東海大學電機工程學系

碩士論文

導入身分鑑別機制的無線感測網路於醫療雲之應用

The Application of Wireless Sensor Networks Based on Identity Authentication Protocol in Health Cloud

指導教授：鐘玉芳 博士

劉嘉惠 博士

研 究 生：孫先昱 撰

中華民國 104 年 6 月

東海大學電機工程學系碩士學位

考試委員審定書

電機工程學系研究所 孫先昱 君所提之論文

導入身分鑑別機制的無線感測網路於醫療雲之應用

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：賴永康 （簽章）

委 員：陳玉賢

劉嘉惠

鐘玉汝

蔡坤霖

中 華 民 國 104 年 06 月 12 日

誌謝

有句話是這樣說的:「結束時總會想到開始」。回想起剛進學校時對未來的茫然、親戚朋友質疑的眼光，到現在順利完成論文、考上台電、結婚生子都在這短短兩年完成，連婚紗照都是在東海拍的，一路走來的煎熬令我回想起來不禁百感交集，但我想人生就是不間斷的戰鬥、磨練，只要不放棄目標必定能嚐到甜美的果實，畢竟沒有經過煎跟熬怎麼會得到美味呢?

首先感謝指導教授鐘玉芳博士、陳澤雄博士及劉嘉惠博士三位老師的教導，感謝老師不僅關心學生們的課業，也關心學生們的生活，在我人生陷入低潮時適時給予幫助。謝謝澤雄老師、玉芳老師，不僅在論文、課業上指導我，也放手讓我完成夢想，還送很多小孩的衣服、玩具減輕學生的負擔；謝謝嘉惠老師對岱倫跟我的用心指導，用心改正論文中的錯誤，每次開會都從遙遠的台北趕來真是太辛苦了，能夠有位亦師亦友的指導老師是學生的榮幸；三位老師都是我的貴人，無法以言語表達我心中的感謝，我會謹記於心。

感謝口試委員賴飛羆老師、蔡坤霖和陳志賢老師對論文提出寶貴的建議與批評，讓演算法能夠更加的完善，論文更加豐富。

先昱能夠完成東海大學電機研究所的碩士學位，是由家人與同學們的一路支持與奮鬥才能達到，感謝我的父母，沒有你們就沒有今天的我。感謝一起奮鬥的夥伴岱倫、華健、鳴峯、俊毅、崑峻，我會記得大家在實驗室聊天打屁、一起打球拿到冠軍的日子。

最後特別感謝我的老婆妙蒨，三年來一路陪伴我讓我完成我的夢想，朋友和我弟都說如果是別的女生早就跑了，最驚喜的是還為我生一個可愛的兒子，真是辛苦妳了，謝謝妳參與我過去三年以及接下來的未知人生，我愛妳。

孫先昱 謹誌

民國 104 年 6 月 28 日

摘要

醫療院所或是健康照護機構應用無線感測網路技術進行醫療照護服務，若缺乏一個完善的安全性架構，將無法得到使用者信任，也降低了在醫療照護服務方面的品質。然而，無線感測網路環境下，為了讓被照護者攜帶方便，蒐集與發送生理資訊之設備需為一個微型設備，因此其運算能力與儲存空間極為有限；另外，無線感測網路拓樸架構(wireless sensor network topology)也可能隨著使用者移動而改變；以上種種因素使得傳統網路服務之安全性架構與網路安全通訊協定(network security protocol)不適用於無線醫療照護系統。而利用無線感測器所收集的各項生理資料，攸關被照護者的個人隱私，由於無線感測網路具開放性，因此被照護者傳遞資料的過程中，如何保護使用者資訊安全與隱私、如何防範網路的惡意攻擊、如何提供各裝置間的安全認證，成為醫療照護應用無線感測網路所面臨的重要議題。一個安全的認證機制能確保只有合法的使用者能登入系統，經身分確認後才得以運用系統服務資源。

本論文主要是針對在醫療院所或是健康照護機構應用無線感測網路進行醫療照護監測的環境下，提出具安全與隱私保護使用者認證機制與資料傳輸方式，讓醫護人員能即時掌握被照護者的健康狀況；此認證機制利用智慧卡和通行碼的雙重認證方法，確保只有合法的醫護人員才可以擷取病患的體溫、心跳與血壓等資訊，並採用雙線性配對密碼系統(cryptosystem based on bilinear pairing)提出一個具有安全性的資料傳輸方式，防止不法者的入侵與竊聽。

關鍵字：無線感測網路、身分認證、資訊安全、醫療照護、隱私保護

Abstract

Medical institutions or healthcare facilities apply the use of wireless sensor networks technology for health care services, but if the technology lacks comprehensive security architecture, it would not be able to get the users' trust. In the meantime, it also reduces the quality of medical care services. However, in the wireless sensor network environment, in order to allow the patients ease in carrying the device, the system needs a miniature device for retrieving and transmitting physiological information; therefore, its computing capacity and storage space is extremely limited. In addition, the structure of wireless sensor network topology can be changed with the users' movement. All these factors above make the security architecture and network security protocols of traditional network services and network security protocol unable to be applied to the wireless medical care system. The physiological data that have been collected by the use of wireless sensors are all involved in the patients' personal privacy, because of the openness of the wireless sensor networks; therefore, the process of transmitting the patients' information, the issues of how to protect the security and privacy of users' information, how to prevent malicious networks' attacks, and how to provide secure authentication between devices have become important issues for the use of wireless sensor networks in medical care. A secure authentication mechanism ensures that only legitimate users can log into the system, after the confirmation of users' identification, and access the system's resources. This article is aimed to address the use of wireless sensor networks for medical monitoring in the environment of medical institutions and health care facilities, with security and privacy protection for user authentication mechanisms and data transmission. These allow medical staff to have immediate access to the condition of the patients. This authentication mechanism uses a smart card and a user-password as dual authentication, ensuring that only legitimate medical staff can retrieve patients' information. This scheme can resist common attacks. It also construct a cryptosystem based on bilinear pairing to provide a secure data transmission in order to prevent illegal invasion and eavesdropping.

Keywords: wireless sensor network, authentication scheme, secure data transmission, healthcare system, privacy preservation

Contents

List of Figures

Chapter 1 — Introduction

1.1 Research Motivations

Because of the improvement in health care and medical technology, the ranking of the most common diseases in Taiwan has changed to chronic and degenerative diseases being the most common. A low average income among younger adults, high price levels, increasing stress in daily living, late marriage, decreasing birth rate, and the increasing national average life expectancy have all contributed to the increase in the aging population in Taiwan. The population aging of Taiwan and Japan is the most severe in Asia, and medical expenditure in these countries continues to increase. Emerging aging societies, changes in the living habits of people, and improvement in medical technology have caused mortality from chronic and degenerative diseases, such as diabetes, cardiovascular diseases, and dementia, to gradually outnumber mortality from infectious diseases in the global population. Consequently, demands for medical assistance have increased continually. Furthermore, multigenerational extended families have gradually been outnumbered by nuclear families, in which the family population is decreasing continually. When the younger members of a family leave for work, the older members who require long-term care are forced to live solitarily. Subsequently, the needs for medical care of older people have increased substantially, causing a consequent increase in healthcare demands and rapid development of hospitals.

Recently, wireless networks have rapidly become widespread and commonly applied in various fields. Wireless sensor network (WSN) technology is used to supplement physiological measurement technology and healthcare devices, enabling patients to manage their health autonomously in hospitals and healthcare institutions. In addition, WSNs provide long-term care to patients and collect the physiological parameters of patients, enabling medical personnel to provide patients with appropriate medical care and monitor their physiological conditions according to the acquired information. Moreover, WSNs reduce the time required for adjusting diagnostic prescriptions, helping medical personnel adequately grasp the

physiological conditions of patients. Thus, medical expenditure decrease, and patients receive favorable medical and healthcare services. Therefore, numerous hospitals have adopted healthcare systems based on WSNs, which involve employing physiological sensors, dynamic medical analyses, and data transmission technology. These healthcare systems substitute expensive professional caregivers and enable the health conditions of patients to be monitored at all times.

1.2 Research Purpose

In hospitals and healthcare institutions, applying WSNs for medical monitoring typically involves using remote monitoring technology for diagnoses, monitoring, treatment, and education. Remote monitoring technology facilitates collecting and transmitting daily physiological data between user ends and caregiver ends. Because of the development of WSN technology, wireless sensors enable sensing and detecting targets, collecting relevant valid data, and transmitting data remotely to data centers at the rear end through self-organization networks. Therefore, wireless sensors are suitable for medical monitoring.

Using WSN technology for medical care requires a comprehensive security structure to establish trust among users and maintain high-quality medical services. However, in a WSN environment, to enable patients to conveniently carry the devices used to collect and transmit physiological data, these devices must be microdevices, which limit their computational abilities and storage space. Moreover, the WSN topology might change as users move, rendering the security structure and network security protocols of conventional network services unsuitable for wireless medical care. In addition, collecting physiological data by using WSNs concerns the personal privacy of patients. Because WSNs are open, when patient data are transmitted, protecting the security and privacy of user data, preventing malicious network intrusion, and providing secure authentication to the devices are crucial concerns for WSNs applied for medical care. A secure authentication system enables only legal users to log in. Users must be authenticated to access the system resources.

Regarding the use of WSNs for medical monitoring in hospitals and healthcare institutions, this paper presents an authentication system that facilitates security and privacy protection and enables medical personnel to instantly monitor patient

conditions and provide patients with prompt and comprehensive health care. In addition, when the system transmits physiological data and information, it safeguards the personal privacy of patients. The authentication system stores information to be authenticated in a smart card and performs authentication through a cryptosystem based on bilinear pairing. In addition, a secure data transmission approach is employed to prevent illegal intrusion and eavesdropping.

1.3 Thesis Organization

This thesis can be divided into five parts. The first chapter is about introduction, motivation and purpose. The second chapter contains about relevant research, including Wireless sensor network and the example of application of telemedicine care, then having a detailed description of sensor nodes that are used in the Wireless sensor network environment, the communication protocol as well as bilinear pairing. In chapter three, first there is a clear definition of the operating environment, and how to use the Wireless sensor network in medical environment. Next, there is an introduction of how to effectively verify the identification while the user access for data. Only medical personnel and families which have permission can ask for related medical data. Finally, in the last part of this chapter, an example is proposed to derive. The main content of chapter four is to make safety analysis, and discuss for methods to prevent from being invaded after listing five ways of attack. And the last chapter is the conclusion.

Chapter 2 — Literature Review

2.1 Application and Development of Medical Care

Technological development and communication technology advancement have gradually diversified conventional medical services. Telemedicine is a type of medical approach that enables clinical work to be performed using information and communication technology (ICT). Specifically, medical information of the patient is transmitted to medical personnel remotely by using specific communication technology, and medical personnel then diagnose and treat patients according to the information [1-5]. The evolution of information and communication, physiological measurement, and assistive technologies, and care equipment has facilitated the rapid development of global health care industries and markets. Adopting technology reduces exorbitant medical expenditure and time for making hospital trips. Thus, hospital resources can be reorganized, excessive use of medical resources can be reduced, and medical production and operations can be continually improved, promoting the quality of medical services.

Wireless telecare involves using wireless ICT to perform remote care in hospitals and health care institutions. Remote monitoring technology facilitates collecting and transmitting daily physiological data between user ends and caregiver ends. For example, by employing transmission technology, wireless communication, and physiological sensors for transmitting physiological signals, the physiological statuses of patients can be monitored. Thus, patients can enjoy comfortable daily living and receive comprehensive medical care without hospitalization [33]. In an aging society, enabling self-care and self-management at home or in healthcare institutions is imperative [29-30].

Telecare differs from remote medical treatment in that it does not frequently involve medical practices. Consequently, senders and receivers of health information might be caregivers, patients, family members, nurses, or other medical professionals instead of medical personnel. Therefore, using telecare to satisfy the home health care needs of older people and patients with chronic diseases has become crucial for the

medical care development [6-7]. Accordingly, telecare can be defined as employing ICT to effectively provide and manage health care services for patients in hospitals, in healthcare institutions, and at home [8].

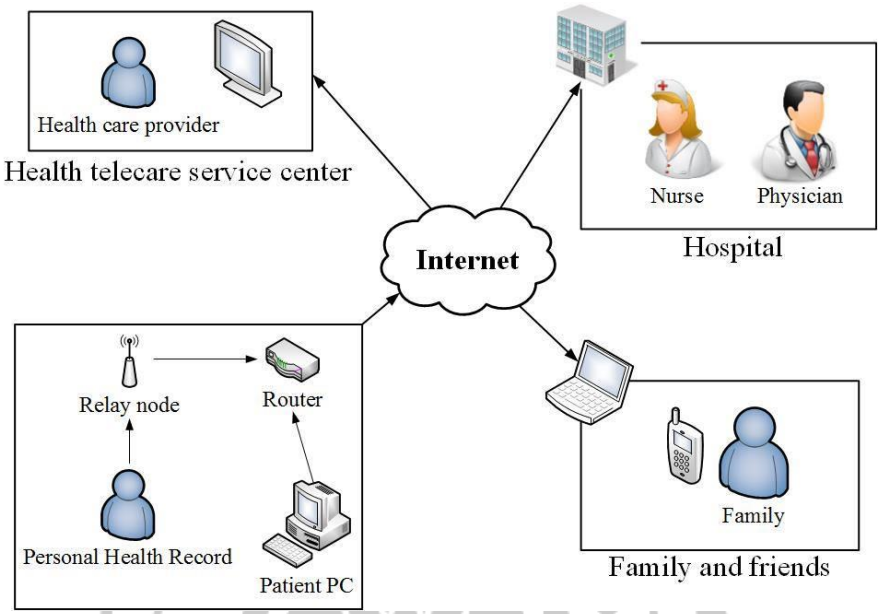

Figure 2.1 : A Telecare System

Figure 2.1 illustrates a telecare system [9]. To provide comprehensive care services remotely, telecare involves using ICT to enable monitoring, transmitting, and analyzing data and emergency service management. Users measure their blood pressure, blood glucose, weight, heart rate, and activities of daily living at home. Alternatively, various wireless sensors and cameras are installed at their homes to record their physiological information [31-32]. The data are then transmitted to data receivers wirelessly. Subsequently, the data are transmitted to external networks through wireless routers and sent to the main servers in specified healthcare centers or hospitals through the Internet [19]. Families or caregivers can examine these data remotely on the Internet, thereby determining the physiological conditions of the patients. If anomalies in the monitored physiological signals are detected or if emergency call signals from patients are received, home telecare systems immediately transmit warning signals to families or caregivers. When diagnosing patients, medical personnel can reference long-term physiological data for highly accurate diagnoses, improving the quality of medical services [37-39].

Typically, telecare systems involve using wireless networks to transmit data, and wireless sensors are employed to collect data. The sensors are equipped with wireless transceivers, forming a WSN. Thus, users of such telecare systems can enjoy comfortable and convenient daily living and move freely without needing to carry wired sensors [34-36]. In addition, using wireless communication networks considerably reduces wiring costs. Currently, numerous studies have sought to improve the transmission effectiveness of WSNs in telecare [40-41]. For example, cluster architectures have been adopted for power-efficient transmission [10], and smart proxies have been applied to improve resource management [11]. Moreover, studies have considered establishing home telecare systems in various locations, such as remote home care service M-Care in Taiwan, the Finnish–Japanese collaborative Finnish Wellbeing Center (FWBC), and MobiHealth in the European Union, which are detailed individually as follows:

1. *M-Care* [12]: Hualien, which is located in the mountainous area of Taiwan, encompasses numerous remote indigenous tribes. Young people typically leave for metropolitan areas for work, resulting in numerous older people to live in Hualien solitarily. Because traffic was inconvenient and medical resources were deficient in Hualien, the M-Care remote home care service was developed to provide older people living in Hualien with medical monitoring at all times. By using this service, medical personnel could monitor and determine the health condition of each patient at all times (Figure 2.2). This service enabled patients to autonomously measure their physiological information such as weight, heart rate, blood pressure, and blood glucose. The information was transmitted to WiMax base stations and then to remote care management platforms through wireless devices. In the areas not encompassed by WiMax service, the long-term physiological data were transmitted to healthcare center platforms through asymmetric digital subscriber lines at home. Medical personnel in clinics and community hospitals could then establish the health condition of each patient through the platforms. Thus, patients could immediately receive appropriate medication and treatment according to the physiological data that medical personnel receive, and medical personnel could promptly remind patients and families to pay attention to their health conditions when abnormalities occurred, thereby achieving preventive care. However, this service structure exhibited the

following problems: using the system was complex and difficult for older people; establishing WiMAX networks was expensive; and most critically, this service structure did not include a security and privacy protection mechanism in transmitting personal information.

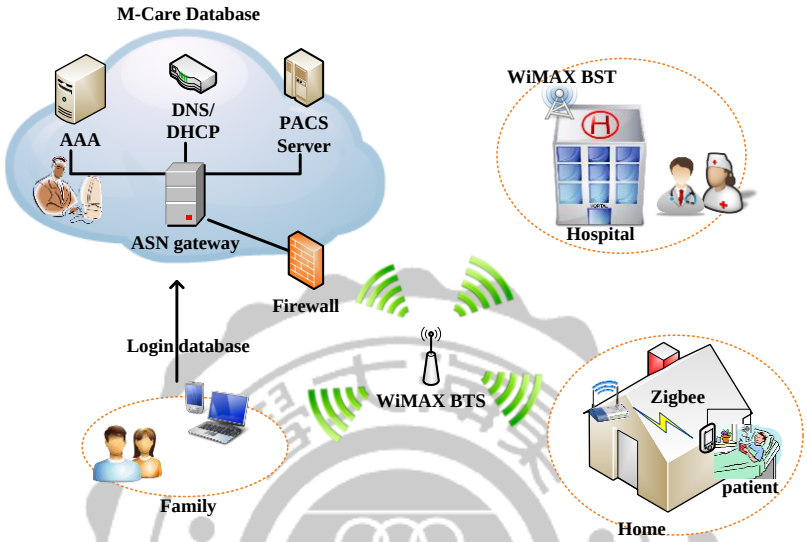

Figure 2.2 : M-Care Remote Home Care Service

2. *Finnish Wellbeing Center*: The Finnish–Japanese collaborative FWBC [13], initiated in 2003 (Figure 2.3), was an attempt to include information technology industries to develop hardware and software suitable for various healthcare services of older people in daily living. Advanced digital products from Japan and ICT from Finland were integrated and applied to establish digital families and their service industries, providing and developing services, products, and equipment with high added value, such as home security, environmental control, and health care, thereby advancing industries. This service structure primarily provided homecare services, daily care services, rehabilitation, assistive technology, and general services. However, no corresponding security systems were developed to protect the security and privacy of the physiological data of users during transmission in this project. Furthermore, patients had to measure their physiological data autonomously and upload them to home care centers. No responsive measures were established for situations in which patients were unable to seek help

autonomously during emergency.

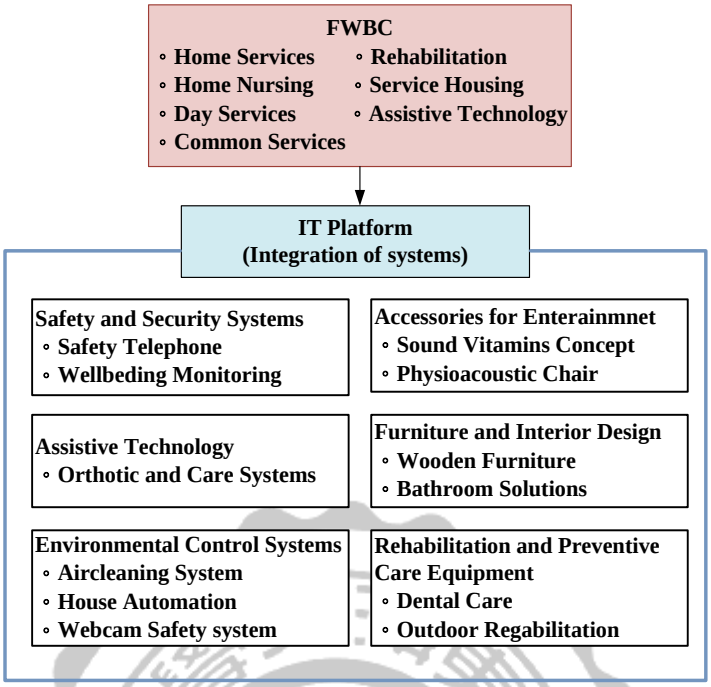

Figure 2.3 : Finnish Wellbeing Center

3. *MobiHealth*: A multinational healthcare project by the United Kingdom, Germany, the Netherlands, Sweden, and Spain [23, 26], MobiHealth is promoted collaboratively by 14 units such as medical services, academic researchers, health care suppliers, mobile communication industries, and communication equipment suppliers. This project involved attaching wireless sensors, which consisted of body area networks and 2.5G / 3G wireless communication technology, to the bodies of users [24-25], enabling physiological data to be automatically transmitted. These sensors could be applied for remote medical diagnoses, disease prevention, home care, and long-term physiological data recording of patients with chronic diseases (Figure 2.4). The objective of this project was to combine wireless mobile value-added services with healthcare services to provide patients with increasingly comprehensive home telecare and health management, subsequently reducing medical costs. Because this project was multinational, the transmission routes for physiological data might have been long. During transmission, stability must be safeguarded. The infrastructure of this project involved the integration of complex heterogeneous systems, resulting in high

difficulty and costs in establishing the project. In addition, a corresponding secure access module was required to ensure the privacy of users.

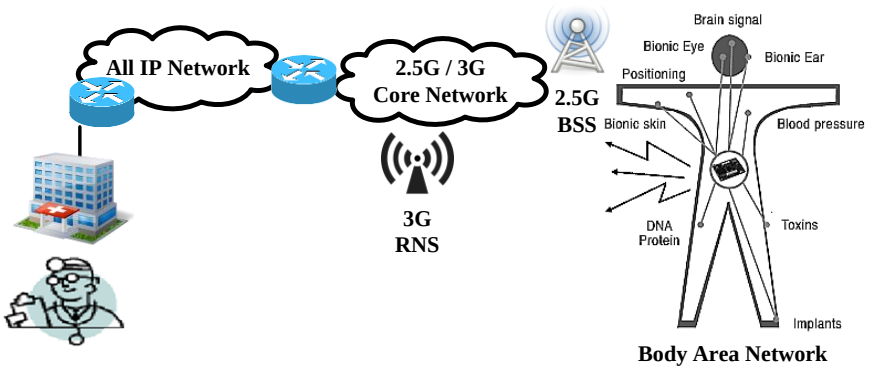

Figure 2.4 : Mobihealth Architecture

2.2 Wireless Sensor Network Technology

1. *Wireless Sensor Networks*: WSNs, which originated from the Smart Dust research project of the University of California, Berkley, are a type of technology that combines sensors, calculation, and wireless networks. Figure 2.5 illustrates the general structure of a WSN [14], in which numerous sensor nodes are distributed in areas for sensing to collect data on the external environment such as temperature, humidity, and lighting levels. The self-organization protocols then connect the nodes to the communication network. Through one-hop or multihop transmission approaches, the data are transmitted to data receivers and forwarded to management personnel or users.

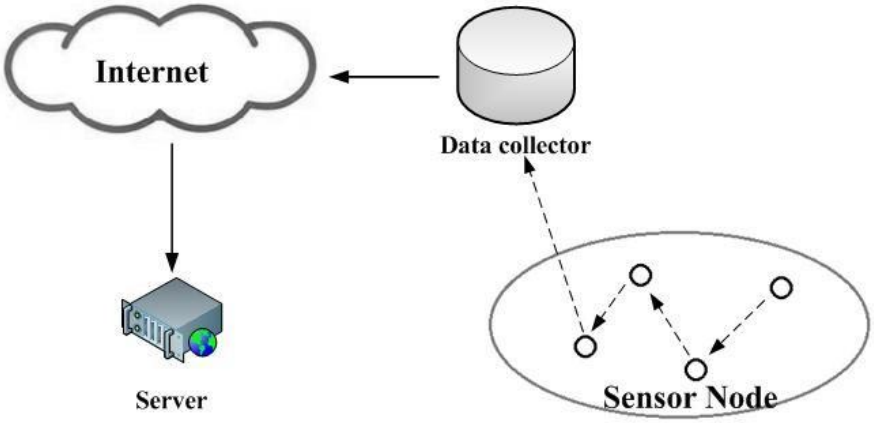

Figure 2.5 : A General Structure of A WSN

WSNs exhibit the following characteristics: low costs, low power consumption, small size, short wireless transmission distances, fault tolerance, and self-configuration [14]. The development of microdevices and imbedding technology enabled accurate sensing, calculation, and communication to be imbedded in microelectronics. This type of wireless sensor nodes facilitates detecting and collecting data on the external environment as well as analyzing and processing the collected data. Generally, the hardware structure of a sensor node consists of four major units: the sensing unit, processing unit, transceiver unit, and power unit.

(1) *Sensing Unit*: This unit consists of a sensor, which collects data on the external environment, and an analog-to-digital converter, which converts the analog signals of data collected by the sensor to digital signals.

(2) *Processing Unit*: This unit consists of a processor, which calculates digital signals according to preset commands, and a storage subunit, which stores collected data.

(3) *Transceiver Unit*: This unit enables data to be received from other sensor nodes and transmits them to wireless data collectors through infrared and wireless fibers.

(4) *Power Unit*: This unit monitors the power supply of each component of the sensor nodes, which is typically provided by batteries.

2. *Wireless Network Security Protocols*: In a wireless sensor network, data are transmitted between sensor nodes through wireless communication. Currently, applied wireless transmission technology includes microchip-based MiWi, Radio Frequency Identification, Bluetooth, Simple Media Access Controllers, ZigBee, and Z-Wave. Each type of protocol exhibits its own advantages and disadvantages and is applied in different fields. The following are comparisons of the current commonly applied wireless transmission technology [15-8]:

   (1) *Radio Frequency Identification*: Enables identifying specific targets and reading their data through radio signals without requiring mechanical contacts between the identification system and the targets. The basic components of Radio Frequency Identification are electronic tags, antennas and readers, and frequency [27-28].

(2) *Bluetooth*: A type of short-distance, low-power consumption wireless transmission technology designed to replace the wired cables among existing personal computers, printers, fax machines, and mobile phones. The primary advantage of Bluetooth is that it can replace the existing wired connection with a wireless interface at all times, enabling interconnection among laptop computers, mobile phones, and personal digital assistants (PDAs) through Bluetooth [15-16]. Bluetooth is a type of open standard for wireless data and voice communication, which was created to solve compatibility problems among electronic devices worldwide. Bluetooth protocols work in the 2.45-GHz Industrial Scientific Medical frequency band that does not require a license, and the data transmission speed of Bluetooth is approximately 2–3 Mbps.

(3) *ZigBee*: A wireless communication standard developed collaboratively by the Institute of Electrical and Electronics Engineers 802.15.4 and ZigBee Alliance [16], ZigBee enables two-way communication, is inexpensive, consumes little power, enables short transmission distances and a low transmission speed, and supports numerous network nodes and various network topologies. Because ZigBee can support numerous network nodes and is easy to expand, it is currently used for remote monitoring, home care, and safety care of older people. However, because ZigBee is a wireless communication technology, it is vulnerable to eavesdropping, intrusion, and even denial of services. Therefore, data transmission security becomes increasingly crucial. Generally, the requirements for data transmission security consist of four levels, according to which protection is performed to increase the security of ZigBee.

   A. *Confidentiality*: Regarding data transmission, Advanced Encryption Standard 128 is applied for encrypting data in ZigBee.
   B. *Verifiability*: Serial numbers are added into transmitted packets in ZigBee to enable data receivers to identify packet loss or tampering.
   C. *Integrity*: To ensure data integrity, data must be protected from malicious tampering, which causes irreversible damage to data. During transmission, verification codes are used to verify the integrity of data in ZigBee.

D. *Nonrepudiation*: Machine coding is used in ZigBee to track data transmission records, preventing users from repudiating having transmitted signals.

2.3 WSN Security

1. *WSN Security Threats*: Because there are no infrastructures in WSNs, causing limitations in resources, multihop approaches must be used for communication. Because network topology is dynamic, WSNs are divided into three layers, namely physical, link, and network layers, each of which exhibits security risks.
   (1) *Physical Layer*: An effective data encryption system is established in this layer for selecting frequencies, detecting signals, and encrypting data. If a malicious network node transmits numerous spam packets, normal communication would be blocked.
   (2) *Link Layer*: This layer provides a reliable channel. A sensor node listens to the communication channel and transmits data through the channel only if no neighboring nodes are transmitting data through the channel. If an attacker transmits data continuously through the channel by using a transmitter, the other nodes would not be able to transmit data through the channel.
   (3) *Network Layer*: This is the riskiest layer, which primarily encounters the following attacks:
      A. *Sybil Attacks*: Involves illegally counterfeiting nonexistent node coordinates through a malicious node to deceive or confuse its neighboring nodes, which misidentify the counterfeit nodes as their neighboring nodes. Thus, the entire network is disrupted and fails to operate normally. These nonexistent nodes are collectively termed Sybil nodes.
      B. *HELLO Flood Attacks*: Numerous protocols require nodes to transmit HELLO signals to their neighboring nodes. Nodes that receive the HELLO signals identify the senders as one-hop neighbors. If an attacker transmits numerous HELLO signals to other sensor nodes according to this characteristic, within the range of the signal of the attacker, nodes that receive the signals would misidentify the attacker as a one-hop neighbor.

C. *Replay Attacks*: If a node records the legal control message of another node and retransmits the message, the other nodes would record their old routes, forming a routing table. During transmission, the message of the nodes may be intercepted by an attacker and counterfeited using false messages before arriving at their target node with neither the sender nor the receiver identifying the attack.

D. *Denial of Service*: An attacker transmits and transfers counterfeit messages to the sensor nodes in an entire network, causing loaded buffers and power wastage in the nodes. Alternatively, in a system with limited power, an attacker infiltrates the power management mechanism of the system, preventing its sensor nodes from switching to a low power mode and causing the power of the nodes to be depleted.

E. *Node Replication Attacks*: An attacker might steal the data of nodes. If successful, the attacker might replicate the nodes and replace them in their original locations for attacking.

2. *WSN Security Mechanisms:* To ensure the data transmission security in WSNs, routing protocols must include corresponding security mechanisms [42], such as identity authentication, mutual authentication, restrictions on topology structures, decentralization, and multiroute transmission, to prevent various attacks. In addition, the wireless transmission characteristic in WSNs causes the personal data of patients to be vulnerable to illegal retrieval during transmission. The secure transmission mechanisms of WSNs include the following:

   (1) *Full pair-wise key*: A unique key exist between each pair of sensor nodes as encryption keys for data transmission. Because connections might occur between any pair of nodes, each node must store the keys of other nodes to guarantee data transmission security. Accordingly, n-1 keys must be distributed and stored in each node, resulting a high total number of keys to be stored. Therefore, although this pair-wise key mechanism can provide sufficient security and flexibility, it requires a large amount of memory space.

   (2) *Single Master Key*: A single master key is shared among all the sensor nodes in an entire WSN. Although this mechanism is easy to implement, if a malicious attacker captures any sensor node, the confidential data of the

entire system would be leaked.

(3) *Random Key Pre-distribution*: Each sensor node selects *k* keys randomly from the key pool *p* as its key ring. If two sensor nodes share the same key, the two sensor nodes share a secure link. Consequently, a large key pool increases the probability of shared keys and connectivity rate. However, it also requires large memory space for storage.

(4) *Group-Based Key*: An entire WSN system is divided into several unique groups. Each sensor node includes an internally shared group key for secured transmission between any pair of nodes within the group. The group-based key mechanism is more effective and scalable and has more storage capacity than the three aforementioned key mechanisms. However, because sensor nodes may switch to different groups, implementing this key mechanism exhibits a certain difficulty.

2.4 User Authentication

The development and increasingly widespread use of wireless networks and mobile communication devices have enabled an increasing number of users to acquire resources and services through networks at all times. Typically, before users can receive services in a network environment, they must be authenticated. Authentication is the first and most critical data protection measure. User authentication involves identifying whether users are legal users of a system, preventing illegal users from intruding the system for critical information [46-48].

Unlike conventional methods, network services do not enable face-to-face authentication. Consequently, identity theft might occur. Therefore, an effective and secure authentication technology is required to strengthen information security. The most commonly used and convenient authentication mechanism in networks is password authentication, which requires users to be authenticated using account names and passwords. When users enter their account numbers and passwords to log into a system, the system verifies whether the data are correct. When the data are verified to be correct, the users are identified as authorized users of the system; otherwise, the users' login requests are denied. Although using passwords for authentication is easy, if the passwords of users are too simple, they risk being compromised. To improve this flaw, smart card and password authentication methods

are typically combined to complement the flaws of each other. Because password authentication is simple, convenient, and highly adaptable, the authentication method is the most widely used [49]. Generally, a user authentication system is divided into three phases [50], as shown in the Figure 2.6, namely the registration phase, login phase, and authentication phase, which are detailed as follows:

1. *Registration Phase*: Before users use a system, they must apply for approval from an administrator. After verification, the administrator provides users with data for authentication, such as smart cards or passwords. Only then are users authorized to access the information in the system.
2. *Login Phase*: When users log into the system, they must present the authentication data provided by the administrator for authentication.
3. *Authentication Phase*: The administrator then verifies whether the users are legal users by examining the user data such as account names, passwords, or smart cards. If the users are legal users, then they would be allowed to access information in the system.

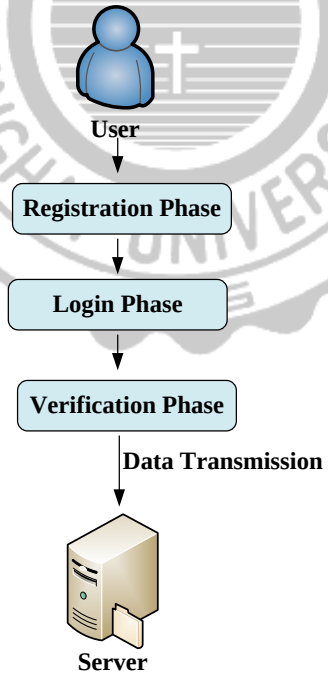

Figure 2.6 : Authentication Process

2.5 Smart Card

Smart cards enable controlling data security and data authentication, are rewritable or deletable, and performs logic algorithms and data processing. They are small and highly portable and can reduce communication costs through offline operations. In addition, the encryption and decryption functions provide smart cards with high security, preventing easy counterfeiting and duplication.

2.6 Basic concepts of bilinear pairing

In 1984, an identity-based cryptosystem has been proposed by Shmair [52]. The conception is to utilize the personal information of a user as the public key of the user. For lack of an efficient cryptosystem, Boneh and Franklin [53] use pairings function to develop an efficient identity-based encryption (IBE) system.

Weil pairing associated with supersingular elliptic curves can be modified to construct such bilinear map. They also contain the same characters of bilinear pairings. First, they let p be a prime such that $q \mid p-1$ for some great prime q and let G_1 and G_2 indicate two cyclic groups of the same prime order q, where G_1 will be an additive cyclic group of points on an elliptic curve E over F_p, and G_2 will be a multiplicative cyclic group of a finite field F^*_{p2}. The bilinear map function is $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ has the following properties:

1. Bilinear: Let $P, Q, R \in G_1$, thus
   (1). $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$
   (2). $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$
   (3). $\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, Q)^{ab}$
   where $a, b \in Z_q^*$.
2. Non-degenerate:
   If P is a generator of group G_1, then $\hat{e}(P, P)$ is a generator of group G_2. There exists $\hat{e}(P, P) \neq 1$.
3. Computable:
   There exist efficient algorithms such that $\hat{e}(P, Q) \in G_2$ can be computed within polynomial time for all $P, Q \in G_1$.

Note that the Weil pairing associated with supersingular elliptic curves can be modified to create such bilinear map. We use the bilinear Diffie-Hellman Problem

(BDHP) for a bilinear pairing [54] in this paper. Let $\hat{e}$:$G_1 \times G_1 \rightarrow G_2$ is defined as follows: Given P, aP, bP, $cP \in G_1$, $W \in G_2$ where a, b, c are random numbers from Z_q^*, it is infeasible to compute the group element $W=\hat{e}(P, P)^{abc} \in G_2$ without knowing a, b or c.

Chapter 3 — Methodology

In recent years, with the rapid development of wireless technology, more and more hospitals and medical institutions to use the wireless sensor networks for medical and health care services. These applications provide physiological monitoring services between the patient and the care provider to collect and transmit data daily. However, it requires secure and reliable user authentication mechanisms to ensure the safety and privacy of wireless medical sensor networks. This paper proposes a reliable authentication mechanism that uses a smart card and a user-password as dual authentication, ensuring that only legitimate medical staff can retrieve patients' information. This scheme can resist common attacks, such as impersonation attacks, replay attacks, on/off-line password guessing attack, and stolen-verifier attack. There are three phases composed of this scheme; they are the registration phase, the login phase, and the verification phase. The main entities include caregiver and the remote trust authority server (TA). Before the hospital's physicians access the patient information, they should register to TA. In the registration phase, all users would be issued their exclusive smart cards and the login passwords. After the TA has verified user's identities, passwords, and the transmitted parameters, they would be allow to login to the remote server through smart cards to acquire the medical information of patients.

3.1 The System Architecture

To establish a medical care system that enables security and privacy protection, this study developed a reliable and secure authentication and data transmission system based on WSN technology. This system is used to provide patients with favorable medical care and enables professional caregivers to determine the health conditions of patients at all times as well as provide them with appropriate health care. In addition, this system safeguards the privacy and security of its users, preventing malicious intrusion and eavesdropping during the transmission of physiological data. The targeted users of home telecare systems in this study were patients in hospitals and healthcare institutions or older people who require medical care. Figure 3.1 illustrates the comprehensive structure of the telecare system, which could be established in a

hospital or healthcare institution.

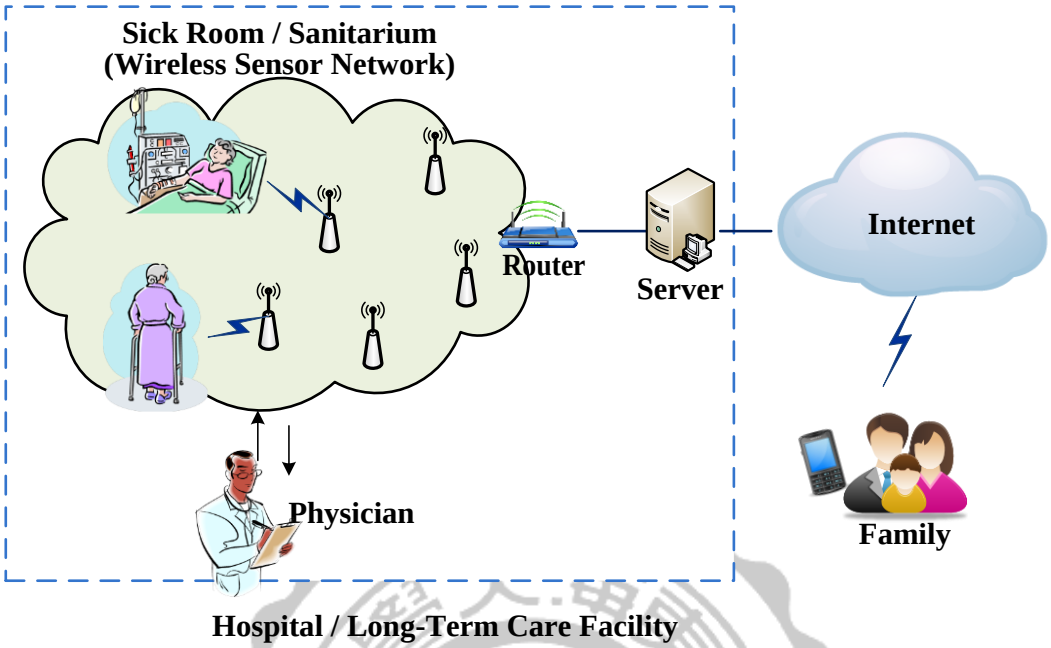

Figure 3.1 : System Architecture

When patients live in hospitals or healthcare institutions, the system stores their physiological data instantly and continually. The data are then transmitted to the servers of care centers, enabling caregivers and families to monitor the physiological conditions of patients remotely. Appropriate monitoring instruments enable physiological monitoring by measuring and capturing the physiological data of patients and transmitting them to the servers of care centers. Figure 3.2 shows the typical processes of physiological monitoring.

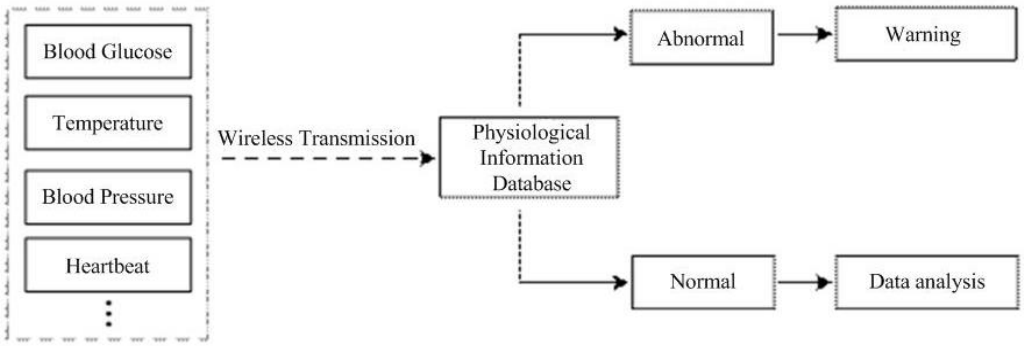

Figure 3.2 : The Processes of Physiological Monitoring.

Patients wear mobile-care devices for this system to capture their physiological data. Base stations transmit requests to the sensors on patients, which then transmit physiological data to the base stations. Data are transmitted to the wireless routers installed in the hospitals or healthcare institutions via wireless sensors. Data are transferred to data transmitters station-to-station through the multihop approach. Subsequently, physiological data are uploaded to the servers in care centers, enabling professional caregivers to examine and analyze the data and assess whether patients need help or a health reminder. Regarding the security threat and privacy problem of data transmission in WSNs, this study developed a reliable authentication system and secures data transmission method for WSNs.

When physicians, nurses, or other medical personnel in hospitals or healthcare institutions wish to inquire information on patients, they must register with the trust authority. After successful registration, the trust authority provides users with secure smart cards. Users can then use the smart cards and mobile devices, such as PDAs or notebooks, to log into the telecare system. After successful authentication, users can inquire and use the data of patients in hospitals or healthcare institutions installed with sensor nodes within a limited time, thereby legally acquiring the physiological data and medical information on patients. As shown in Figure 3.3, physicians can examine the physiological information on patients, such as body temperature, heart rates, blood pressure, and ward information, such as room temperature and lighting levels, by combining smart cards and PDAs.

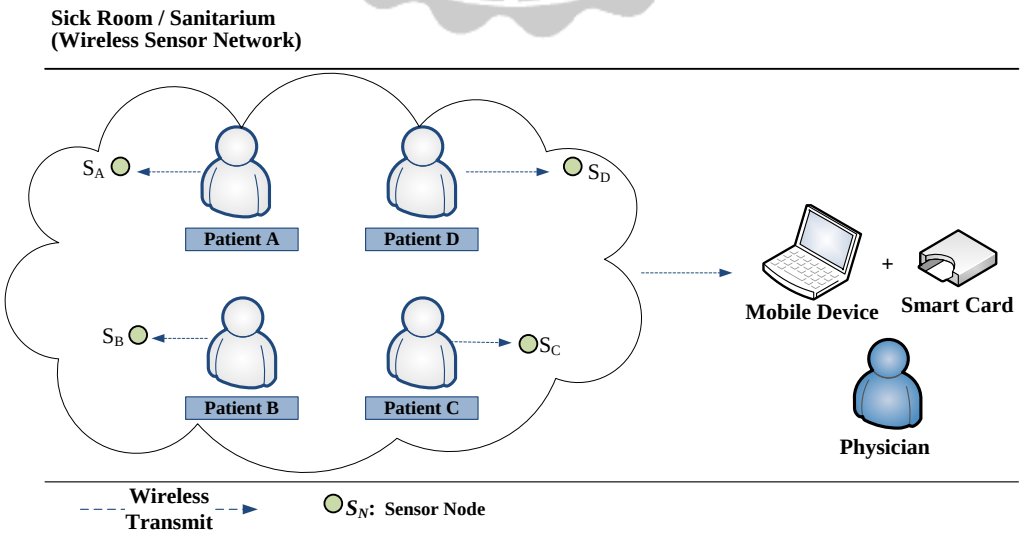

Figure 3.3 : Access Data from Wireless Sensor Node

3.2 Reliable Authentication Method

3.2.1 Initial phase

Step 1: TA selects a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ and $P_0 \in G_1$.

Step 2: TA generates two one way hash functions H_1, H_2.

$$H_1 : \{0,1\}^* \rightarrow G_1$$

$$H_2 : G_2 \rightarrow \{0,1\}^*$$

Step 3: TA seletcs a random number $s_0 \in Z^*_q$, and then computes a public parameter $P_{pub} = s_0 * P_0$

Step 4: TA computes $W = r' * P_0$.

1. *Registration Phase*:

Step 1: User U_i registers an authentication ID_i with the trust authority (TA) and sets password PW_i.

Step 2: The TA calculates $U_{priv} = s_0 * U_{pub}$.

Step 3: The TA personalizes the smart card of the user, and includes the parameters $< h, U_{priv}, ID, PW, a >$, where h represents a one-way hash function, and a represents a private parameter generated by the TA and is stored in the smart card. The user cannot retrieve a directly or indirectly, and all the sensor nodes of the TA include a.

Step 4: The TA sends the smart card to user U securely and privately.

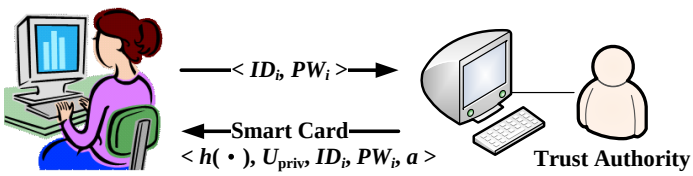

Figure 3.4 : Registration Phase

2. *Login Phase:*

The user inserts the smart card into the device and enters the *ID* and *PW*. The smart card then executes the following steps:

Step 1: Examine whether the *ID* and *PW* entered by the user matches those stored in the smart card. If yes, execute Step 2.

Step 2: Calculate $Sig = r^* U_{priv}$, where $r = h\ (ID \| PW \| a \| T_L)$, where T_L represents the login time.

Step 3: Transmit <*Sig*, *r*, *ID*> to the TA.

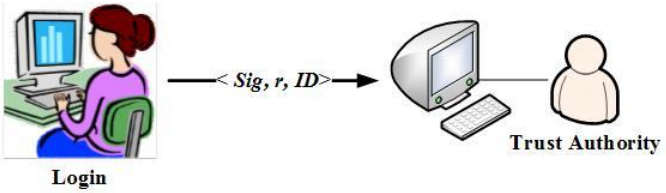

Figure 3.5 : Login Phase

3. *Verification Phase:*

When the TA receives the request and parameters <*Sig*, *r*, *ID*> from the user, the TA authenticates the user through the following steps:

Step 1: If the user *ID* matches that recorded by the TA and $\hat{e}(P_0, Sig) = \hat{e}\ (P_{pub}, r^* U_{pub})$, then the TA approves the request of the user.

Step 2: If $T_{now} - T_L < \Delta T$, where T_{now} represents the current time and ΔT represents the transmission delay, execute Step 3. If the login time exceeds the transmission delay, the login request is denied by the system.

Step 3: Calculate $E=h(b \oplus U_{pub})$, where *b* represents a random number. The TA transmits *E* to the user.

Step 4: The TA transmits $<T_u, b, ID>$ to all the sensor nodes and notifies them that the user is legal. T_u represents the time limit on the legal acess to sensor node data by the user.

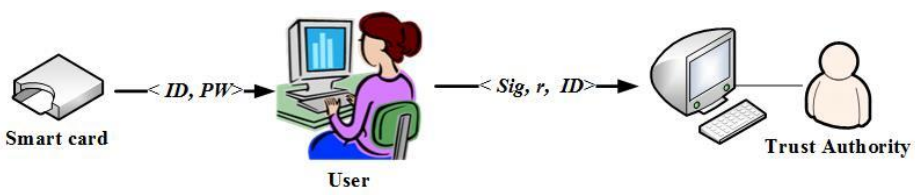

Figure 3.6 : Verification Phase

3.3 Access Control and Encryption Method

After the user is authenticated as legal, the user can access data in the sensor nodes legally within a limited time and transmit data securely through the following steps:

Step 1: Insert the smart card into the device and enter the *ID* and *PW*. The smart card verifies whether the *ID* and *PW* entered matches the data stored in the card. If yes, execute Step 2.

Step 2: The smart card calculates $C= h(a\| ID) \oplus E$ and transmits $<C, ID, T'>$ to sensor node *S*. T' represents a time interval.

Step 3: *S* examines the time. If $(T_{now} – T' < \Delta T)$ and $T_{now} = T_u$, execute Step 4.

Step 4: *S* calculates $C'=h(a\|ID)\oplus h(b\oplus U_{pub})$ by using the *b* transmitted by the TA and public U_{pub} of the user to examine whether $(C = C')$. If yes, then the data are transmitted; if not, the algorithm ends.

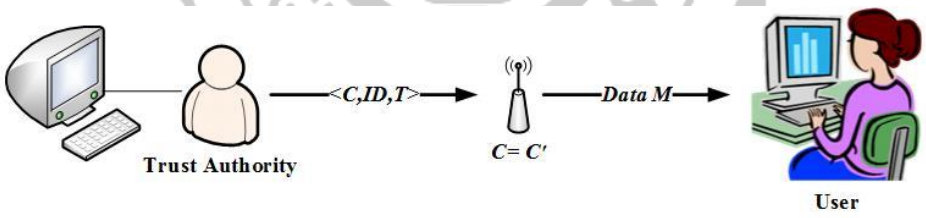

Figure 3.7 : Data Transfer Phase

Step 5: *S* transmits the data *M* required by the user to the user through the following calculation method:

$$M= m\oplus H_2(\hat{e}(U_{pub}, P_{pub}))$$

Step 6: *S* transmits *M* to user *U*.

Step 7: *U* uses the private key U_{priv}, *M*, and the public *W* to perform the following calculation to obtain *m*:

$$M = m \oplus H_2(\hat{e}(U_{priv}, W))$$

3.4 Application Examples

This section describes the application of the method proposed in this paper to an application environment. First, the current structure and application of the system environment is described. Second, the authentication approach proposed in this paper is detailed. In a telecare system, data transmitted by sensor nodes are encrypted, stored on a cloud server, and managed collectively by an administrator. The administrator assigns varying access rights to patients, physicians, nurses, and families. Each user registers to acquire a personal smart card, which is used to log into the system. The user can then extract or use data in areas installed with sensors nodes within a limited time.

1. *Example 1*:

   (1) Assume a caregiver registers with the TA for a legal account ID_1 and sets the password PW_1, and TA calculates $U_{priv1} = s_0 * U_{pub}$ and personalizes the smart card for the user.

   (2) The user inserts the smart card into a device, such as a laptop or PDA, and enters ID_1 and PW_1, using the key to calculate $Sig = r * U_{priv1}$, where r = h ($ID \| PW \| a \| T_L$). A message < Sig, r, ID_1> is returned to the TA. T_L represents the login time.

   (3) When the request and <Sig, r, ID_1> from the user are received, the TA authenticates the user by using $\hat{e}(P_0, Sig) = \hat{e}(P_{pub}, r * U_{pub})$. $E = h(b \oplus U_{pub})$ is calculated and transmitted to the user, with b representing a random number. Thus, the authentication of the user is complete, and the user can now access and transmit data.

2. *Example 2*:

   (1) The smart card calculates $C = h(a \| ID) \oplus E$ and transmits <C, ID, T'>, where T' represents a time interval, to sensor node S. The sensor node then uses the

b transmitted by the TA and the public U_{pub} by the user to calculate $C' = h(a \| ID) \oplus h(b \oplus U_{pub})$ and verify whether ($C = C'$). Subsequently, the system begins transmitting data to the user.

$E = h(b \oplus U_{pub})$

$C = h(a \| ID) \oplus E$

$= h(a \| ID) \oplus h(b \oplus U_{pub})$

$= C'$

(2) S transmits the requested data M to the user through the following calculation:

$M = m \oplus H_2(\hat{e}(U_{pub}, P_{pub}))$

The user uses the private key U_{priv1}, M, and the public W to perform the following calculation to obtain m:

$M = m \oplus H_2(\hat{e}(U_{pub}, P_{pub})^{r'}) \oplus H_2(\hat{e}(U_{priv1}, W))$

$= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})^{r'}) \oplus H_2(\hat{e}(s_0 * U_{pub}, r' * P_0))$

$= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})^{r'}) \oplus H_2(\hat{e}(U_{pub}, r' * P_0)^{s_0})$

$= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})^{r'}) \oplus H_2(\hat{e}(U_{pub}, s_0 * P_0)^{r'})$

$= m \oplus H_2(\hat{e}(U_{pub}, P_{pub})^{r'}) \oplus H_2(\hat{e}(U_{pub}, P_{pub})^{r'})$

$= m \oplus 0$

$= m$

Chapter 4 — Security Analysis

4.1 Password Protection

Guaranteeing users of all levels in the telecare system proposed in this paper, namely physicians, nurses, caregivers, and patients, that using passwords to log into the system is reliable and secure from malicious hacking is imperative. The ability of the system to prevent password leaks must be confirmed.

1. Stolen-Verifier Attacks:

   This type of attacks involves stealing confidential information of users, such as ID numbers and passwords, from verification tables in servers. If servers are not required to store verification tables, then this type of attacks is avoided.

2. Online Password Guessing Attacks:

   This type of attacks involves linking to a target computer directly and acquiring legal access to an account through password guessing and trail and error.

   During the login phase, the signature *Sig* and private parameter U_{priv} are calculated. An attacker must crack the U_{priv} to obtain the password. However, this parameter is used in the bilinear map $\hat{e}$, which is based on eliptic curve cryptography. Thus, the attacker must solve the bilinear Diffie-Hellman problem (BDHP) to crack the parameter, which is extremely difficult to achieve. In addition, the attacker must crack the password within a limited time before being denied access. Therefore, online password guessing attacks are inapplicable.

3. Offline Password Guessing Attacks:

   This type of attacks involves obtaining the password of a target user by intercepting data or through other security flaws. A specific program is employed to guess the password continuously until the correct password is obtained or the cracking attempt fails.

   In the proposed system, even if an attacker intercepts *Sig*, because of the difficulty of the BDHP, the attacker would be unable to crack U_{priv}. Moreover, the attacker must solve the one-way hash function and guess the secret parameter a to obtain the password. Therefore, this system is safe from offline password guessing attacks.

4.2 Data Transmission Security

When a user, such as a caregiver, physician, nurse, or family member, is successfully authenticated by the TA of the telecare system, the user can legally transmit data to sensor nodes. Safeguarding confidential data from identification, tampering, and deletion during transmission is critical.

During the data acquisition phase in this study, the T' from the session key $<C, ID, T'>$ was used to ensure that data transmission was executed only within a legal time. C and ID were used by sensor nodes to transmit data to the user after authentication. During transmission, bilinear mapping was used to encrypt data. Because bilinear pairing renders cracking data difficult, thus the data can be transmitted securely.

4.3 Legal User Impersonation Attacks

Impersonating a legal user is a typical method used to attack a system. After intercepting the request message $<Sig, r, ID>$, an attacker may use the message to request to log into the system. However, in the proposed system, the time interval of the user is verified, rendering this set of message invalid and preventing the attacker from logging in. In addition, the attacker cannot impersonate a legal user because of the lack of the password and a of the legal user. Cracking the password from a login signal or obtaining the a from a smart card is difficult, and the registration data of a legal user from U_{priv} cannot be counterfeited. The attacker must solve the BDHP to crack U_{priv} or steal the smart card of the user to obtain $U_{priv.}$ Therefore, impersonation attacks are inapplicable against the system proposed in this paper.

4.4 Replay Attacks

Intercepting a message for replay attacks on the proposed system is impossible. After receiving a login request, the system verifies whether the time interval is within the legal delay; if not, the system denies the request. An intercepted and replayed login request cannot pass the time interval verification, rendering replay attack inapplicable.

Chapter 5 — Conclusion

Using WSN technology to establish wireless healthcare systems requires a comprehensive security mechanism to safeguard the privacy of users and obtain their trust, improving the quality of health care. However, the security mechanisms and network security protocols of conventional network services are inadequate for use in telecare systems. The physiological data collected using wireless sensors concerns the personal privacy of care receivers. Because WSNs are open, during patient data transmission, protecting the security and privacy of user data, preventing malicious attacks on networks, and providing secure authentication to devices are critical for applying WSNs to healthcare systems. A secure authentication system ensures that only legal users can log into the system and access the system resources after their identities are authenticated. Therefore, on the basis of using WSN technology to establish healthcare systems that enable protecting security and privacy, this paper proposes a reliable user authentication system and secure data transmission mechanism. When patients live in hospitals or long-term care institutions, the system can access and store their physiological data instantly and continuously. The obtained physiological data are then transmitted to the servers of care centers through the Internet, enabling caregivers and families to determine the physiological conditions of care receivers remotely. Appropriate monitoring instruments can be adopted to measure and extract the physiological data of care receivers and transmit them to the servers of care centers.

The proposed user authentication system enables medical personnel to instantly determine the health conditions of patients. In addition, the system protects the privacy of its users. Smart cards are used to store authentication data, and the cryptosystem based on bilinear pairing was designed for authentication. Furthermore, a secure data transmission approach is proposed to enable caregivers to obtain data, safeguarding the privacy and security of both caregivers and care receivers simultaneously. Passwords used to log into the telecare system are guaranteed to be secure, reliable, and free from the threat of malicious hacking, and attacks on security are prevented. The security analysis verified that the proposed system can resist common attacks such as impersonation attacks, replay attacks, online and offline password guessing attacks, and stolen-verifier attacks.

References

[1] G. Eysenbach, “What is e-health?,” *Journal of Medical Internet Research*, Vol. 3, No. 2, e20, 2001.

[2] American Telemedicine Association, ATA, http://www.atmeda.org/

[3] P. Burn, “Telehealth or telehype? Some observations and thoughts on the current status and future of telehealth,” *Journal of Healthcare Information Management*, Vol. 13, No. 14, pp. 1-10, 2001.

[4] H. J. Cheong, N. Y. Shin, and Y. B. Joeng, “ Improving korean service delivery system in health care: Focusing on national e-health system,” *IEEE Conference on Ehealth, Telemedicine, and Social Medicine*, pp. 263-268, 2009.

[5] Z. Y. Wu et al., “A secure authentication scheme for telecare medicine information systems,” *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1529-1535, 2012.

[6] B.G. Celle, N. H. Lovell, and J. Basilakis, “The business case for home telecare: a comparative analysis between the USA, Europe and Australasia,” *IEEE International Conference on Engineering in Medicine and Biology Society*, pp. 6151, 2007.

[7] Google health. http://www.google.com/

[8] Office of Health and Information Highway, “International activities in tele-homecare”, Health Canada, 1998.

[9] X.H. Peng, G.C. Zhang and X.Y. Gu, "Cooperative data dissemination for telecare systems via wireless pervasive networking," *IEEE International Workshop on Ubiquitous Healthcare and Supporting Technologies*, Finland, 2010.

[10] M. H. Jin et al, “Sensor network design and implementation for health telecare and diagnosis assistance applications,” *The 11th IEEE International Conference on Parallel and Distributed Systems*, Fukuoka, 2005.

[11] M. A. Valero et al., “An intelligent agents reasoning platform to support smart home telecare,” *Lecture Notes in Computer Science*, Vol. 5518, pp. 679-686, 2009.

[12] T. Paul Y. Tseng, and H. H. Chen,“Creating a new wireless business model of healthcare: The WiMAX project in Hualien, Taiwan,” *IEEE Mobile WiMAX Symposium*, ISBN 1-4244-0957-8, pp. 138-143, 2007.

[13] Finnish Wellbeing Centerhttp://www.fwbc.fi/

[14] I. F. Akyildiz et al., "A survey on sensor networks," *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, 2002.

[15] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," *IEEE Wireless Communication*, Vol. 12, No. 1, pp. 12-16, 2005.

[16] N. Baker, "ZigBee and Bluetooth: Strengths and weaknesses for industrial applications," *IEEE Computing and Control Engineering*, Vol. 16, No. 2, pp 20-25, May 2005.

[17] P. S. Nee. and H. Dighe, "Robust factory wireless communications: a performance appraisal of the Bluetooth and the ZigBee collocated on an industrial floor," *IEEE International Conference on Electron*, pp. 2381-2386, 2003.

[18] R. Beckwith "Report from the field: results from an agricultural wireless sensor network," *IEEE International Conference on Local Computer Networks*, pp. 471-478, 2004.

[19] T. Gao, C. Pesto, et al., "Wireless medical sensor networks in emergency response: implementation and pilot results," *IEEE International Conference Technologies for Homeland Security*, Waltham, USA, 2008.

[20] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644-654, 1976.

[21] J. Wiley, "An application-driven approach to designing secure wireless sensor networks," *Wireless Communications and Mobile Computing*, Vol. 8, No. 3, pp. 369-384, 2008.

[22] K. Malasri and L. Wang, "Design and implementation of a secure wireless mote-based medical sensor network," *Proceedings of the 10th International Conference on Ubiquitous Computing*, pp. 172-181, 2008.

[23] R. Bults, et al., "Mobile patient monitoring: The MobiHealth system," *IEEE Engineering in Medicine and Biology Society*, pp. 1238-1241, 2009.

[24] E. Jovanov, "Wireless technology and system integration in body area networks for m-health applications," *IEEE Engineering in Medicine and Biology Society*, pp. 7158-7160, 2005.

[25] T. Norgall, et al., "Body area network BAN- a key infrastructure element

for patient-centered medical applications." *Biomedizinische Technik. Biomedical Engineering*, Vol.47, pp.365, 2002.

[26] F. Miao, X. Miao, W. Shangguan, and Y. Li, "MobiHealthcare system: body sensor network based m-health system for healthcare application," *E-Health Telecommunication Systems and Networks*, Vol. 1, No. 1, pp. 12-18, 2012.

[27] J. Ayoade, "Security implications in RFID and authentication processing framework," *Computers and Security*, Vol. 25, pp.207-212, 2006.

[28] R. Tesoriero, J . Gallud et al. "Using active and passive RFID technology to support indoor location-aware systems," *IEEE Transaction on Consumer Electronics*, Vol. 2, pp. 578-583, 2008.

[29] T. Falas, G. Papadopoulos, and A. Stafylopatis, "A review of decision support systems in telecare", *Journal of Medical Systems*, Vol. 27, No. 4, pp. 347-356, 2003.

[30] A. Illarramendi et al., "Aingeru: an innovating system for tele-assistance of elderly people," *Telecare*, pp. 27-36, 2004.

[31] B. S. Lee, T. P. Martin et al., "Dynamic daily-living patterns and association analyses in tele-care systems," *4th IEEE International Conference on Data Mining*, pp. 447-450, 2004.

[32] L. Lamothe, J. P. Fortin et al., "Impacts of telehomecare on patients, providers, and organizations," *Telemedicine Journal of e Health*, Vol. 12, pp. 363-369, 2006.

[33] M. Chan, E. Campo, and D. Esteve, "Assessment of activity of elderly people using a home monitoring system," *International Journal of Rehabilitation Research*, Vol. 28, pp. 69-76, 2005.

[34] E. Jovanov, D. Raskovic et al., "Synchronized physiological monitoring using a distributed wireless intelligent sensor system," *IEEE Engineering in Medicine and Biology Society*, Vol. 2, pp.1368-1371, 2003.

[35] C. Baber, A. Schwirtz et al., "Sensvest-on-body physiological monitoring system," *IEEE Eurowearable*, pp. 93-98, 2003.

[36] S. P. Nelwan, T. B. Dam et al., "Ubiquitous mobiles access to real-time patient monitoring data," *Computing Cardiology*, pp.557-560, 2002.

[37] A. Rogers, S. Kirk et al., "Established users and the making of telecare work in long term condition management: implications for health policy," *Social Science and*

Medicine, Vol. 2, No. 7, pp. 1077-1084, 2011.

[38] O. Onyimadu and J. Briggs, "Designing a telecare product for the elderly," 5th *International Conference on Pervasive Computing technologies for healthcare*, pp. 336-339, 2011.

[39] D. Berian and V. Topac, "A hybrid solution for a telecare system server," *6th IEEE International Symposium on Applied Computational Intelligence and Informatics*, pp. 589- 592, 2011.

[40] Y. Y. Chen, W. T. Huang et al., "Development of a novel bidirectional control telecare system over a wireless sensor network and the Internet," *Asia-Pacific Services Computing Conference*, pp. 907-913, 2008.

[41] M. ElHelw, J. Pansiot et al., "An integrated multi-sensing framework for pervasive healthcare monitoring," *Proceedings of Pervasive Computing Technologies for Healthcare*, pp. 1-7, 2009.

[42] B. Kannhavong, H. Nakayama et al., "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, Vol.14, No.5, pp. 85-91, 2007.

[43] M. S. Nikjoo, A. S. Tehrani, and P. Kumarawadu, "Secure Routing in Sensor Networks," *Proceedings of Canadian Conference on Electrical and Computer Engineering*, pp. 978-981, Canada, 2007.

[44] M. Wen, H. Li et al., "TDOA-based Sybil Attack Detection Scheme for Wireless Sensor Networks," *Journal of Shanghai University*, Vol. 12, No. 1, pp. 66-70, 2008.

[45] M. Conti, R. D. Pietro et al., "Requirements and open issues in distributed detection of node identity replicas in WSN," *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, Vol. 2, pp. 1468-1473, Taiwan, 2006.

[46] M.S. Hwang, CC Lee and YL Tang, "A simple remote user authentication scheme," *Mathematical and Computer Modeling*, Vol. 36, No. 1, pp.103-107, 2002.

[47] W.H Yang and SP Shieh, "Password authentication schemes with smart cards." *Computers & Security*, Vol. 18, No. 8, pp.727-733, 1999.

[48] I.C Lin, M.S Hwang and L.H Li, "A new remote user authentication scheme for multi-server architecture." *Future Generation Computer System* Vol.19, No.1, pp.13-22, 2003.

[49] C. C. Chang and T. C. Wu, "Remote Password Authentication with Smart Cards,"

IEEE Computers and Digital Techniques, Vol. 138, No. 3, pp. 165-168, 1991.

[50] M. S. Hwang, "A Remote Login Authentication Scheme Based on the Digital Signature Method," *International Journal of Computer Mathematics*, Vol. 70, No. 4, pp. 657-666, 1999.

[51] A. Catherine and William J Barr. (1997). Smart Cards: Seizing the Strategic Business Opportunities. McGraw-Hill.

[52] A. Shamir. "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology-Proceedings of CRYPTO'84*, pp. 47–53, 1984.

[53] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing," *Advances in Cryptology-Proceedings of Crypto*, Springer-Verlag LNCS 2139, pp. 213–229, 2001.

[54] A. Joux, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems," *in Proceedings Fifth Algorithmic Number Theory Symposium, Springer-Verlag. LNCS*, 2002.