone can present fake biometrics or a copy at a sensor, for instance a fake finger. It is also possible to try and resubmitting previously stored digitized biometrics signals such as a copy of a fingerprint image.

(c) It extract features, encode and store information in the template based on the system vendor’s proprietary algorithms. Template size might vary, depending upon the vendor.

(d) Single biometrics technology may not always be able to meet wireless communication requirements.

IX. CONCLUSION

Biometrics is the analysis of biological data using mathematical and statistical methods. Wireless communication may be used to transfer information over short distances or long distances. Wireless communications communicate without connecting wires or other material contacts.

The wireless GSM and the optical FTTP the transmission medium of these two networks is different as well as the transported bandwidth and the link length, different encryption procedures, protocols and standards are employed.

Among the most critical data transported over the access network is biometric data. Biometric data are unique to each person and therefore they constitute the personal key with which authorized access to buildings, accounts, terminal and more is granted. The combined biometrics and encryption algorithms assure that unauthorized access will be deterred. In this paper we described the biometric authentication process, we describe the key authentication processes in the GSM and in the FTTP optical access networks.

X. REFERENCES

1. Stamatios V. Kartalopoulos," Communications Security: Biometrics over Communications Networks", IEEE GLOBECOM 2006 proceedings.
2. Mouhcine Guennoun and Marjan Zandi, Khalil El-Khatib," On the Use of Biometrics to Secure Wireless Biosensor Networks".
3. W. Stallings. Cryptography and network security. Prentice Hall. 1998.
4. E. Jovanov et al., "A Wireless Body Area Network of Intelligent MotionSensors for Computer Assisted Physical Rehabilitation," J. NeuroEng. and Rehab., vol. 2, no. 11, Mar. 2005, p. 6.