Secure Data Aggregation and Access Control in Cloud Assisted eHealth Care System

by

Mrinmoy Barua

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2014

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Recently electronic health (eHealth) care system has drawn a lot of attention from the research community and the industry to face the challenge of rapidly growing elderly population and ever rising health care spending. The health care sector is also driven by the need to reduce costs while simultaneously increasing the service of quality for patients, especially extending health care to patient's residence. Advances in wireless body area networks (WBANs) have made it possible to monitor patient's physiological signals (such as electrocardiogram (ECG), blood oxygen levels) and other health related information (such as physical activity levels) in a residential setting or a mobile setting. Integrating this technology with existing 3G or 4G wireless technologies permits real-time mobile and permanent monitoring of patients, even during their daily normal activities. In such a heterogeneous wireless environment, we can use Ad-hoc network instead of traditional infrastructure-based wireless networks that can reduces cost of deployment, enhances network performance, increases the overall network coverage area as well as reduces the service cost. However, secure communication with data integrity and confidentiality in this type of network is a very challenging task due to different wireless technologies and subscription from various service providers. In addition, instead of storing the PHI at local health-service provider, the recent advancement of cloud computing allows us to store all personal health information (PHI) at cloud-storage and ensures availability with reduce the capital and operational expenditures. However, they also bear new risks and raise challenges with respect to security and privacy aspects. Stored data confidentiality with patient-centric access control is considered as one of the biggest challenges raised by cloud-storage used in eHealth care system.

To address these challenges, in this thesis, we first identify unique features of the eHealth care system with security and privacy consideration. We then propose a light weight secure data forwarding scheme for the WBNs environment. A hybrid approach, integrated with public and private key cryptography was adopted to ensure the effectiveness of the scheme. Due to critical and real-time nature of the health application, WBANs also need to provide acceptable Quality of Service(QoS) in order to provide an efficient, valuable and fully reliable assistance to patients. Taking QoS as an evaluation metric, we study packet scheduling schemes for realtime transmission in WBAN and classified real-time and non real-time traffic to minimize the waiting time of eHealth application's data traffic.

Secondly, we propose an Agent-based Secure and Trustworthy packet-forwarding Protocol (ASTP) for a cooperative mobile social network. In a cooperative mobile social network environment patient equipped with WBANs forms an on-demand adhoc network and use multi-hop routing to enhance network performance, minimize the cost of deployment,

increase the coverage area as well as reduce the overall service cost. We use Semi-agent-symmetric trust metric, considering neighbor nodes' previous and recent activities and incorporate with proper security tools that enhanced the overall performance. Renewable pseudo-identities are used to ensure patients' identity privacy. Security analysis and experimental results demonstrate that ASTP improves the average packet delivery ratio and maintains the require security and privacy at the cost of an acceptable communication delay.

Considering patients living in rural area, thirdly we introduce a delay-tolerant secure long-term health care scheme, RuralCare, for collecting patients sensitive PHI by using conventional transportation vehicles (e.g., cars, buses) as relay nodes. These vehicles are expected to store, carry, and forward the PHI to the health-service-provider located mostly at the city area following an opportunistic routing. RuralCare improves network performance by providing incentive to the cooperative vehicles, and encompasses identity based cryptography to ensure security and privacy of the PHI during the routing period by using short digital signature and pseudo-identity. Network fairness and resistance to different possible attacks are also ensured by RCare. Extensive security and performance analyses demonstrate that RuralCare is able to achieve desired security requirements with effectiveness in terms of high delivery ratio.

Finally, to store patients sensitive PHI at the cloud storage and ensure availability with reducing the capital and operational expenditures, we propose a patient-centric personal health information sharing and access control scheme (ESPAC). ESPAC relieves the health service providers (HSP) additional burden for PHI storage, management, and maintenance by incorporating cloud storage services to electronic Health (eHealth) care system. ESPAC adopts attribute based encryption and assigns different attributes to PHI access requesters based on their roles and relation to the patient. To ensure authenticated PHI access with minimum computation, we further enhance the proposed scheme ESPAC as M-ESPAC by introducing multi-parties proxy re-encryption protocol. Light weight partial and block PHI audits make the M-ESPAC efficient to ensure stored PHI integrity and availability. Extensive performance and security analyses demonstrate that proposed schemes are able to achieve desired security requirements with acceptable computation and storage costs.

The research results of the thesis should be useful for the implementation of secure and privacy-preserving eHealth care system with patient centric access control of stored PHIs.

Acknowledgements

I would like to thank all the people who made this possible. This thesis would not have been possible without the help and support of my supervisor, my thesis committee members, and my colleagues in the Broadband Communications Research (BBCR) group. During my PhD research I learned many new things, and without the people surrounding me I could not enjoy from this period of my life.

First of all, I gratefully acknowledge my supervisor, Professor Xuemin (Sherman) Shen. He made available his support and aid in a number of ways. He always does care about his students, and I had this opportunity to discuss the obstacles encountered me in my study and research openly with him. He not only helps me to develop the academic skills, but also guides me to strive for excellence. I would also like to thank Prof. Xianbin Wang for serving as my thesis external examiner and sharing his invaluable insight on information and communication security with me. I would also like to extend my appreciation to the other members of my examining committee, Professor Sagar Naik, Professor Zhou Wang, and Professor Xinzhi Liu, for the time and efforts to read my thesis. In spite of their busy schedules, all have been readily available for advice, reading and encouragement.

At BBCR group, I would like to thank Professor Xiaodong Lin. I would also thank Dr. Rongxing Lu, Dr. Xiaohui Liang, Dr. Shamsul Alam, Mr. Kuan Zhang, Mr. Amila Gamage, Mr. Ning Lu, Mr. Qinghua Shen, and Mr. Ning Zhang. We worked collaboratively at the BBCR group, and we had many discussions to brainstorm and collaborate on interested research topics.

There are many other people whose names are not mentioned here. It does not mean that I have forgotten them or their help. It is a privilege for me to work and share life with so many bright and energetic people. Their talent and friendship have made Waterloo such a great place to live for me.

In addition, grateful acknowledgements are made for the financial support of the Natural Sciences and Engineering Research Council of Canada (NSERC), Ontario Research and Development Challenge Fund Bell Scholarship, and numerous awards from the University of Waterloo.

Finally, I am very much thankful and grateful to my family, i.e., my late father, my mother, my wife and my brother. I would never get this far without their support. I thank them for always believing in me and supporting me. Their love and encouragement have been and will always be a great source of inspiration in my life. I would continuingly work hard to fulfil my career goals and never disappoint them.

Dedication

To my beloved son and daughter.

Table of Contents

List of Tables xii

List of Figures xiii

List of Abbreviations xv

1 Introduction 1

1.1 eHealth Care System and Challenges 1

1.1.1 eHealth Characteristics 4

1.1.2 Application of eHealth 4

1.2 Security and Privacy Threats 7

1.3 Security and Privacy Requirements 8

1.4 Research Motivations and Contributions 9

1.5 Outline of the Thesis 12

2 Technical Background 13

2.1 Pseudonym Technique for Identity Privacy 13

2.2 Cryptographic Techniques 14

2.2.1 Bilinear Groups of Prime Order 14

3 Energy Efficient and Secure Data Aggregation in WBAN **16**
3.1 Introduction . . . 16
3.2 WBAN Architecture . . . 18
3.3 Security and Privacy Requirement at WBAN . . . 19
3.3.1 Security and Privacy in Communication Initialization . . . 19
3.3.2 Network Communication Data Security . . . 19
3.4 Related Works . . . 20
3.5 System Model and Data Processes Steps in WBAN . . . 21
3.5.1 Security Model . . . 22
3.6 Proposed Approach for Secure Data Aggregation in WBAN . . . 22
3.6.1 Security initialization . . . 22
3.6.2 System Initialization by the User . . . 23
3.6.3 Source Authentication . . . 23
3.6.4 Message Encryption and Decryption: . . . 24
3.6.5 Signature and Verification . . . 26
3.7 Performance Analysis . . . 26
3.8 Security Analysis . . . 28
3.8.1 Resilience to Packet Analysis Attack . . . 28
3.8.2 Resilience to Source Authentication Attack . . . 29
3.8.3 Resilience to Data Authentication Attacks . . . 29
3.9 Proposed scheduling scheme . . . 30
3.9.1 High-priority queue . . . 31
3.9.2 Low-Priority queue . . . 32
3.10 Performance Evaluation of Scheduling Approach . . . 33
3.11 Summary . . . 33

4 ASTP: Cooperative Trust Aware Data Aggregation in Urban Area 36
4.1 Introduction . . . 36
4.2 Related Work . . . 37
4.3 Security Requirement and System Model . . . 38
4.3.1 Security Requirements . . . 38
4.3.2 System Model . . . 39
4.4 The Proposed ASTP Protocol . . . 39
4.4.1 System initialization . . . 39
4.4.2 Routing Establishment Phase: . . . 41
4.5 Performance Evaluation . . . 45
4.6 Security Analysis . . . 48
4.7 Summary . . . 49

5 RuralCare: Incentive Based Secure Data Aggregation in Rural Area 50
5.1 Introduction . . . 50
5.2 Related Works . . . 52
5.3 Models and Design Goals . . . 53
5.3.1 System Model . . . 53
5.3.2 Design Goals . . . 55
5.4 The Proposed RuralCare Scheme . . . 57
5.4.1 Notations and complexity assumptions: . . . 57
5.4.2 The RuralCare Scheme . . . 58
5.4.3 Signature Correctness . . . 62
5.4.4 Incentive and Reputation Granting: . . . 62
5.5 Security Analysis . . . 62
5.6 Performance Evaluation . . . 64
5.6.1 Probabilistic Model . . . 65
5.6.2 Cryptographic Overhead . . . 66
5.6.3 Simulation . . . 66
5.7 Summary . . . 71

6 Enabling Patient-centric Access Control of Aggregated Data in Cloud Computing **72**
6.1 Introduction . . . 72
6.2 Related Works . . . 74
6.3 System Model and Security Requirements . . . 75
6.3.1 System Model . . . 75
6.3.2 Security Requirements . . . 77
6.4 Defination . . . 78
6.5 Proposed ESPAC Scheme . . . 80
6.5.1 Phase-A: secure data communication: . . . 80
6.5.2 Phase B: Control of data requesters access . . . 82
6.6 Security Analysis . . . 84
6.7 Performance Analysis . . . 86
6.8 M-ESPAC:Modified ESPAC for User Revocation and Audit . . . 89
6.8.1 Multi-parties Proxy Re-encryption Protocol . . . 90
6.8.2 System Initialization . . . 90
6.8.3 Communication Between Patient and HSP . . . 92
6.8.4 PHI Encryption Based on Privacy . . . 92
6.8.5 Storing PHI at Cloud . . . 93
6.8.6 PHI Access and Multi-parties Proxy Re-encryption . . . 94
6.8.7 PHI access by DAR . . . 95
6.9 Audit of Stored PHI . . . 95
6.9.1 Partial Audit . . . 95
6.9.2 Block Audit . . . 96
6.10 Summary . . . 96

7 Conclusions and Future Work **97**
7.1 Conclusions . . . 97
7.2 Future Work . . . 98
7.3 Final Remarks . . . 99

Author's Publications 100

Bibliography 102

List of Tables

1.1 Different eHealth scenario - Indoor 6
1.2 Different eHealth scenario - Outdoor 6
3.1 Time and energy cost for cryptographic operations 27
4.1 Simulation Parameters 46
5.1 Simulation Parameters 67
6.1 Time cost for ESPAC operations 86
6.2 Simulation Parameters 89

List of Figures

1.1 Data flow diagram of patient's health information 2
1.2 eHealth infrastructure 5

3.1 A coexisting application scenario of WBAN with WPAN and WLAN . . . 17
3.2 Multilevel Architecture of WBAN 18
3.3 Multi-Hop WBAN 22
3.4 Flowchart of the secure data processes in WBAN 25
3.5 Average Energy Per Round 29
3.6 Traffic scheduling at PDA 30
3.7 Mean waiting time with variable weighting factor 34
3.8 Mean waiting time with different arrival rate 35

4.1 System model of the ASTP 40
4.2 Routing steps of the proposed ASTP protocol 44
4.3 Relation among P_{Tr}, p, and n 45
4.4 Average Packet Delivery Ratio 47
4.5 Average Packet Delivery Delay (in ms) 47

5.1 System model of proposed RuralCare scheme 54
5.2 Data Packet architecture of RuralCare scheme 61
5.3 Relation among P_f, p_i, and n 65
5.4 Packet delivery ratio with HT=45min 68

5.5 Packet delivery ratio with HT=2hrs 68
5.6 Delivery ratio with N=60 69
5.7 Delivery ratio with N=100 69
5.8 Average delay within 12 hours simulation with number of vehicles N=60 and 100 70

6.1 Major steps of the proposed ESPAC scheme 76
6.2 Access trees based on different data privacy level 78
6.3 Two major phases of the proposed scheme 80
6.4 Data packet architecture 83
6.5 Computation time of encryption and decryption with different no. of attributes 86
6.6 Queuing comparisons for the QoS requirements 88
6.7 Comparison of average end-to-end delay 88
6.8 Framework of multi-parties proxy re-encryption protocol 91
6.9 Sample PHI block architecture 92

List of Abbreviations

WBAN	Wireless Body Area Network
MANET	Mobile Ad hoc Network
DTN	Delay Tolerant Network
VANET	Vehicular Ad hoc Network
ABE	Attribute Based Encryption
CP-ABE	Cipher-text Policy Attribute Based Encryption
TA	Trusted Authority
HSP	Health Service Provider
CSP	Cloud Service Provider
DAR	Data Access Requester
AT	Access Tree
RSU	Road Side Unit
OBU	On Board Unit
RAP	Rural Access Point
PHI	Patient Health Information

Chapter 1

Introduction

1.1 eHealth Care System and Challenges

Electronic Healthcare (eHealth) system has drawn a lot of attention from the research community and industry to face the challenge of rapidly growing elderly population and rapidly rising health care cost. It is defined as the application of information and communication technologies across the whole range of function that affect the patient's Personal Health Information (PHI), Fig.1.1 shows the data flow diagram of PHIs.

The eHealth service provisioning is an increasingly important need today as the number of chronic illness in the industrialized countries is growing rapidly and an urgent solution for minimizing the health services cost is needed. Various statistics reports indicate that 133 million people, or almost half of all Americans live with a chronic condition. That number is projected to increase by more than one percent per year by 2030, resulting in an estimated chronically ill population of 171 millions [1]. In Canada, the aging population is considered to be a key contributor to the rising costs of healthcare [2]. This is due to the fact that over 50 per cent of an individual's lifetime expenditures on healthcare occur after the age of 65, and the number of individuals over the age of 65 is expected to rise extensively [2]. The current percentage of the Canadian population over age 60 is 17 per cent; however, this is projected to increase to 28.5 per cent by the year 2031 [3]. This portion of population however, accounted for 42.7 per cent of the total health expenditure for Canada [2]. In [4], it is shows that $5,170 per person has spent for health care in the year 2008 in Canada. This amount is increasing as the percentage of the elderly people is also increasing over the years. On the other hand, waiting time to have a house-physician and waiting time in the clinic and hospitals is still considered as a stress from the patient's side. All these statistics

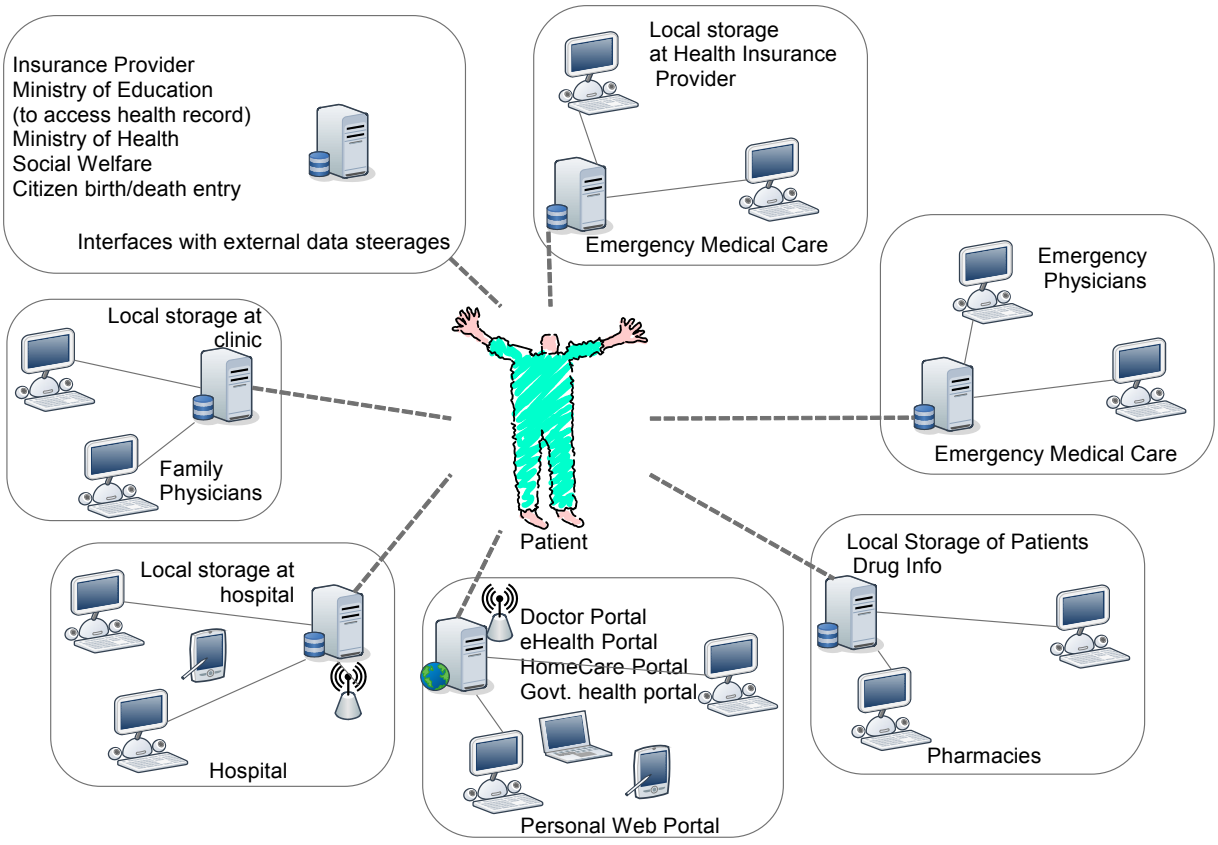

Figure 1.1: Data flow diagram of patient's health information

suggest that health care needs a shift toward more scalable and more affordable solutions. Restructuring our healthcare systems towards proactive managing of wellness rather than illness, and early detection of diseases is the answer to these problems. Introducing the eHealth care system will lessen the economic impact due to the citizen health care and an increased lifespan of the humans can be achieved via pervasive monitoring of health indicators to detect diseases in early stages. Not only does it help reduce the effect of chronic illness, it also may potentially save life.

Till now, medical monitoring requires the use of wires that connect patients with monitoring devices and reduce their mobility and comfort at the same time that also hamper the work of doctors and medical staff. Due to its numerous wires, rigid form, and adhesive electrodes, comfort is compromised and making it cumbersome and unnatural for the user to wear the devices continuously. In addition, these systems work as off-line and patients need to visit the clinic to retrieve and analyze the recorded data. All of these lacking and the increasing pressure for the health support bring the necessity of the wireless technology to be used in the health care system. Therefore, The wireless technology in eHealth care system will open the door of the remote home care facilities integrating with the quality health services. Advances in wireless communications and computing technologies have lent great forces to the migration of health care systems from current paper based to eHealth system.

Recent technological developments in low-power integrated circuits, wireless communications and physiological sensors promote the development of tiny, lightweight, ultra-low-power monitoring devices. A body-integrated network, so called Wireless Body Area Network (WBAN), can be formed by integrating these devices. It is now possible to deploy bio-sensors on,in, or around the patient body and allow to continuous monitoring of physiological parameters (e.g. electrocardiogram (ECG), blood oxygen level, heart rate, temperature, blood pressure, glucose levels etc.) with physical activities. Inexpensive radio transceivers that integrated with different bio-sensors form the body area network, where a PDA (Personal Digital Assistant) works as gateway or network coordinator. WBAN has lent great forces to the migration of health care system from hospital or care-unit to the patient's residence and mitigates the overall health-care expenses. Integrating this technology with the existing wireless technologies (e.g., cellular 3G, WiMax, Wi-Fi, GSM, GPRS) forms an integrated heterogenous wireless network and permits real-time mobile and permanent monitoring of patients, even during their daily normal activities. In the heterogenous network, multi-hop routing reduces cost of deployment, enhances network performance, increases the network coverage area as well as reduces the service cost [5, 6]. Routing the patient's highly sensitive PHI over this unsecured wireless environment must need to ensure proper security with data integrity and confidentiality.

In addition, the eHealth care system needs to ensure the availability of PHI in electronic form adheres to same level of privacy and disclosure policy as applicable to present day paper-based patient-records accessible only from the physician's office. Instead of storing the PHI locally, the recent advancement of cloud computing allows us to store PHI at cloud-storage and ensures availability with reduces capital and operational expenditures [7] (e.g., HealthVault from Microsoft, Health Cloud from google). Moving patients' PHI into a cloud or in a central storage offers enormous conveniences to the eHealth-care-providers, since they don't have to care about the complexities of direct hardware management. However, patient's privacy with proper access control of this available PHI is a growing concern in the eHealth care industry due to the direct involvement to human. Traditional data access schemes which are used to provide data confidentiality mostly depend on the system itself to enforce authorization policies and rely on the system trusted infrastructure. These schemes are not appropriate for eHealth care system, as cloud storage providers are not fully trusted and patients generally want to be sure that their sensitive health information can only be accessed by particular authorized users with identity privacy.

1.1.1 eHealth Characteristics

Depending on the location of patient, either wired or wireless technology can be used in the eHealth care system. Indoor and outdoor applications are the two scenarios for the proposed eHealth care system. Patient stays in hospital, long-term care center, nursing/old home etc. in indoor scenario and patient locates at social gathering spot (mall, prayer hall etc.), surrounding areas of health service provider or patient's residence etc. In all possible cases data traffic flows mostly from patient to the service provider side. Fig.1.2 shows the possible eHealth infrastructure and Table 1.1 and 1.2 show different application scenarios with network and security constants. Low, medium, and high are used to show security requirements, where 'high' means a mandatory requirement, medium is used for optional and good to be used, and low is not that much important.

eHealth care services are expected to use mobile ad-hoc network, delay tolerant network, and vehicular ad-hoc network depending on patient's location to provide cost effective health care services.

1.1.2 Application of eHealth

The applications of eHealth aim at providing better healthcare services to patients. Integrating with WBAN has shown great potential to expand the use of eHealth care system

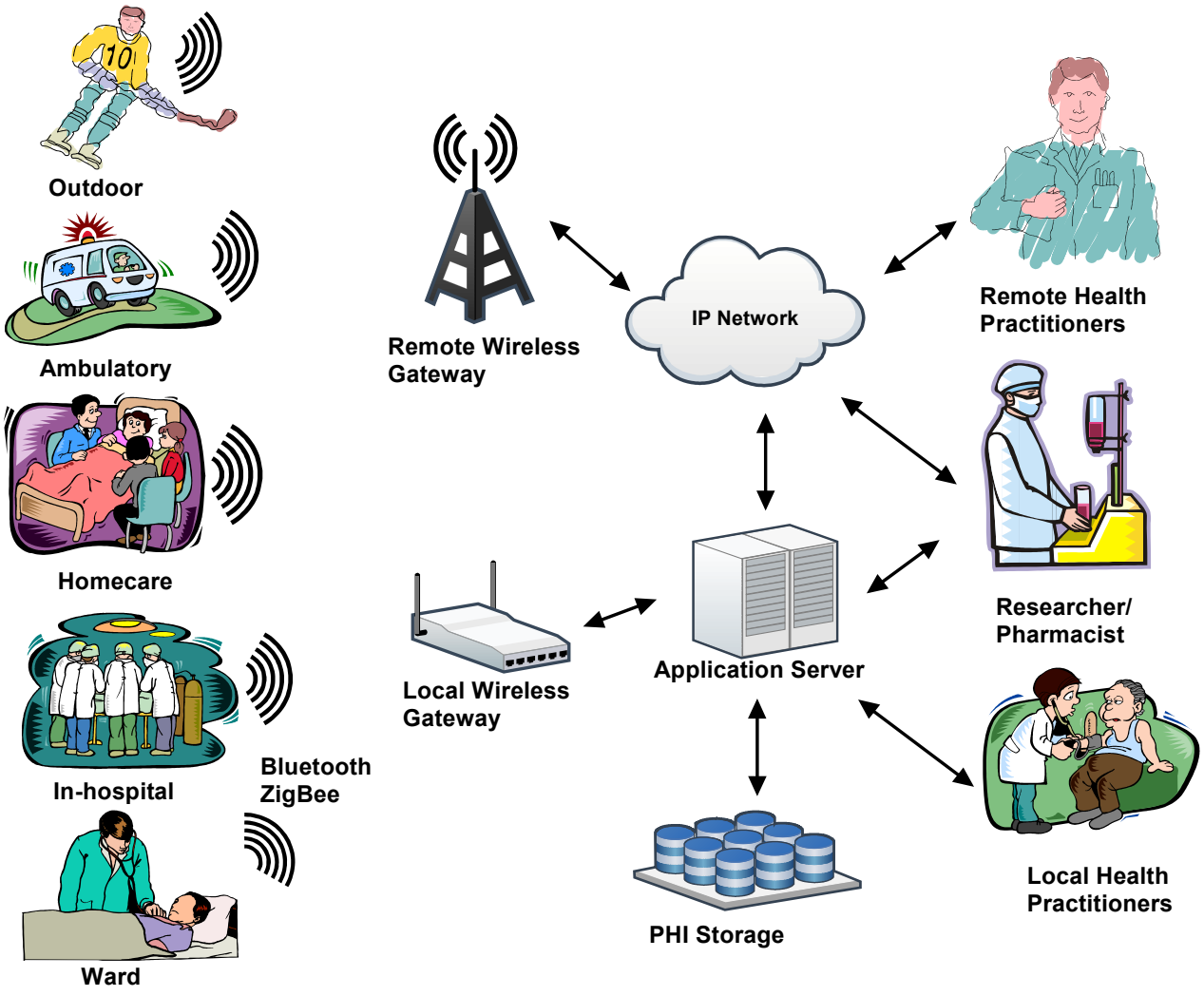

Figure 1.2: eHealth infrastructure

Table 1.1: Different eHealth scenario - Indoor

Description	**Network type**	**Security Requirements**
Patient resides in the hospital-cabin or in incentive care unit	Wired	Low
Patient in residence or in hospital cabin	Wireless (One-hop to Access Point (AP))	medium
Patient in hospital, long term care center, shopping mall, prayer hall	Wireless (multi-hop)	High

Table 1.2: Different eHealth scenario - Outdoor

Description	**Network type**	**Security Requirements**
Patient close to health service provider, shoping mall, park	Mobile Ad-hoc Network (MANET)	High
User is traveling	Delay Tolerant Network (DTN) Vehicular ad-hoc network (VANET), MANET	High
Users reside at rural area	DTN, VANET	High

from from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems.

1. Continuous Monitoring: Continuous monitoring is one of the promising applications of eHealth. People with different degrees of cognitive and physical disabilities will be enabled to have a more independent and easy life. Elderly people don't need to be accompany 24/7 days. It will also ease the life of patient's relatives and minimize the nursing cost.

2. Global Health Support: Patient health-care-giver can access to stored patient's PHI though internet by proper authorization. It will provide anytime-anywhere patient care. In the near future, people will get the boarder-less health services using the RFID-enabled healthcard or national card [8].

3. Emergency Health Support: Body sensor used in WBAN will help to identifying emergency situations like heart attacks or sudden falls in a few seconds, and in a life-threatening emergency situation it will be possible to provide immediate care to patient when the patient might be insensible.

4. Patient care at rural area.

5. Location tracing: GPS(Global Positioning System) enabled eHealth devices will help the care givers to locate the users.

6. Social network: Patients having same types of diseases may form a group and can maintain a social network. They may share the health related information among them.

7. Physicians appointment booking: The system will automatically book an appointment in advance based on the merit of the critical sensed data.

8. Family member's health monitoring: Patient's responsible family members can know the latest health condition of patient using eHealth care services, despite of their different locations.

1.2 Security and Privacy Threats

Although eHealth care system is expected to use different wireless technologies but security and privacy are the common issues. In addition, healthcare facilities have specific security concerns that are not found in most other environments. Maintaining an acceptable level of security in this unique environment is extremely difficult. Furthermore, health care organizations, dealing with such sensitive data as patients' personal health information, have to be extremely wary of the potential privacy and security risks of converting to electronic information infrastructures. In general, the security threats in the eHealth care system can be classified into following categories.

Passive Attackers

- Eavesdropping attack: An attacker listens to the transmissions between the legitimate network entities. Some sensitive information such as the exchanged data or routing information could be leaked to an attacker. This attack can be prevented by using an end-to-end encryption; even if an attacker intercepted a packet, he can not interpret it. In the eHealth care system, the transmitted information is the patient PHI, which is highly privacy-sensitive to the owner. If an attacker is able to eavesdrop the PHI during the wireless transmission, the application cannot be accepted.

- Privacy violation attack: An attacker reveals confidential information regarding the identities and locations of the participant users. One technique to thwart this attack is to hide the real identity by using pseudonyms instead of one permanent identity.

Active Attackers

- Jamming attack: An attacker deliberately generates a huge amount of bogus messages to join or interrupt the on-going communication. It may prevents the genuine patient to do their regular communication.
- Forgery attack: An attacker can launch forgery attack, which could potentially cause distrust problems among the legitimate network entities. Therefore, the freshness and correctness of the transmitted message are very important to ensure that the received message are not forged. In the eHealth care system, the forged PHI would result in the compromising medical circumstances for patients, and the forged emergency message would waste a huge amount of heathcare resources.
- Insider attack: Malicious insider can be able to access the stored PHIs and can be succeed in stealing a legitimate user's identity and impersonates another user for malicious purposes, or sell the sensitive PHI to the third party.
- Collusion attack: Multiple attackers including the revoked untrusty user initially conspire to find the secrets of the PHI storage server. Then they try to get a copy of patient's sensitive PHI. Users' roll-based access control to the stored PHIs is required to prevent collusion attack.
- Replay attack: An attacker monitors the traffic (passive attack) then retransmits the message as the legitimate patient. Time-stamps with data encryption is needed to prevent this attack.

1.3 Security and Privacy Requirements

In order to protect the eHealth applications against the threats mentioned above, the security and privacy preservation mechanism employed in the eHealh care system must have the following properties [9, 10].

- Authentication: It is the ability to ascertain that a thing is indeed the one that it claims to be. Message authentication is of vital importance in eHealth care system because it ensures that a received message is indeed sent from a legitimate and registered patient in the networks.

- Integrity: It is the ability to assure that the transmitted messages have not been subject to modifications, additions, or deletions. Integrity assures that all the PHI sent from the patients PDAs or gateway to the online PHI databases should be unaltered.

- Non-repudiation: Non-repudiation is the ability to prevent an authorized user from denying the existence or contents of the message sent by itself. Non-repudiation for eHealth is a critical property because it can prevent an attacker from denying the attacks that he/she has launched.

- Access control: It is necessary to ensure reliable and secure operations of a system. In the eHealth care system, the legal users should have fine-grained capabilities to access the different parts of PHI for the different purposes; any malicious user should be revoked from the network to protect the safety of the privacy-sensitive PHI.

- Privacy: It is the ability to protect private information from an untrusted user. Identity and location information of any individual should be protected in an eHealth care system and the information can only be used in an emergency situation or used by the TA for the conflict resolutions. Moreover, multiple transactions of one individual should not be linked together by other entities except the TA.

1.4 Research Motivations and Contributions

The research in this thesis focuses on developing a suite of protocols to deal with the challenging security and privacy-preserving issues in eHealth care systems. Specifically, the research motivation and contribution are summarized as follows:

- First, secure data aggregation process starts from the patient side and the wearable body sensors' perform the initial sensing task. Generally medical sensors are implanted on,in or around the patient's body and can continuously monitor patient's PHI. Body sensors work individually and form an ad-hoc network where a power-adequate sensor or PDA works as gateway. Since frequently changing or charging the batteries of the deployed sensors is a burdensome work for patients, the power consumption of the PHI transmission is desired to be highly efficient. Meanwhile, the output transmission power of the sensor nodes must be kept minimal for health issues; adverse biological effects will be caused by wireless radio intensive radiation for

long-term inspection. Thus, it is very promising to design a multi-hop routing protocol where the transmission range is required to be shorter. However, due to sensitive data type and human social involvement, security and privacy is also a challenging issue in WBAN like other traditional wireless networks. In addition, the limited power supply of the body sensors poses critical computation and communication constraints on designing a secure and privacy preserving schemes for body sensors. For example, the computational cost and communication overhead of a traditional encryption, such as public key encryption, are unaffordable to the body sensors. Many research efforts on secure communication in WBANs [11–15] have been carried out. The common goal of these works is to efficiently and securely assign a secret key among deployed sensors and gate-way in a WBAN environment. In this thesis, we review some related protocols and study the security and privacy issues in WBANs. We find the existing works neglect user mobility, sensor's energy and computational power inefficiency, and reusability of sensor devices for different patients. To address these issues, we propose a light-weight secure protocol based on hybrid cryptographic operations and integrate session key with time-stamp to ensure reusability. We also propose a secure infrastructure for multi-hop communication in WBANs that ensures secure communication with minimum energy requirement. During the work on secure protocol design, we found that patient's health information can be classified into different categories and a packet priority management scheme need to be implemented at the gate-way of WBAN to ensure reliable and efficient PHI aggregation. Addressing this issue, we also propose a priority management scheme integrated with our secure protocol that ensures QoS with adequate security and privacy.

- Second, delivering the PHI from an individual PDA or gate-way to the eHealth care service provider is very difficult when patients do not have direct link to the Internet. Even if the patient is in a cellular network coverage, due to service-cost and continuous data forwarding requirement it is not a suitable solution for continuous patient monitoring. Extending existing wireless network to cooperative multi-hop wireless network can permit long-term permanent patient monitoring with low-cost. In this cooperative environment, users can form an on-demand ad-hoc network and use multi-hop routing to enhance network performance, minimize the cost of deployment, increase the coverage area as well as reduce the overall service cost. In a multi-hop wireless network, participant nodes act as relay nodes to forward neighbor's data packets. However, not every node is cooperative or willing to forward others data traffic. The noncooperative node leads to degradation in the Quality of Service (QoS) of the network by dropping data packets. Moreover, noncooperative node may be a malicious node and fabricates the network routing information, as

well as modifies the message that passes through it. Choosing the cooperative relay node becomes more challenging in an environment where users have the services from different service providers and the application has to support real-time data communication, like as remote patient monitoring. Many research works [16–20] studied the cooperation data forwarding with incentive. In this thesis, we propose a data aggregation scheme based on mutual thrust and historical behaviour with incentive, where trusted authority (eHealth care giver) plays a vital role. In addition, data integrity with authentication, network availability, and user privacy during the communication is also considered as a key requirement for an uninterrupt secure PHI aggregation scheme. The designed protocol also includes trust management, incentive and reward provision policy, and the patient's privacy requirements.

- Third, due to the recent growth of urbanization, people are moving from rural to urban areas. But half of the world population still lives in the rural area. Specifically, in USA and Canada, around 20% of the total population lives in rural area, 56% of the population in the 27 Member States of the European Union (EU) lives in rural areas, and 60% in China [21]. Moreover, some large metropolitan areas contain small towns and these small towns are isolated from the central cluster. Providing long-term health care to these areas is also challenging. To overcome this challenge, we propose a Delay Tolerant Network (DTN) based PHI aggregation scheme, where conventional transportation vehicles (e.g., cars, buses) act as relay nodes. These vehicles are expected to store, carry, and forward the PHI to the health-service-provider located mostly at the city area following an opportunistic routing. Network fairness and resistance to different possible attacks are also ensured by the proposed work.

- Fourth, the central trusted authority in an eHealth care system maintains a database of aggregated PHI to ensure future availability and to provide long-term access to the health professionals. Traditional data access schemes which are used to provide confidentiality are mostly depend on the system itself to enforce authorization policies and rely on the system trusted infrastructure. Instead of storing the PHI locally, the recent advancement of cloud computing allows us to store all PHI at the cloud storage and ensures availability with reduces the capital and operational expenditures. However, storing the patients' PHI at cloud-storage increases data-owners concern to his sensitive PHI. Patient generally wants to be sure that his sensitive health information can only be accessed by particular users and his original identity will not be exposed in general. Health service provider needs to ensure only the legal entity will get the stored PHI access. Patients' consent and willingness need to be considered

to design a PHI access role. Many research works [22–28] studied secure architecture for cloud storage. In this thesis, we present a patient-centric access control of aggregated stored PHI with minimum computation at the cloud side. We propose proxy re-encryption, where trusted health service provider works for a registered user and re-encrypts PHI for a specific PHI access requester. To ensure stored data correctness, our scheme is further updated with an audit system. Trusted authority can easily check the correctness of the stored data by using the propose scheme.

1.5 Outline of the Thesis

The organization of the remainder of the thesis is as follows. Chapter 2 review some basic techniques and definitions of cryptographic operations. Chapter 3 presents a secure and efficient data aggregation scheme for a WBAN that combines public and private key cystography and ensures power-efficient secure communication among energy and storage constant body sensors. Chapter 4 presents a secure and trustworthy PHI aggregation scheme considering the neighbor nodes' previous and recent activities. A cooperative packet forwarding protocol using vehicular delay tolerant networks is presented in chapter 5. Chapter 6 presents patient-centric access control of the aggregated PHI with auditing in a cloud environment. Finally, conclusions and future research work are described in Chapter 7.

Chapter 2

Technical Background

In this chapter, we briefly describe different definitions and techniques that used in this thesis.

2.1 Pseudonym Technique for Identity Privacy

A pseudonym is a name that a person assumes for a particular purpose, which differs from his or her original or true name. Pseudonyms have no literal meanings, and they can be used to hide an individual's real identity. In a network environment, pseudonyms have been widely adopted to preserve user's identity privacy [29]. An offline trusted authority (TA) is considered to initialize pseudonyms for users prior to the network deployment. The TA will assign multiple pseudonyms for each individual user. These pseudonyms cannot be linked by anyone but the TA. Each user changes their pseudonyms in the communications when needed such that their behavior cannot be linked by the different pseudonyms. When users consume all the pseudonyms, they can contact with the TA to update with new pseudonyms.

To avoid the forgery attacks of pseudonyms, the TA assigns an additional secret to users according to their pseudonyms. Only with the secret, a user can prove that the pseudonym is legally held. The identity-based signature can be a solution. The TA generates a private key for each pseudonym, and assigns the private key to the user. The user can always sign on any message with the private key, and the generated signature can be verified with the pseudonym. In this way, the forgery attacks of pseudonyms can be prevented.

However, with pseudonyms, users may launch malicious attacks, such as sybil attacks. To prevent the abuse of pseudonyms, the TA needs to set a trapdoor when generating the pseudonyms such that it can trace user behavior. Generally, mapping function is used to implement traceable pseudonyms:

- Mapping function: The TA generates k pseudonyms pid_i for user u_i. For each pseudonym pid_i, the TA also generates a corresponding pseudonym secret key psk_i and sends the key to u_i in a secure channel. Then, u_i is able to use pid_i in the communication protocols. He can generate a signature using psk_i to make others confirm that u_i is the legal holder of pid_i. In the meantime, the TA maintains a map from these pseudonyms to the real identity id_i of u_i. When needed, others can always report the signature to the TA who is able to track u_i's behavior.

2.2 Cryptographic Techniques

2.2.1 Bilinear Groups of Prime Order

Bilinear pairing is an important cryptographic primitive and has been widely adopted in many positive applications in cryptography [30] [31]. Let $\mathbb{G}$ be a cyclic additive group and $\mathbb{G}_{\mathbb{T}}$ be a cyclic multiplicative group of the same prime order q. We assume that the discrete logarithm problems in both $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are hard. A bilinear pairing is a mapping $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$ which satisfies the following properties:

- Bilinear: $\forall P, Q \in \mathbb{G}_1, \forall a, b \in Z_q^*$
  $e(aP, bQ) = e(P, Q)^{ab}$
- Non-Degeneracy: $P \neq 0 \Rightarrow e(P, P) \neq 1$
- Symmetric:$\forall P, Q \in G_1, e(P, Q) = e(Q, P)$.
- Computability: e is efficiently computable.

Definition 1 *(Bilinear Generator) A bilinear parameter generator Gen is a probability algorithm that takes a security parameter as input and outputs a 5-tuple* $(q, P, \mathbb{G}, \mathbb{G}_T, e)$*, where* q *is a -bit prime number,* $(\mathbb{G}, +)$ *and* $(\mathbb{G}_T, \times)$ *are two groups with the same order* $q, P \in \mathbb{G}$ *is a generator, and* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ *is an admissible bilinear map.*

In the following, we define the quantitative notion of the complexity assumptions, including Computational Diffie-Hellman (CDH) Problem, Decisional Diffie-Hellman (DDH) Problem, Bilinear Diffie-Hellman (BDH) Problem, and Decisional Diffie-Hellman (DBDH) Problem.

Definition 2 *(Computational Diffie-Hellman (CDH) Problem) The Computational Diffie-Hellman (CDH) problem in* $\mathbb{G}$ *is defined as follows: Given* $P, aP, bP \in \mathbb{G}$ *for unknown* $a, b \in \mathbb{Z}_q^*$*, compute* $abP \in \mathbb{G}$*.*

Definition 3 *(Decisional Diffie-Hellman (DDH) Problem) For* $a, b, c \in \mathbb{Z}_q^*$*, given* $P, aP, bP, cP \in \mathbb{G}$*, decide whether* $c = ab \in \mathbb{Z}_q$*. The DDH problem is easy in* $\mathbb{G}$*, since we can compute* $e(aP, bP) = e(P, P)^{ab}$ *and decide whether* $e(P, P)^{ab} = e(P, P)^c$ *[32].*

Definition 4 *(BDH Parameter Generator) An algorithm Gen is called a BDH (Bilinear Diffe-Hellman) parameter generator if Gen takes a sufficient large security parameter* $K > 0$ *as input, runs in polynomial time in* K*, outputs a prime number* q*, the description of two groups* $\mathbb{G}_1$ *and* $\mathbb{G}_2$ *of order* q*, and the description of a bilinear map* $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$*.*

Definition 5 *(BDH Problem hardness) Given a random element* $P \in \mathbb{G}_1$*, as well as* aP*,*bP*,*cP*, for some random* $a, b, c \in \mathbb{Z}_q^*$*; there is no efficient algorithm to compute* $e(P, P)^{abc} \in \mathbb{G}_2$ *from* $P, aP, bP, cP \in \mathbb{G}_1$*. This implies the hardness of the BDH in the group* $\mathbb{G}_1$ *[30].*

Chapter 3

Energy Efficient and Secure Data Aggregation in WBAN

3.1 Introduction

Wireless Body Area Network (WBAN) is considered as a promising technology that provides short range, low power and reliable wireless communication in a close proximity to or inside human body. A PDA (Personal Digital Assistant) works as a gateway or network coordinator in this network. The major uses of this technology can be classified as medical and non-medical applications. Different bio-medical sensors are deployed on, in, or around the patient body to measure the different health data, such as Temperature, Heart rate monitor, Blood pressure monitor, Pulse oximeter SpO2, pH monitor, Cardiac arrhythmia monitor/recorder, Brain liquid pressure monitor [33]. Real time video, audio streaming, data file transfer, remote control application, real time gaming, body positioning etc. are some non-medical applications using the WBAN technology.

The use of WBAN in eHealth, which is crucial for human life, highlights the importance of security and privacy. Computation, memory, and communication capabilities limited sensors need to be securely connected with the PDA. We also need to ensure confidentiality and integrity of the user's bio-medical sensed data. To minimize the network overhead and maximize the network life time, sensors have to communicate themselves using a group key. Sensors use this group key to ensure a reliable group communication in the WBAN.

Supporting the real-time application in the resource inadequate WBAN is always considered as an important issue. Different real-time and non real-time applications in WBAN

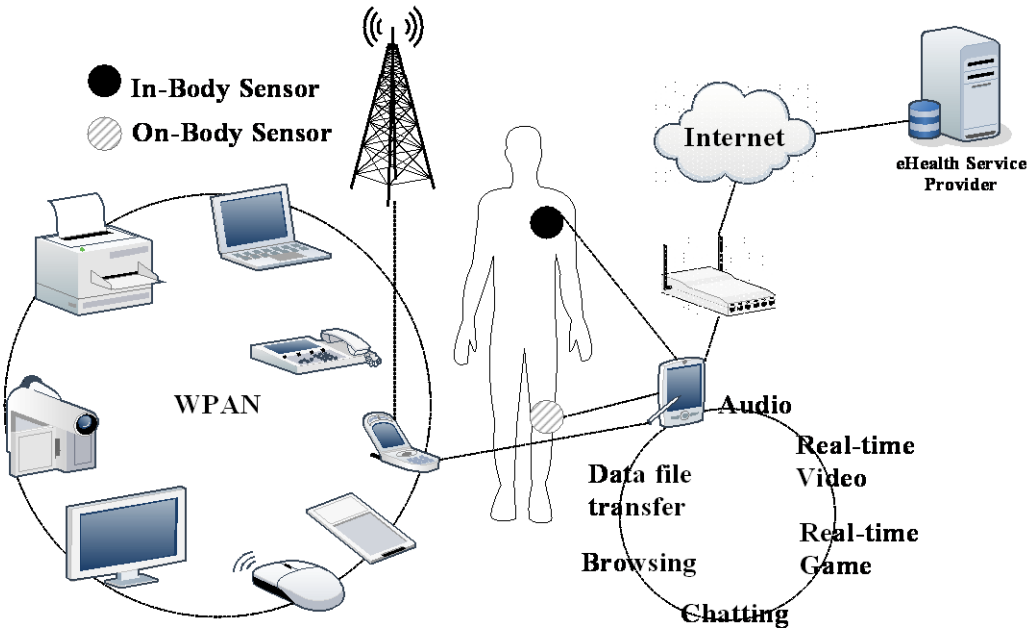

Figure 3.1: A coexisting application scenario of WBAN with WPAN and WLAN

need different types of services and require specific analyses and accurate estimation of the QoS levels. The emergency data packets of the eHealth applications must be served with the required QoS level so that a pervasive and trusted assistance is provided to patients under the different health risks. The issue becomes more critical if the network capacity is insufficient. Other non-medical real time applications like multimedia streaming application, gaming also need fixed bit rate and they are also delay sensitive. Proper prioritization among these real-time applications can only guarantee a certain acceptable level of performance. Among different QoS parameters, availability, confidentiality and privacy, data delivery latency, reliability, and mobility support are considered the major requirements of an eHealth care system [34]. In this work, we propose a secure and privacy preserving communication including real-time traffic scheduling using WBAN. We classify the real-time and non real-time traffic in WBAN to minimize the mean waiting time of the high priority, delay sensitive eHealth application traffic.

3.2 WBAN Architecture

Wireless body area network (WBAN) consists of low-power, lightweight, small-size, and intelligent sensors that are placed on, in or around the human body ,and generally used to monitor different humans physiological signals and motion for medical, personal entertainment and other applications and purposes. Compared with traditional WLANs, WBANs enable wireless communications in or around a human body by means sophisticated pervasive wireless computing devices [35]. Based on the type of application, various sensors deployed in, on or around the body continuously or periodically monitor vital signals and send data to nearby gateway (PDA, mobile devices or personal server). This gateway is also called as Network Coordinator (NC).

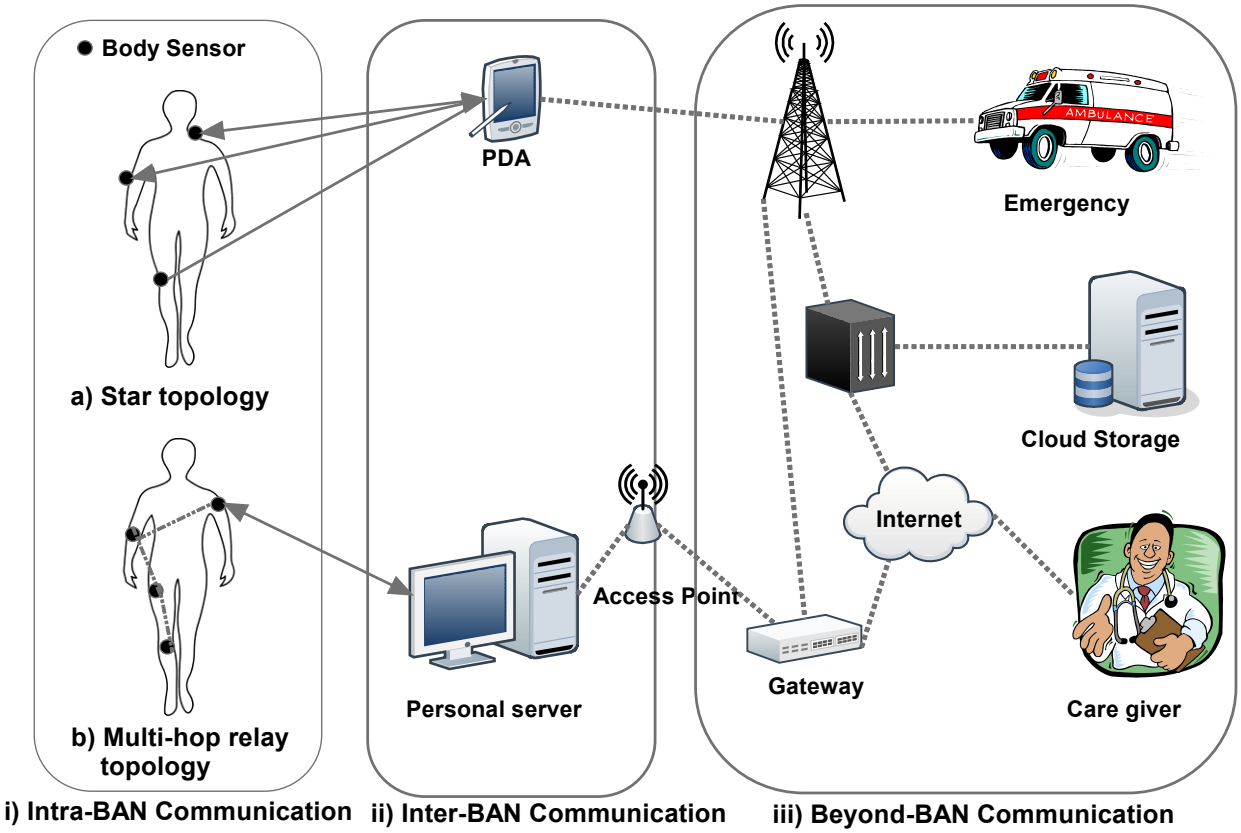

Figure 3.2: Multilevel Architecture of WBAN

Fig. 3.2 demonstrates multi-level architecture of a WBAN. Intra-BAN communication

can be performed using Star or Multi-hop relay topologies. Inter-BAN communication usually refer to radio communication of about 2 meters around the human body using Bluetooth or Zigbee [36]. Beyond-BAN communications is designed to use in Metropolitan Area Network (MAN) and involves on health care related applications.

3.3 Security and Privacy Requirement at WBAN

Before presenting our approach to ensure data security and user privacy for WBANs, we first describe the security and privacy requirements for a WBAN. The term of data security means the sensed data is securely stored and transferred, data privacy means the data can only be accessed by authorized users, and user privacy means data owner's identity privacy. We categorized security and privacy requirements in a WBAN for an eHealth application into two categories: security and privacy in communication initialization and network communication data security.

3.3.1 Security and Privacy in Communication Initialization

Secure Management

Based on the diversity of the health application, body sensors might be owned by a specific user or might be shared by a group of authenticated users at the care giver place. Network coordinator with help of trusted health service provider ensures proper selection of encryption and digital signing algorithm with system parameters.

Device Initialization and Bindings

It confirms the identity of the original source node. The WBAN coordinator must need to verify the original source of data before accepting the received data. Sensor devices need to be bind with a specific coordinator to ensure secure communication.

3.3.2 Network Communication Data Security

Data Confidentiality

Among different data security requirements, confidentiality of patient data is considered as one of the major requirements. It is required to protect the data from disclosure [37, 38].

Patient's vital health information should not be leaked to external or other WBAN network situated in the network coverage. An adversary or attacker can eavesdrop on the communication, and can overhear the critical patient's health information. This eavesdropping may cause severe damage to the patient since the adversary can use the acquired data for many illegal purposes.

Data Integrity

Keeping the data confidential by using traditional encryption does not protect it from external modifications. An adversary can always manipulate the data within a packet by adding additional fragments and this packet can later forwarded to the WBAN's coordinator or master node. Lack of data integrity can cause severe problem in the case of life-critical events, where emergency data is altered by the attacker.

Data Authentication

It confirms the identity of the original source node.

Data Freshness

The adversary may sometimes capture data in transit and replay them later using the old key in order to confuse the coordinator. Data freshness implies that the data is fresh and that no one can replay old messages.

3.4 Related Works

Recently, trust based routing has gained much attention as an effective way to improve data routing security. Chi et al. [39] identified the unique features of trust metrics compared with QoS-based routing metrics. In that protocol, a systematic analysis of the relationship between trust metrics and trust-based routing protocols was presented. A model for trust evaluation and trust update based on fuzzy logic is described in [40]. This model is first used to analyse the physical requirements and psychology of the malicious attackers and then modify the corresponding nodes trust values. Cooperation between neighbour nodes are used to find out the trust node in [16, 41]. To provide fairness, an incentive mechanism is integrated with the routing protocol in [16]. The overhead of the communication was

reduced by using a cheating detection system. Lu et al. [42] improve the packet delivery ratio and resist most possible attack in a vehicular delay tolerant networks by presenting a social-based privacy preserving packet forwarding protocol. A secure multicast strategy is proposed in [43] to allow trustworthy nodes participate in the communication. Wang et al. [6] present a linear trust evaluation method based on self-observed information of a certain node and other nodes.

Security and Privacy issues in eHealth care systems are addressed in [43–45]. Patient privacy, one of the most serious concerns of patients, is fairly addressed in [44]. Xiaodong et al. [45] proposed a privacy preserving scheme for heath care that can effectively work against global adversary. In [46], an authentication protocol is developed. The protocol uses "Time-stamp" to describe and verify the signature and the freshness of the message. Decker et al. [47] present a privacy-preserving eHealth protocol based on a credential systems. Entity authentication and item integrity are provided by verifiable public key cryptography.

3.5 System Model and Data Processes Steps in WBAN

Consider a WBAN composed of s body sensors that have minimum computational capabilities. We denote $S = s_0, s_1, ..., s_n$ the sensors set and s_0 is denoted as the coordinator. Each sensor is associated with a unique identifier such as MAC address or manufacture serial number by which it can be distinguished from others. Two nodes are called neighbour nodes if they are within each other communication range and there received signal strength is stronger compare to others. Neighbor nodes in a WBAN construct a stable backbone link for a multi-hop WBAN.

A shortest path tree rooted at the data sink n_0 is constructed using stable backbone link based on received acknowledgement signal strength. Here we would like to note that the multi-hop communication is only applicable to WBAN where the sensor's energy level is less than pre-defined threshold point. Instead of using real-time next hop selection routing protocol, we prefer to use defined next hop selection. Energy and computation inefficient sensor does not need to perform real-time next hop selection and we can ensure long life of the network. Fig. 3.3 shows the multi-hop communication architecture of WBAN.

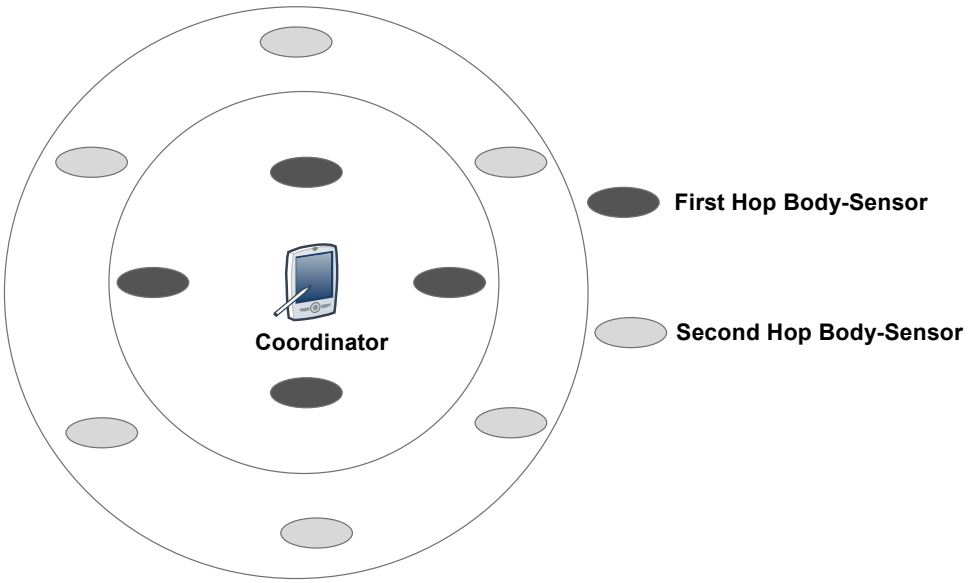

Figure 3.3: Multi-Hop WBAN

3.5.1 Security Model

In our work, we have considered external attacks in a WBAN where adversaries outside the network launched the attack. Inside attack in a WBAN environment is negligible as network is formed around or close to the user. DoS attacks are out of scope of this work. We do not consider lower-layer jamming or side-channel attacks. We used encryption and one-way hashing function to prevent eavesdropping attacks and data modification at low cost. Public-key cryptography usually consumes more energy to compute encrypted data, so we used hybrid approach (Public and Private key combinations) to minimize the overall cost.

3.6 Proposed Approach for Secure Data Aggregation in WBAN

3.6.1 Security initialization

At the very fist initialization phase, The trusted service provider or trusted authority (TA) will run the function $Gen(S)$ to compute the bilinear parameters $(q, \mathbb{G}, \mathbb{G}_T, e, P)$. The TA

will then do the following steps

1. Select a random numbers $\alpha \in Z_q^*$ and compute public key of a body sensor node as $PK_{SN} = \alpha \times P$;
2. Stores the PK_{SN} and secret keys α in the respective sensor nodes;
3. Provides an unique ID to the subscribers ID_{user};
4. Generate the secure hash function $H_1 : \{0,1\}^* \rightarrow G_1^*$
5. Distribute ID_{user}, PK_{SN}, and H_1 to the subscribers.

3.6.2 System Initialization by the User

The individual user will do the following steps:

1. Compute the sensors' pseudo-identity $PID_{SN} = H_2(ID_{SN}); H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$;
2. Select a random number $\beta \in_R Z_q^*$, to calculate the session key $P_\beta = \beta \times P$
3. Choose a random number $r \in Z_q^*$ and compute the public key $PK_U = r \times P$.

3.6.3 Source Authentication

The major source and data authentication tasks are performed by the WBAN's gateway. But during the multi-hops communication phase, participated sensors need to perform source authentication to confirm membership of the same network. Following steps are followed to perform the source authentication:

- Step 1: Let the provided secret key of the gateway is s_0 and the corresponding public key is $PK_{gw} = s_0 P$. The gateway generates the secret key of the sensor node as $S_{ID} = t \times PID_{SN} = s_0 H_2(ID_{SN})$.
- Step 2: Chooses an arbitrary $R \in \mathbb{G}$ and picks a random integer $k \in \mathbb{Z}_q^*$. Gateway or PDA then computes $\bar{r} = e(R,P)^k$.
- Step 3: Generates $m = MAC||KEY$, where MAC is the unique Media Access Control (MAC) address and KEY is the session key chosen by the authenticated user.

- Step 4: Computes $v = H_2(m, \bar{r})$ and $u = vS_{ID} + kP$.
- Step 5: Sends (u, v) as signature to sensor.

After receiving the message (u, v), sensor nodes perform the following verification to ensure source authentication.

- Step 1: At first, computes $\bar{r} = \frac{e(u,p)}{e(H_2(ID),PK_{gw})}$
- Step 2: Confirm source authentication if $v = H_2(m, \bar{r})$ is validated.

3.6.4 Message Encryption and Decryption:

Here we present how a sensor and PDA can encrypt and decrypt a message using the bilinear pairing cryptography. The processes will be followed at the first time of a session to distribute a session key securely among the nodes in a WBAN. Let K is the session key chosen by the PDA; it then compute

$$v = Enc(PK_{SN}, K, PK_U) = K \oplus H_4(g_U^r) \tag{3.1}$$

Here $g_U = e(Q_U, PK_U)$, $Q_U = H_3(PID_{SN})$; $H_3 : \{0,1\}^* \rightarrow G_1^*$ and $H_4 : G_2 \rightarrow \{0,1\}^*$ are secure hash functions.

The encrypted key is decrypted using the $Dec(PK_{SN}, v, d)$ function, here $d = \alpha H_3(PID_{SN})$ and α is the secret key of the corresponding sensor.

$$Dec(PK_U, v, d) = K \tag{3.2}$$

$Dec(PK_U, v, d) = v \oplus H_4(e(d, PK_U)$
$= v \oplus H_4(e(\alpha H_3(PID_{SN})), rP)$
$= v \oplus H_4(e(H_3(PID_{SN}), P)^{r\alpha})$
$= v \oplus H_4(e(H_3(PID_{SN}), \alpha P)^r)$
$= (K \oplus H_4(g_U^r) \oplus H_4(g_U^r)) = K$

Fig. 3.4 demonstrates the proposed secure the data process in a WBAN.

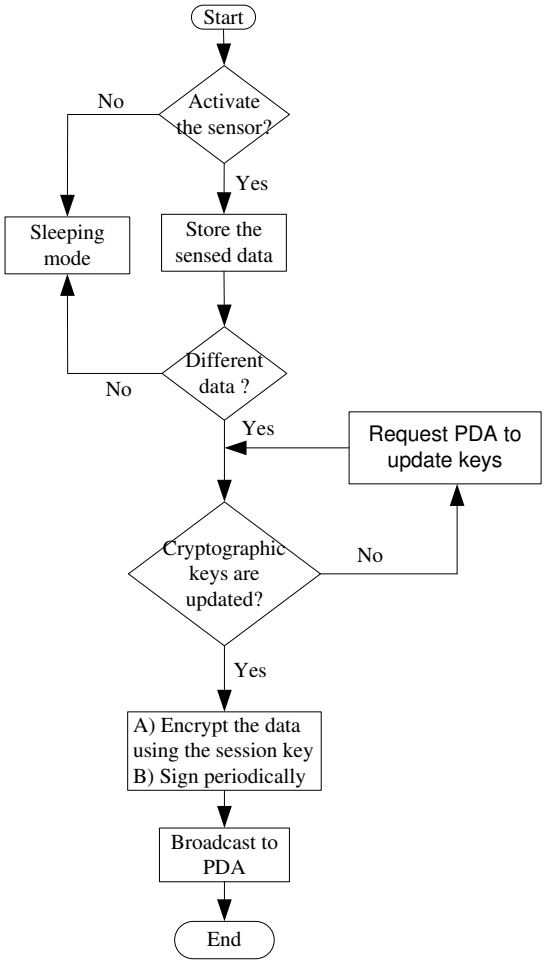

Figure 3.4: Flowchart of the secure data processes in WBAN

3.6.5 Signature and Verification

User U will sign the message v using the cryptographic digital signature (equation 3.3) that is also based on bilinear pairing.

$$S = Sig(v, \beta, r) \tag{3.3}$$

$$S = \frac{1}{v+\beta+r}P$$

The sensors will verify it using the equation (3.4).

$$e(vP + P_\beta + PK_U, S) = e(P, P) \tag{3.4}$$

$e(vP+P_\beta+PK_U, S) = e((v+\beta+r)P, (v+\beta+r)^{-1}P) = e(P,P)^{(v+\beta+r)(v+\beta+r)^{-1}} = e(P,P)$.

The sensor only need to verify the signature during the periodic key updating process. When the session key is securely distributed among the sensors, they will simply use the key K to encrypt the message as $Enc(K, message)$ or decrypt the ciphertext as $Dec(K, Enc(K, message))$ to obtain the sensitive medical data.

Secure data aggregation in WBAN using multi-hop communication (Fig. 3.3) can also be performed by the steps shown above. In this case, second and first hop sensors securely communicate with each others using symmetric key cryptography, where session key is used as shared key.

3.7 Performance Analysis

Compared with the symmetric key cryptography, the public key cryptography is more expensive in terms of computation, and has been taken not suitable in sensor's application in the past. However, recent reports showed that the public key techniques with efficient software and hardware design is very viable on low power sensor nodes, and a number of subsequent studies following a public key technique have appeared in recent researches [48] [49]. Moreover, in our proposed scheme, we have only used public-key cryptography for key management in WBAN and rest of the time low cost symmetric key cryptography has used.

We adopt the bilinear parameters $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ described in [50] with $|q| = 160$ bits, $|P| = 512$ bits, such bilinear parameters can achieve the same security level as 1024-bit RSA. We assume that each body sensor node is equipped with a low-power, high

performance Intel PXA27x series processor [51]. Pairing operation is considered the most energy-hungry operation and computational cost is much more higher than other operations needed to implement bi-linear cryptography. It is shown that a single pairing needs about 10 times more time to compute than a scaler multiplication [52]. We denote by C_e a computation of the pairing, and C_m a scalar multiplication in G_1. According to [48] [53], pairing operation needs around 140 ms and energy consumption is 25.5 mJ, whereas energy consumption on the modulus multiplication operation (C_m) is 2 mJ. Time cost of used cryptographic operations is given in table 6.1.

Table 3.1: Time and energy cost for cryptographic operations

Operation	Time	Energy
Encryption1	140 ms (C_e)	25.5 mJ
Decryption1	140 ms (C_e)	25.5 mJ
Signature	15 ms (C_m)	2 mJ
Verification	155 ms ($C_m + C_e$)	27.5 mJ
Encryption2	20 $\mu s/byte$	1.62 μJ
Decryption2	20 $\mu s/byte$	2.49 μJ

We denote data encryption and decryption using public key cryptography as functions $Encrypt_1$ and $Decrypt_1$ and Symmetric key cryptography as $Encrypt_2$ and $Decrypt_2$. Implementation of data encryption and decryption using 128 bits Advanced Encryption Standard (AES), integrated with wireless sensor (CC2420), need 1.62 and 2.49 μJ respectively, whereas a button size 1.5V battery has 15624 J of energy [54].

We consider a WBAN deployed on the body of a person with height 1.7m. The network is composed of n nodes, where $\frac{n}{2}$ nodes are in the first hope distance and the rest are in the second hop distance. Considering network coordinator n_0 is placed at the middle of the body, first-hops sensors $n_{1..3}$ are placed in the 25cm(d_1) distance from the coordinator. Second-hops are in placed 40cm(d_2) from first-hop's sensor. Using a simple radio model in free space [55], we sum-up the following equations to calculate the total energy needed for single-hop and multi-hop communications.

$$E_{sh} = \frac{n}{2} E_{TX}(l, d_1) + \frac{n}{2} E_{TX}(l, d_1 + d_2) + nE_{RX}(l) \tag{3.5}$$

$$E_{sh} = \frac{n}{2} E_{TX}(l, d_2) + nE_{TX}(l, d_1) + nE_{RX}(l) \tag{3.6}$$

Equation 3.5 refer to the total energy needed to transmit l-bits messages using single-hop communication and Equation 3.6 shows the total energy needed for multi-hops com-

munication, where n is the total number of sensors. We use the simple radio model to calculate the energy spend at the receiver and the transmitter [55]. To transmit a l bit message for d distance, the energy spend is

$$E_{TX}(l, d) = lE_{elec} + lE_{mp}d^4 \tag{3.7}$$

where E_{elec} is the energy used by the transmitter electronics and E_{mp} is the amplifier energy. To receive a l bit message the energy spend is

$$E_{RX}(l) = lE_{elec} \tag{3.8}$$

In our simulation, we use the Table 3.1 values and system parameters values as $E_{elec} = 50\mu J$ and $E_{mp} = 0.13\mu J$ [55] to calculate average energy with different number of sensors. As the intermediate sensor nodes need to transmit additional data packets for the second-hops node, they are going to be out of energy earlier compare to others. As shown in Fig 3.5, multi-hops communication consumes less average energy compare to single-hop. We then proposed an optimize solution. In the optimize approach, intermediate nodes integrate second-hop's data to its own data by doing some advance observation. Deployed sensor mostly sensed a specific pattern of data and sensed data can be represented as the difference of previous and current sensed data. Even, sensed data may not be varied in a normal healthy condition. In this case, intermediate relay node only adds few bits with its data packet and thus only add energy consumption for symmetric key encryption and decryption with the single hop equation.

3.8 Security Analysis

In this section, we analyse the security properties of the proposed protocol.

3.8.1 Resilience to Packet Analysis Attack

In the proposed protocol, data aggregation at the WBAN is performed by using session key and the dynamic session time is updateable based on the location. Without knowing the secret session key, the adversary cannot recover the plain text by performing packet analysis. In addition, because the pseudo identity is used instead of original identity, no identity information will be disclosed. Therefor, the proposed protocol for WBAN can resist the packet analysis attack.

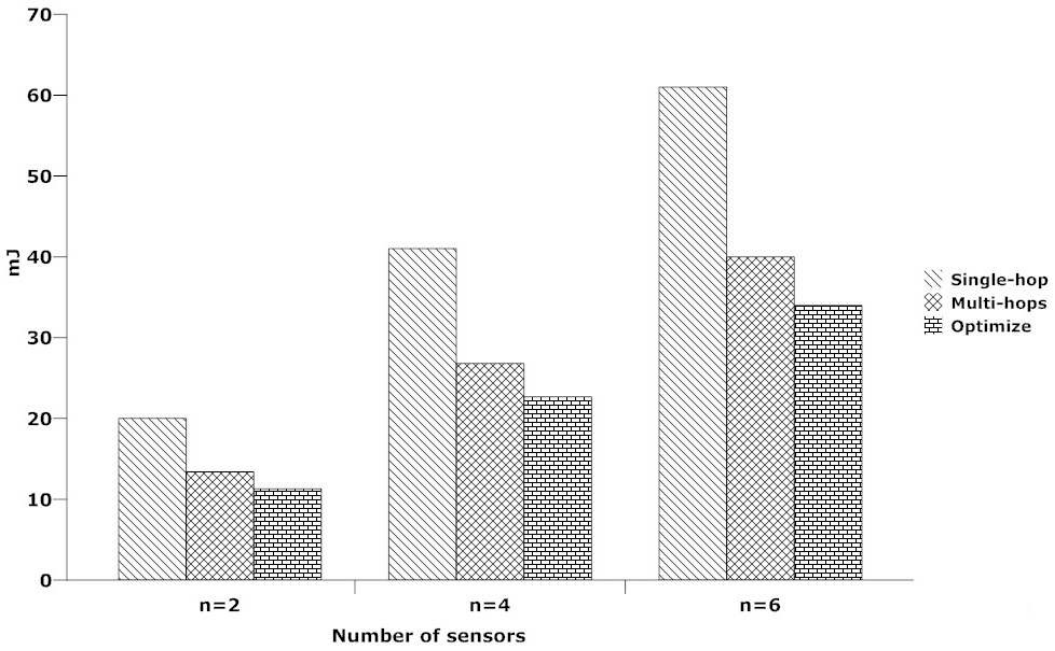

Figure 3.5: Average Energy Per Round

3.8.2 Resilience to Source Authentication Attack

In the initialization phase, trusted authority ensures the proper set of body sensors for a specific user. WBAN's gateway first matches sensor identifications with its pre-loaded sensors set. The secret key is only share among the sensors if and only if the the sensors pass the identification test step. In addition, sensors identity is cryptographically attached with the message signature. Thus the intermediate node or the gateway can easily verify the source authentication.

3.8.3 Resilience to Data Authentication Attacks

A receiver node accepts only data packets that contain valid message signature. Recall that the session key updates frequently and attacker cannot obtain any information about the session period by doing exhaustive packet analyzing. Any false data packet will be rejected directly by the receiver node if attached the signature is invalid.

3.9 Proposed scheduling scheme

In this section, we proposed a scheduling scheme for eHealth care data packets based on different priorities. Usually the network coordinator(PDA) works in a multi-tasking environment to support different applications run by the user (Fig. 3.6).

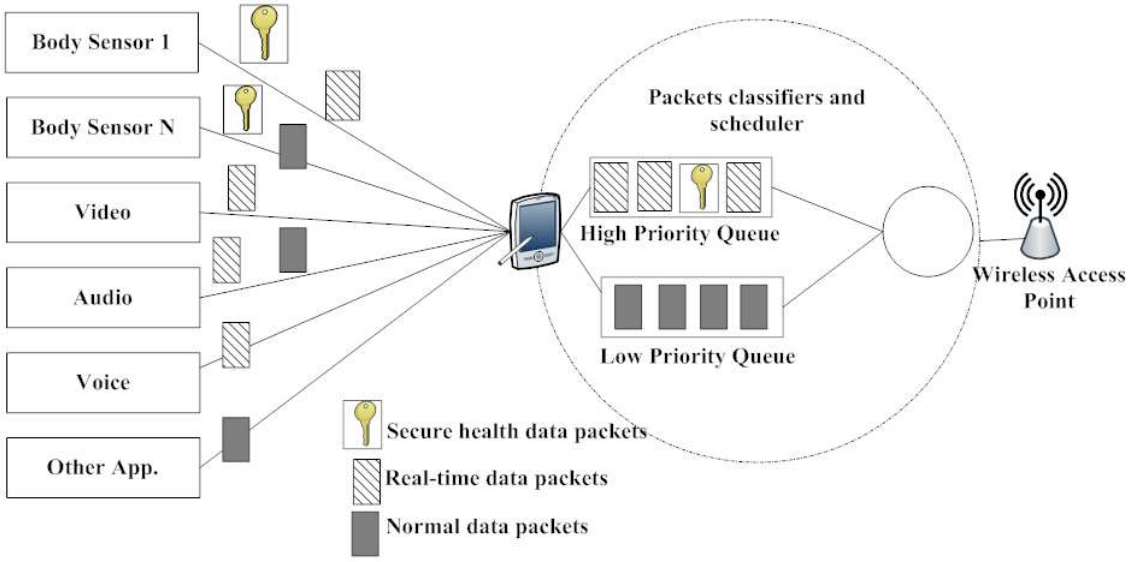

Figure 3.6: Traffic scheduling at PDA

In a conventional queuing packet scheduling scheme, priority is assigned to the real time traffic and other types of traffics are marked as normal traffic. But in a WBAN different types of real-time traffics need to be classified. In our non-preemptive queuing model, the PDA will do the following steps:

- Check if the arrival traffic is real-time or non real-time traffic;
- Check if it is an emergency health application traffic or not;
- Classify the traffic and store them into the high and low priority queues;
- Classify the high-priority traffic based on their QoS requirements;
- Select the packet from the queue for the next servicing based on the priority and QoS requirements. Ensure that running process will finish its task first.

The packets stored in the high priority queue (Q_h) are served at $\alpha\mu$, prior to the non priority class with a service rate of μ. We use the M/G/1 queuing system to model this multiple-queues and single server system. In our analysis, we assume the packets that are related to high-priority queue and low-priority queue (Q_l) are called class-h (C_h) and class-l (C_l) packets with the average length of L_h and L_l, respectively. Both C_h and C_l packets are traveling according to the Poisson process, with arrival rate of λ_h and λ_l, respectively. The service times are generally distributed, and the sensor nodes and PDA are assumed to be stationary.

3.9.1 High-priority queue

The average service time for a C_h packet is $E[S_h] = \frac{1}{\alpha\mu_h} = \frac{L_h}{R}$. Transmission rate and packet length are marked as R and L_h respectively. Different real-time traffic is classified by the weighting factor α. Here, the aim is to calculate the queuing delay for each C_h packet that is defined as the expected waiting time $E[W_h]$. The waiting time of C_h consists of two components: a) remaining service time of a packet in service $E[T_R]$, and b) required time to serve all of the packets with higher and same priorities $E[T_h]$,i.e.,

$$E[W_h] = E[T_R] + E[T_h] \tag{3.9}$$

A packet of C_h is in service with probability $\rho_h = \lambda_h E[S_h]$, which is the utilization of Class-h packets. As the arrival time is randomly selected and the class (either C_h or C_l) that is already being served is unknown, the expected remaining time is

$$E[T_R] = \rho_h \frac{E[S_h^2]}{2E[S_h]} + \rho_l \frac{E[S_l^2]}{2E[S_l]} \tag{3.10}$$

Using the Little's law, the second term of the equation 3.9 can be written as

$$E[T_h] = \frac{\lambda_h E[W_h]}{\alpha\mu_h} = \rho_h E[W_h] \tag{3.11}$$

Substituting the value of $E[T_R]$ and $E[T_h]$ into equation 3.9, $E[W_h]$ can be calculated as follows

$$E[W_h] = \frac{\rho_h \frac{E[S_h^2]}{2E[S_h]} + \rho_l \frac{E[S_l^2]}{2E[S_l]}}{1 - \rho_h} \tag{3.12}$$

The second moment of service requirement of a C_h packet can be expressed as follows:

$$E[S_h^2] = Var[S_h] + (E[S_h])^2 \tag{3.13}$$

In our approach, the PDA has a fixed service time to serve its packets, hence the service time is deterministic with zero variance ($Var[S_h] = 0$). Thus equation 3.13 can be re-written as $E[S_h^2] = (E[S_h])^2 = (\frac{L_h}{R})^2$. Finally from equation 3.12, the mean waiting time of the Q_h can be expressed as

$$E[W_h] = \frac{\rho_h \frac{L_h}{2R_h} + \rho_l \frac{L_h}{2R_h}}{1 - \rho_h} \tag{3.14}$$

3.9.2 Low-Priority queue

The expected waiting time for the low-priority queue (Q_l) is depends on the expected service time seen by an arriving packet of C_l type in Q_h and Q_l. This waiting time can be written as

$$E[W_l] = E[Y_1] + E[Y_2] + E[Y_3] + ... \tag{3.15}$$

Here $E[Y_1]$ is the expected service time seen by the C_l packet at its arriving in Q_h and Q_l and the time needed to finish the service that already in process. Thus, $E[Y_1]$ can be expressed as:

$$E[Y_1] = E[T_R] + E[T] \tag{3.16}$$

$E[T_R]$ is considered as the remaining time of the packet that already in the service and $E[T]$ is the time needed to serve all of the packets of the high priority queue and equal priority. Using the PASTA property, $E[T]$ can be calculated as:

$$E[T] = \frac{E[N_h]}{\alpha\mu_h} + \frac{E[N_l]}{\mu_l} = \rho_h E[W_h] + \rho_l E[W_l] \tag{3.17}$$

Here N_h and N_l are the packets waiting in Q_h and Q_l to be served. From the equation 3.10 and 3.13, we can derive $E[T_R] = \rho_h \frac{L_h}{2R} + \rho_l \frac{L_l}{2R}$. Substituting the values of $E[T_R]$ and $E[T]$ into equation 3.16, we have

$$E[Y_1] = \rho_h \frac{L_h}{2R} + \rho_l \frac{L_l}{2R} + \rho_1 E[W_h] + \rho_l E[W_l] \tag{3.18}$$

Similarly, $E[Y_2]$ is the expected service time associated with higher priority packets during the $E[Y_1]$ is processing, $E[Y_3]$ is the expected service time associated with the higher priority packets during the $E[Y_2]$ is processing, and so on. Hence the expected waiting time can be written as

$$
\begin{aligned}
E[W_l] &= (E[Y_1] + E[S_h]C_h E[Y_1] + E[S_h]C_h E[Y_2] + ...) \\
&= E[Y_1] + \frac{C_h}{\alpha\mu_h}(E[Y_1] + E[Y_2] + ...) \\
&= E[Y_1] + \frac{C_h}{\alpha\mu_h}E[W_l]
\end{aligned}
\tag{3.19}
$$

The term $\frac{C_h}{\alpha\mu_h}E[W_l]$ can be written as $\rho_h E[W_l]$. Substituting the value of $E[Y_1]$ into equation 3.19, we can simplify the mean waiting time of the low-priority queue as:

$$
E[W_l] = \frac{\rho_h \frac{L_h}{2R} + \rho_l \frac{L_l}{2R} + \rho_h E[W_h]}{1 - \rho_h - \rho_l} \tag{3.20}
$$

3.10 Performance Evaluation of Scheduling Approach

In order to evaluate the performance of the scheduling algorithm, we perform the simulation considering L_h=L_l=64 bytes and R_h=R_l=350 kbps.

Fig. 3.7 shows the mean waiting time of the high and low priority traffic having $\lambda_h = \lambda_l = \lambda$. We classifies the real-time traffic based on their service time and security requirements. Delay sensitive and security require traffic (for health care) is classified as case 1 and we assume $\alpha = 1$ for this pattern of traffic. Other real-time traffic such as video or on line gaming traffic are classified as case 2 with $\alpha = 1.5$. Other type of packets are marked as case 3 with $\alpha = 2$. Traffic is either high priority or low priority based on their QoS bindings. It is shown in Figure 3.7 that the short real time traffic needs less waiting time and hence can be improved the overall performance.

We then differ the arrival rates of the high and low priority traffic as case 1 ($\lambda_h = 0.5\lambda_l$), case 2 ($\lambda_h = \lambda_l$), and case 3 ($\lambda_h = 2\lambda_l$). Fig. 3.8 shows the mean waiting time with different packet arrival rates. The mean waiting time of low priority traffic for case 1 increases significantly at $\lambda = 0.8$ (Fig. 3.8). Sub-figure in Fig.3.8 shows that the waiting time rapidly increase to more then 100 ms when we choose $\lambda_h = 3\lambda_l$ for the low priority traffic of case 1 but the high priority traffic of same case has a steady response.

3.11 Summary

In this chapter, we proposed a hybrid secure data aggregation scheme for WBANs. The protocol uses periodic session key as the secret key. User's privacy is maintained by using

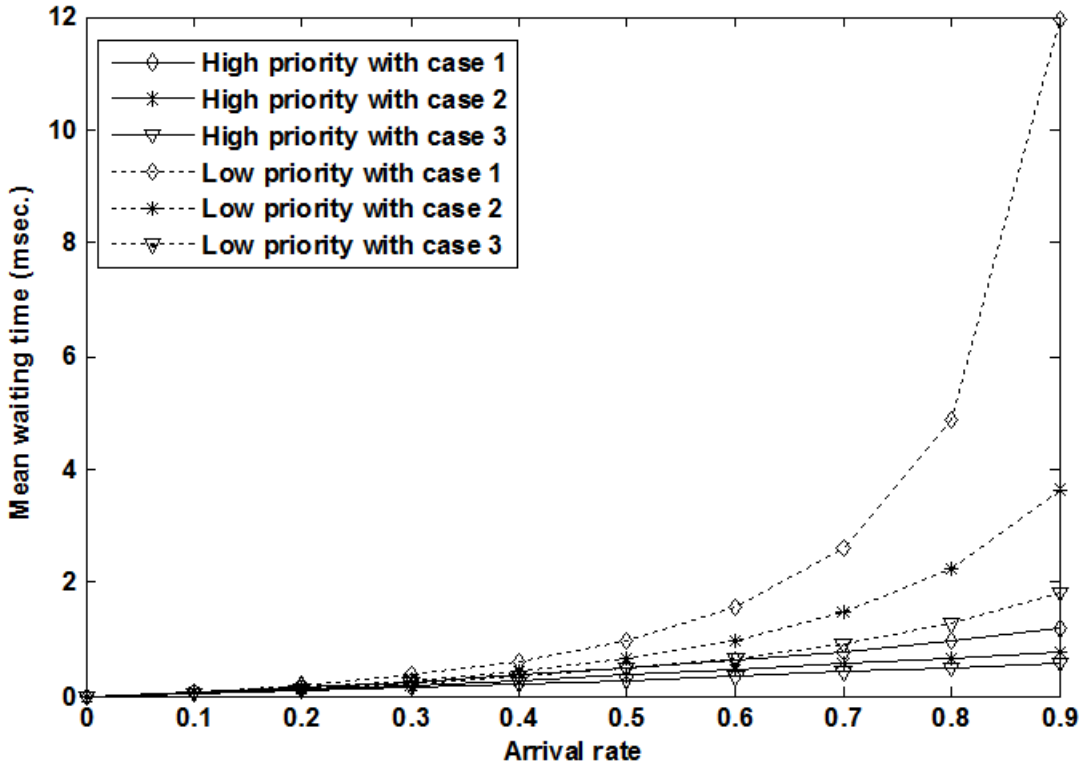

Figure 3.7: Mean waiting time with variable weighting factor

pseudo-identity in all stage of the communication. Our proposed secure communication scheme can minimize the key storage space and need less computation. A priority based traffic scheduling scheme for real-time application in WBAN is proposed and analyzed. Proposed traffic classification scheme ensures the QoS of real-time application by minimizing the mean waiting time. Security analysis and simulation results show that the WBAN's QoS bindings for the eHealth application can be achieved by using our proposed scheme.

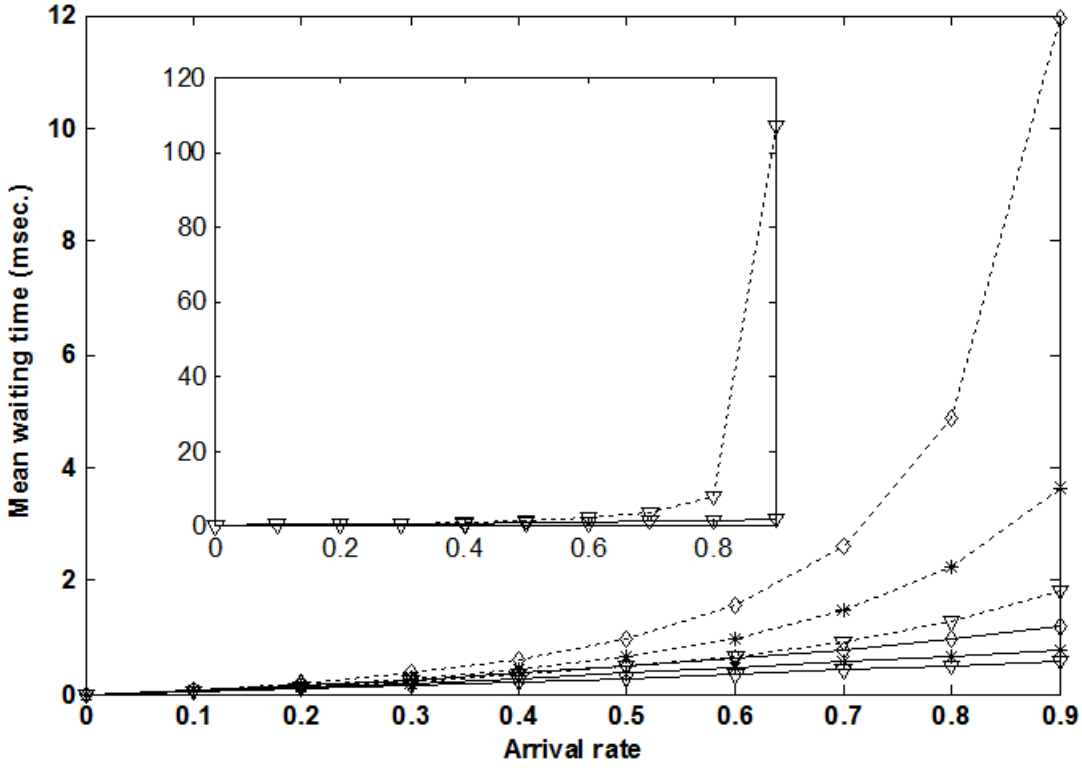

Figure 3.8: Mean waiting time with different arrival rate

Chapter 4

ASTP: Cooperative Trust Aware Data Aggregation in Urban Area

4.1 Introduction

Electronic health care is becoming a vital part of our daily life and exhibits advantages over the paper-based legacy system. The eHealth service provisioning is an increasingly important requirement as the elder population in the industrialized countries is growing rapidly and an urgent solution for minimizing the health services cost is needed. Advances in wireless communications and computing technologies have lent credence in the migration of health care systems from paper based to electronic system. Recent advances in Wireless Body Area Networks (WBANs) have made it possible to deploy bio-sensors on, in, or around the patient body and allow to continuous monitoring of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels etc.) with physical activities. Coexisting and cooperating with other wireless and wired technologies, WBANs permit real-time mobile and permanent monitoring of patients, even during their daily activities. In these cooperative environment, users can form an on-demand adhoc network and use multi-hop routing to enhance network performance, minimize the cost of deployment, increase the coverage area as well as reduce the overall service cost.

In a multi-hop wireless network, participant nodes act as relay nodes to forward neighbor's data packets. However, not every node is cooperative or willing to forward others data traffic. The noncooperative node leads to degradation in the Quality of Service (QoS) of the network by dropping data packets. Moreover, noncooperative node may be a malicious node and fabricates the network routing information, as well as modifies the message that

passes through it. Choosing the cooperative relay node becomes more challenging in an environment where users have the services from different service providers and the application has to support real-time data communication (e.g., eHealth application). In addition, data integrity with authentication, network availability, and user privacy are considered as key requirements for an uninterrupt-secure health monitoring system.

To provide the above mentioned system requirements in a heterogenous wireless environment, this paper presents ASTP using bi-linear pairing. Trust factor used in ASTP is semi-agent-symmetric instead of user-symmetric: If "user A trusts another user B", it does not mean that "user B trusts A" but "user B partially add the trust value of user A that is provided by B's service provider (Agent)". Trust value used in this article to choose the next hop relay node also depends on the node recent activities and its energy level. The implementable security module can be integrated to the gateway of WBANs by simply uploading the proposed security package. The service provider (named as Agent) in this article, will provide the proper incentive to the routing nodes based on their activities and ensure the network availability by minimizing the risk of Denial-of-Service (DoS) attack.

The remainder of the chapter is organized as follows. In Section 2, the related work is briefly discussed. Section 3 presents the security requirements and the system model. The proposed ASTP is introduced in Section 4. The performance analysis of the ASTP is discussed in Section 5. Section 6 analysis the security features followed by conclusion in Section 7.

4.2 Related Work

Recently, trust-based routing has gained much attention as an effective way to choose cooperative relay nodes. Chi et al., [39] identified the unique features of trust metrics compared with QoS-based routing metrics. In that protocol, a systematic analysis of the relationship between trust metrics and trust-based routing protocols is presented. A model for trust evaluation and trust update based on fuzzy logic is described in [40]. This model is first used to analyze the physical requirements and psychology of the malicious attackers and then modifies the corresponding nodes trust value. Cooperation between neighbor nodes are used to find out the trust node in [16, 41]. To provide fairness, an incentive mechanism is integrated with the routing protocol in [16]. The overhead of the communication was reduced by using a cheating detection system. Lu et al., [42] have improved the packet delivery ratio and resisted most possible attacks in a vehicular delay tolerant networks by presenting a social-based privacy preserving packet forwarding protocol. A secure multi-cast strategy is proposed in [43] to allow trustworthy nodes

participate in the communication. Wang et al. [6] present a linear trust evaluation method based on self-observed information of a certain node and other nodes.

Security and Privacy issues in eHealth care systems have been addressed in [43, 45]. Xiaodong et al. [45] proposed a privacy preserving scheme for heath care that can effectively works against global adversary. In [46], an authentication protocol is developed. The protocol uses "Time-stamp" to describe and verify the signature and the freshness of the message. This time variant parameters may be used in authentication protocols to prevent replay and interleaving attacks, and to provide uniqueness of digital certificates with resistibility to certain chosen-text attacks. Decker et al. [47] have proposed a privacy-preserving eHealth protocol based on a credential systems. Entity authentication and item integrity are provided by verifiable public key cryptography.

4.3 Security Requirement and System Model

4.3.1 Security Requirements

We aim at achieving the following security objectives.

- ***Message integrity and source authentication:*** All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated by the recipients. An intermediate node should not be able to substitute a false message for a legitimate one.
- ***Confidentiality:*** Confidentiality protects data from non-authorized users during data communication. The proposed architecture has to prevent disclosure of patient's health information without appropriate authorization.
- ***Prevention of Ciphertext-only attack:*** The system should be secured enough to prevent recover of the plaintext from a set of stored ciphertexts.
- ***Privacy Concerns:*** Privacy is one of the important concern from a patient's perspective. Illegal disclosure and improper use of patient's health records can cause legal disputes and undesirable damaging in patient's personal life.
- ***Non-repudiation:*** Non-repudiation prevents either sender or receiver from denying a transmitted message. As the intermediate routing nodes will get some incentive, message non-repudiation must be ensured.

- ***Secure Routing:*** In a multi-hop communication scenario, secure routing is required for the sensitive patient health information.

4.3.2 System Model

In our system model, we consider that an eHealth user (eU) subscribes health-service from an authorized service provider, identified as Agent (eAg). The Central eHealth Control Authority (CCA) authorizes the Agent (e.g., Hospital, Urgent clinic, Home care unit etc.) to provide secure and reliable health services to the citizen. We classify the In-door communication as users located in the hospital, long term care center, in-home, shopping mall, community center, church/ prayer hall, and need single, or multi hop communication to communicate through network Access Point (AP). On the other side, Out-door scenario includes user mobility around the hospital, malls, parks, or in the public transits where multi-hop communication is chosen most of the time. Between patient and Agent, data packets are routed through different wireless technologies, likely WiFi, WiMax or UMTS. All these network technologies have their own authentication and security mechanisms. But for a real time application (e.g., eHealth), a generalized secure communication architecture is required despite of different network technologies. Taking this into account, the ASTP proposes a unique secure and trust-based packet routing protocol. The proposed protocol aims to solve the issue of secure routing with proper privacy during the communication from user to the corresponding Agent. Secure communication in WBANs is discussed in our previous work [56]. Fig. 6.1 shows the typical eHealth scenarios where data packet is routed on a secure and trusty path (shown in arrowed line).

4.4 The Proposed ASTP Protocol

In this section, we discuss the proposed ASTP protocol in two phases; system initialization with security features is described in first phase and routing establishment based on trust is illustrated in second phase. Notice that 'node' and 'user' are used interchangeably.

4.4.1 System initialization

The security of the proposed system depends on a computational problem related to the Bilinear Diffie-Hellman Problem (BDHP). The pairing implementation and timing analysis is derived in [30, 57].

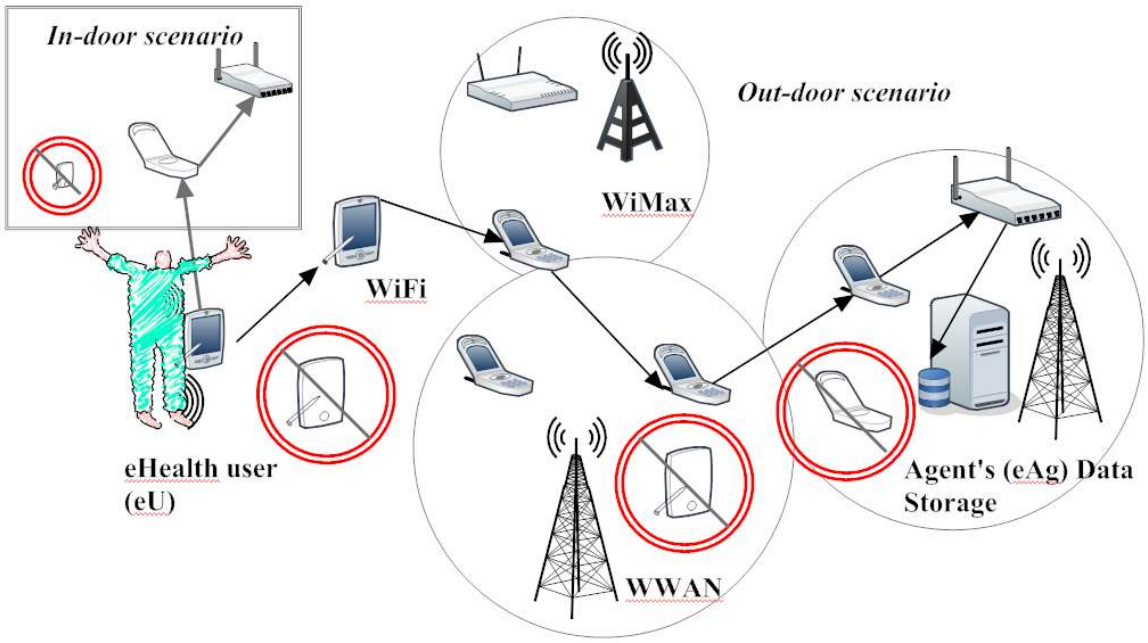

Figure 4.1: System model of the ASTP

System Initialization by CCA

Given the security parameter S, the bilinear parameters (q, G, G_T, e, P) are generated by the function $Gen(S)$. The trusted authority CCA will do the following initializations: selects random numbers $\alpha_1 ... \alpha_n \in_r Z_q^*$ and computes the public key for the Agents $PK_{eAG_{i..n}} = \alpha_1 .... \alpha_n P$ (needed for the communication between CCA and Agent); generates the hash function H_1; securely delivers PK_{eAG} and H_1 to eAG and stores α as a secured key for the corresponding Agent.

System Initialization by Agent (eAG) and User (eU)

The Agent first calculates the public key ($PK_{eAg} = H_1(ID_{eAG})$) by hashing its original identity for message encryption and decryption. It then generates two hash functions, $H_3 : \{0,1\}^* \rightarrow G_1^*$ and $H_4 : G_2 \rightarrow \{0,1\}^*$, and computes the user's pseudo-identity (eU_{PID}), $eU_{PID} = H_2\{eU\_ID\}$; where $H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$. It then distributes eU_{PID}, H_3 and H_4 to its subscribers. On the other side, user eU calculates the public key $PK_{eU} = r \times P$, where $r \in_R Z_q^*$ is a random number. It then selects a random number $\beta \in_R Z_q^*$ to calculate the next session key $P_\beta = \beta \times P$.

Message Encryption and Decryption

In this subsection, we show how an user will encrypt the message 'm' (Eq.4.1) and decrypt the encrypted message by the corresponding agent (Eq. 4.2). The sender encrypts the message, m, using the public key of the corresponding receiver using the identity based encryption [30].

$$v = Enc(PK_{eAG}, m, PK_{eU}) = m \oplus H_4(g_{eU}^r) \tag{4.1}$$

Here $Q_{eU} = H_3(eU\_PID)$; $H_3 : \{0,1\}^* \rightarrow G_1^*$, a random oracle; $g_{eU} = e(Q_{eU}, PK_{eAG})$. and $H_4 : G_2 \rightarrow \{0,1\}^*$, a random oracle. The encrypted message is decrypted using the $Dec(PK_{eU}, v, d)$ function, here $d = \alpha H_3(eU\_PID)$ and α is the secret key of the corresponding agent.

$$Dec(PK_{eU}, v, d) = m \tag{4.2}$$

$Dec(PK_{eU}, v, d) = v \oplus H_4(e(d, PK_{eU}) = v \oplus H_4(e(\alpha$
$H_3(eU\_PID)), rP) = v \oplus H_4(e(H_3(eU\_PID), P)^{r\alpha})$
$= v \oplus H_4(e(H_3(eU_PID), \alpha P)^r) = (m \oplus H_4(g_{eU}^r) \oplus H_4(g_{eU}^r)) = m$

Signature and Verification

ASTP uses cryptographic digital signature ($Eq.(4.3)$), based on the bilinear pairing to provide data integrity. The intermediate routing nodes, as well as the end destination Agent use it and verify that the encrypted message (v) is originated from the specific user and was not altered after signing it. The user first creates session key ($P_\beta = \beta P$) and signed the message as

$$S = Sig(v, P_\beta, T, PK_{U_{PDA}}) = \frac{1}{v + \beta + r + T} P \tag{4.3}$$

Here, T is the routing-token that composed of intermediated routing nodes' hashed value, details illustrate in the 'Routing Establishment Phase'. The agent, and intermediate routing nodes then verify the signature by using the eq. 4.4.

$$e(vP + P_\beta + PK_{U_{PDA}} + TP, S) = e(P, P) \tag{4.4}$$

$e(vP+P_\beta+PK_{U_{PDA}}+TP, S) = e((v+\beta+r+T)P, (v+\beta+r+T)^{-1}P) = e(P,P)^{(v+\beta+r+T)(v+\beta+r+T)^{-1}}$
$= e(P, P)$

4.4.2 Routing Establishment Phase:

ASTP establishes routing path between nodes based on their mutual trust values. The next sub-section describes the proposed trusty neighbor node selection algorithm.

Trusty Neighbor Node Selection

ASTP evaluates neighboring nodes recent activities, trustworthiness to the agent, and Received Signal Strength Indicator (RSSI) to calculate the individual node's trust value. There are different approaches in literature to calculate the trust values, e.g. additive increase and multiplicative decrease, linear trust evaluation, exponential and logarithm based trust analysis [6] [43].

Exponential functions growth rate is proportional to their value. An exponential function $y = a^x\,(a > 1)$ has a slow increase shape when 'x' is not a large number ($x < 1$), and 'y' will increase slowly with the increase of 'x'. This exponential function is suitable for measuring node with significant non-cooperative behavior. On the other hand, logarithm functions, $f(x) = \log_a x$, have a fast increase shape when compared to the exponential functions [43]. This behavior allows us to use logarithm function for cooperative behavior.

Algorithm 1 Routing node selection based on trust value

Require: Source SK,PK,Encrypted message (E_m),Signature, Required trust value(Tr_R)

Broadcast the periodic Routing Request Message (RRM) with Tr_R
while Routing Request (RR) $\neq$ FALSE **do**
  if Neighbor nodes response with their Trust Value(N_{Tv}) **then**
    if $Tr_R < N_{Tv}$ **then**
      Recalculate Tr_R or canceled communication due to lack of trusty neighbors
    else
      $Tr_v \leftarrow \left(1 - \frac{1}{N_{Tv}+1}\right)$
      Calculate the trust factor $\tau = \kappa^{Time} \times (ra + RSSI + AS + Tr_v)$
      if $rt > 0.5$ **then**
        $Tr \leftarrow \Lambda\,(\log_\tau(\tau + 2 \times rt))$
      end if
      if $rt = 0.5$ **then**
        $Tr \leftarrow \Lambda \times \mathrm{rt} \times \tau$
      end if
      if $rt < 0.5$ **then**
        $Tr \leftarrow \Lambda \times (0.5 + rt)^\tau$
      end if
    end if
  end if
  Forward the packet to the RN_1
end while

At the beginning of a communication session, a user first calculates the recent trust ($0 \leq rt \leq 1$) value of its neighbors. Other parameters we have esteemed to calculate the trust factor are recent activities (ra), received signal strength ($0 < RSSI < 1$), residential time (Time), and priority to the same Agent's subscribers ($AS = 1$ for same agent's subscribers, 0.7 for trusted, 0.5 for semi-trusted, and 0 for none). A neighboring node is only allowed to route the packet, when its trust value is greater than the require trust value set by the source node. The pseudo code to choose the next secure and trusted neighbor is given in Algorithm 1. Scaling factors κ and Λ are used to keep the calculated trust value in the range of 0 to 1.

Example: Let node B successfully forwards 10 packets ($ra = 10$) of node A in the past 5 unit of time ($Time = 5$). Scaling factor $\kappa = 0.7$ and $\Lambda = 0.5$. At the beginning of the communication, node B responses with a trust value $N_{Tv} = 0.7$ and rt is set as 0.3. Suppose $RSSI$ and AS have the value of 0.5 each. Calculating the trust factor τ (equation shown in the line no. 8 of Algorithm 1), we have the value of 1.915. Now for $rt = 0.3$, the new trust value Tr will be 0.33. Suppose rt=0.6, Now the new trust value will be $Tr \leftarrow \Lambda\left(\log_{\tau}(\tau + 2 \times rt)\right) = 0.87$.

Routing Steps

The source node first initiates route establishment phase by broadcasting Route Request ($RREQ$) that contains it pseudo-identity (eU_{PID}), required trust value (Tr_R), time stamp, and the corresponding agent identity. Neighbor node replies with acknowledgement having its pseudo-identity and willingness (as trust value N_{Tv}). Source node then chooses the next hop based on the Algorithm1. The process continues until there is a trusty-secure communication link to Agent. At the end of route establishment phase, the Agent calculates the routing token $T = H_2\left(eU_{PID}||eU_{1_{PID}}||....||eU_{n_{PID}}||Time - Stamp\right)$ using all intermediate relay nodes pseudo-identity and time-stamp and replies acknowledgement (ACK) with encrypted 'T' (using Eq. 4.1). The sender then encrypts the message (Eq.4.1) and forwards to the next hop along with message signature (Eq.4.3), public cryptographic information, and session identity. Intermediate routing nodes verify and forward the data packet as shown in *System initialization* section (Eq.4.4). After successful transmission, the agent first checks the time bindings, decrypts the message (Eq.4.2), and ensures proper incentive to the intermediate routing nodes based on their trusted performances. Finally send acknowledgment to the user, shown in Fig. 4.2.

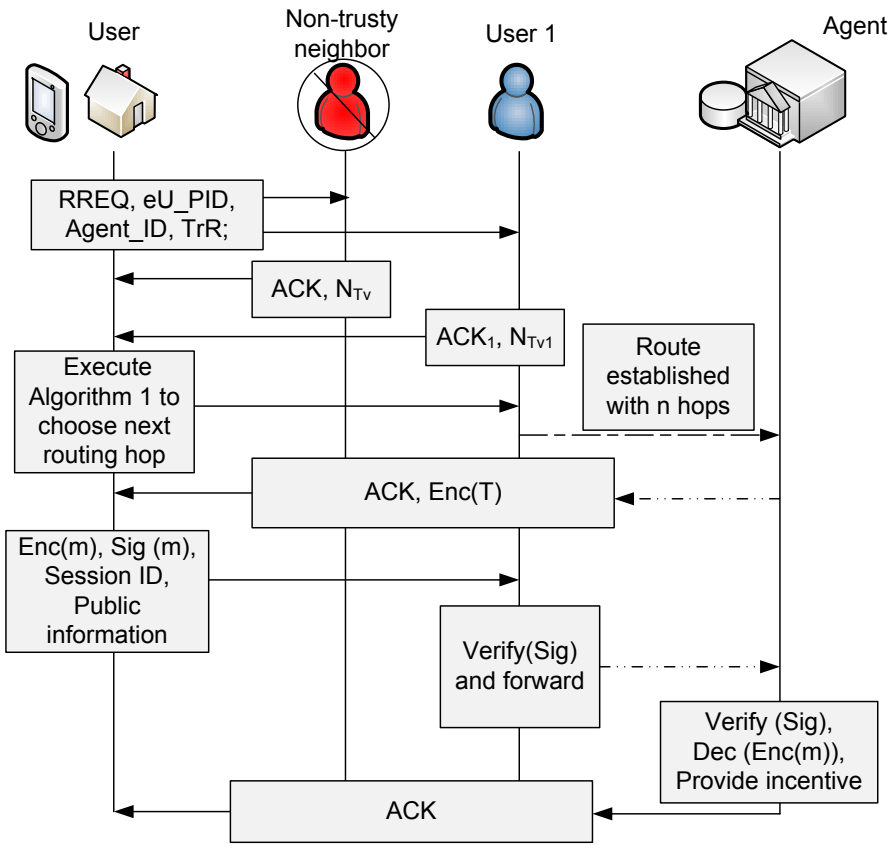

Figure 4.2: Routing steps of the proposed ASTP protocol

4.5 Performance Evaluation

We conduct a probabilistic model to analyze the relation among the number of users (n), intermediate node's successful verification probability (p), and the trust probability (P_{Tr}) which indicates the existence of at least a trusty neighbor node that relays the data packet.

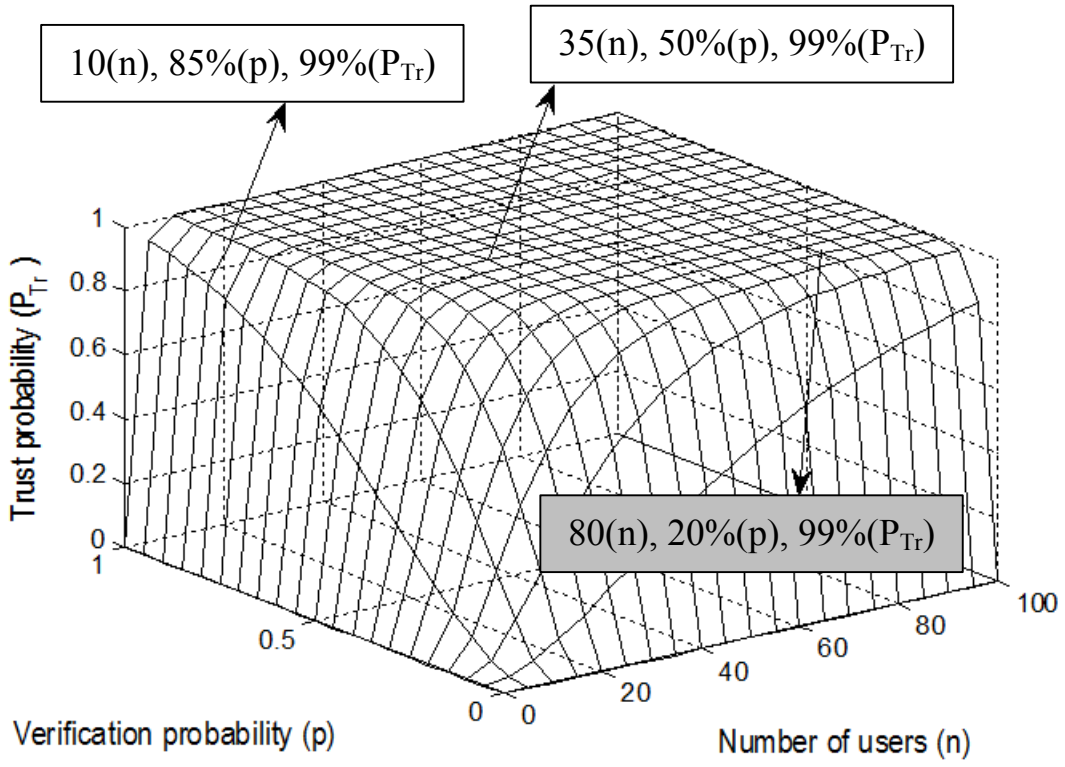

Figure 4.3: Relation among P_{Tr}, p, and n

Let A_i be the event that there are i trusty nodes, and $n-i$ be the number of non-trusty nodes in the communication range of the user U_1, who belongs to the Agent $Agent_1$. Let Tr be the event that there are at least a trusty relay node that will verify the message and relay to the next-hop node. Using the equation of total probability, the relation among Pr{Tr}, n, and p can be represented as: $Pr\{Tr\} = \sum_{i=0}^{n} Pr\{Tr|A_i\}.Pr\{A_i\} = 1+(1-p)^n - 2(1-\frac{p}{2})^n$. Here, $(1-p)^i$ is the probability that none of the i users of the $Agent_1$ will verify the

message sent by U_1, $(1-(1-p)^i)$ is the probability that there is at least one user from the $Agent_1$ will verify the message, and $(1-(1-p)^{n-i})$ is the probability that there will be at least one neighbor user from other agent will verify the message. Hence, $Pr\{A_i\} = \binom{n}{i}(1/2)^i(1-\frac{1}{2})^{n-i}$ and $Pr\{Tr|A_i\} = (1-(1-p)^i)(1-(1-p)^{n-i})$; each user position is independent and follows binomial distribution. Fig.5.3 shows the relation among P_{Tr}, p, and n. It can be seen that P_{Tr} increases as either p or n increases. Fixing the probability to have at least one trusty relay node P_{Tr} to 99%, we have to ensure either large number of users or higher verification probability.

We also conduct simulation using NS 2.33 considering a) In-door, and b) Out-door scenarios. In our simulation, we modify the existing Adhoc On-Demand Distance Vector (AODV) routing protocol to implement the ASTP and compare the results with the existing AODV protocol. $50ms$ is considered as the computation time for the pairing on a super-singular curve proposed in [57]. In our simulation, we randomly deploy nodes in square areas of $350m \times 350m$ and $850m \times 850m$ for in-door and out-door scenarios, respectively. Taking communication interference into consideration, we choose transmission range of each in-door node as $70m$. Nodes deploy in the out-door will probably maintain more Line-of-Sight communication and we select $200m$ as the communication range for the outdoor's node (shown in TABLE 4.1). Other parameters are selected as the example shown in the 'Trusty Neighbor Node Selection' subsection.

Table 4.1: Simulation Parameters

	In-door	Out-door
Area	$350m \times 350m$	$850m \times 850m$
Number of Nodes	20	30&40
Communication range	70m	200m
Simulation time	5h	5h
Mobility	20% nodes at $2Km/hr$	70% node at $2-50Km/hr$
Packet type	CBR	CBR
Packet size	512 bytes	512 bytes

As our main focus is to improve packet deliver rate over an insecure wireless environment, we mainly estimate the performance based on the average packet delivery ratio and corresponding delivery delay.

Figures 4.4 shows the average packet delivery ratio for the in-door (ID) and out-door (OD) scenarios. Here 'LTP' means low trusty nodes detected prior to the communication

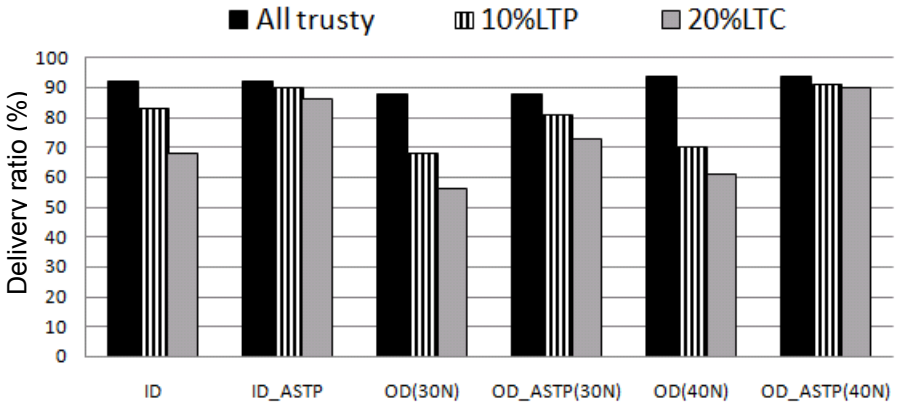

Figure 4.4: Average Packet Delivery Ratio

(choose $rt < 0.5$), 'LTC' means node becomes low trusty any time during the communication, simulation results using AODV are labeled as 'ID' or 'OD', and 'ID_ASTP or OD_ASTP' is used to label the ASTP protocol. We choose 20 nodes for the in-door scenario and for the out-door scenario 30 and 40 nodes. Choosing trusted relay nodes with

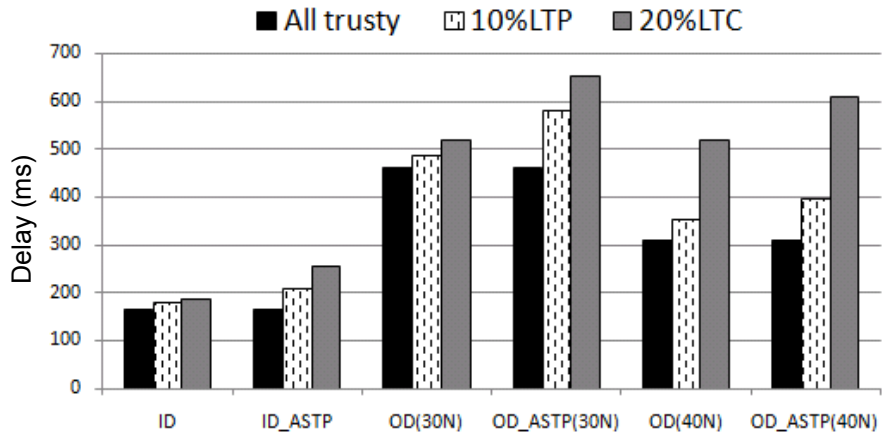

Figure 4.5: Average Packet Delivery Delay (in ms)

proper incentive strategy improves the packet delivery ratios because cooperative relay nodes always try to forward data packets in absence of system failure. Around 26% improvement on the packet delivery ratio is achieved using the proposed ASTP for the indoor scenario. It becomes 63% when we consider out-door scenario with 20% LTC.

Fig. 4.5 shows the average packet delivery delay using AODV and ASTP. Due to computation overhead, average packet delivery delay using the ASTP protocol is larger than the existing AODV protocol. However, simulation results show that increase the number of nodes significantly decreases the average packet delivery delay (around 200 ms for $10\%LTP$) in the out-door scenario because it increases the probability to have more trusted cooperative nodes as neighbors and establishes trusted routing path between source and destination. Analyzing simulation results demonstrate that ASTP increases the average packet delivery ratio significantly at the cost of a reasonable packet delivery delay.

4.6 Security Analysis

The proposed ASTP utilizes users' pseudo identities instead of users' original identities, and these pseudo identities are generated by a strong one-way hash function (H_2). The construction of the hash function is easy to sample and compute but hard to invert. Therefore, the user-privacy is ensured by the ASTP. As the trusty Agent knows the original-identity related to the pseudo-identity, it can always retrieve the real identities of the user and ensure system traceability. The end-to-end data transmission uses proper encryption schemes based on the bilinear pairing. The protocol is secure to chosen ciphertext-only attack due to the hardness of the Bilinear Diffie-Hellman (BDH) problem [30]. It is proven that that there is no probabilistic polynomial time algorithm that can decrypt the message from a set of chosen ciphertext. ASTP ensures message confidentiality by transmitting the message in the encrypted form. Since ASTP uses an efficient digital signature scheme, only the authorized users have the privilege to access the network and proper authentication with message integrity is preserved. A time-stamp is embedded into the routing token (T), it prevents the reply attack. ASTP chooses only the trusty nodes as relay nodes and the Agent assists to ensure secure routing by always monitoring users activities and upgrading the trust values. In the route setup phase, the corresponding Agent sends a signed acknowledgement (ACK) packet, so that the sender can identifies the genuine routing path. It prevent the malicious users to create a black-hole attack by creating a forged route table. An attacker can form a wormhole attack by reeving a packet at one location and tunnels them to another location in the network, and from there the packet are resent into the network. The short session life-time that ensures by the time-stamp, and encrypted routing token use in the ASTP scheme prevents this attack by verification failure and making the packet invalid after a certain time. The relay nodes will feel encourage to forward the data packet because of the incentive provided by the Agent for the cooperative behavior. It will also minimize the probability of denial-of-service (DoS) attack and enhance the system

performance.

4.7 Summary

In this chapter, we have proposed a secure packet forwarding protocol based on mutual trust, that integrates with trustworthiness to Agent, energy level, residential time, and priority to the same Agent's subscriber in a cooperative heterogeneous network. The ASTP protocol can remarkably increase the average packet delivery ratio and achieve excellent efficiency to be used in an eHealth application. Power efficiency at the user level is maintained by computing major calculation at the Agent side. User privacy, an essential part of the eHealth application, is ensured using pseudo identity. Fairness is achieved by providing incentive to the cooperative intermediate routing nodes. Through detailed security analyses, it has been demonstrated that the ASTP is highly effective to resist various possible attacks and malicious behavior.

Chapter 5

RuralCare: Incentive Based Secure Data Aggregation in Rural Area

5.1 Introduction

According to the U.S. Census Bureau, the world's 65-and-older population is projected to triple by 2050; it was 516 million in 2009, projected to be 761 million in 2025, and 1.53 billion in 2050 [21]. This aging population mostly suffers from chronic illness, such as heart diseases, stroke, cancer, diabetes, hypertension, and makes the task of rural health care more challenging. These chronic diseases require long-term monitoring, accurate disease-management, lifestyle changes, and medication screening. Various statistics reports indicate that 133 million people or almost half of all Americans live with a chronic condition. That number is projected to increase by more than one percent per year by 2030, resulting in an estimated chronically ill population of 171 millions [1].

Part of this elderly population or chronic patients living in urban area typically receive better health care comparing to that of rural area due to the lack of care givers and infrastructures. It is true that recent growth of urbanization has people moving from rural to urban areas, but half of the world population still lives in the rural area. Specifically, in USA and Canada, around 20% of the total population lives in rural area, 56% of the population in the 27 Member States of the European Union (EU) lives in rural areas, and 60% in China [21]. Moreover, some large metropolitan areas contain small towns and these small towns are isolated from the central cluster. Providing long-term health care to these areas is also challenging.

Chronic patients live in the rural areas need to be monitored by health professionals regularly and need to be in touched with the care-givers to have an acceptable health status. Providing health care at rural areas faces many barriers, such as lacking of communication infrastructure, travel costs, lacking of health knowledge and care givers and all these prevent deprived residence from seeking acceptable health care with ease and flexibility. Recent advances in Wireless Body Area Networks (WBANs) have made it possible to deploy bio-sensors on, in, or around the patient lives at the rural area and allow to provide long-term monitoring of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical activities. However, technological solution is needed to transfer these aggregated sensed data from the patient residence to the care giver's end.

Delay Tolerant Networks (DTNs) is an emerging network paradigm, which is considered as a potential low-cost solution to the problem of connecting devices in an rural area where end-to-end network connectivity is not available. In DTNs, intermittent nodes use opportunistic connectivity (e.g., a new node moves in communication range or an existing one wakes up) to provide data communication. In this paper, we address the problem of transferring sensed data from patient end to care-giver's end by integrating WBANs with Vehicular Adhoc Networks (VNETS). Authorized Vehicles equipped with On Board Units (OBUs) cooperate as relay nodes and could be used to provide network access for long-term health care application in the rural area. However, selfish nodes in DTNs do not relay other data packets but use honest nodes to relay their own packets. It degrades the network performance, and effects network fairness, as well as security. One of the promising ways to address this issue and stimulate cooperation among selfish nodes in DTNs is the incentive scheme [58]. Although the proposed scheme does not provide the solution of emergency care at the rural area but continuous monitoring with acceptable delay is helpful to set up a proactive health care system where patient life can be saved by some precaution.

In this work, we propose an incentive based delay tolerant long-term health care scheme, RuralCare, which is capable of monitoring patient's health status in a rural area. It uses WBAN, WiFi, and VANETs technologies to provide secure and fair data communication with provision of incentive and good reputation to the cooperative relay nodes. Due to the disconnected nature of DTNs, traditional security schemes are not applicable to RCare. To address this problem, our solution exploits Identity Based Cryptography (IBC) [30] by using aggregate digital signature that ensures proper incentive to all cooperative nodes, as well as ensure data integrity.

The remainder of this chapter is organized as follows. A brief description of related works is described in Section 2 .Section 3 contains system model and design goals with different security and privacy requirements. The proposed RuralCare scheme is introduced in Section 4. Section 5 analyzes the different security and privacy features followed by

performance evaluation in Section 6. Finally, Section 7 draws our conclusions.

5.2 Related Works

Remote patient monitoring provides additional benefits to both patients and medical personnel. The design principle and authentication processes of a remote health care system are described in [46]. Remote health care architecture with patient-centric access control is proposed in [59]. A heterogeneous wireless access-based remote patient monitoring system is presented in [60]. Lin et al. [61] proposed a privacy preserving scheme for health care that can effectively works against global adversary. Masi et al. [62], propose a feasible and effective communication protocol for exchanging patient healthcare information among disconnected clinics and hospitals. By using Telehealth Doorenbos et al. [63] enhance access to professional health education for rural healthcare providers. It can inform and educate rural health-care providers about changes in medicine and evidence-based practices, both os which may help them provide quality care. Secure data communication in a WBAN is discussed in [56], where public and symmetric key cryptography techniques are used for secure key management and data encryption, respectively. Prediction based secure and reliable data forwarding in WBAN is introduced in [64]. This work's major contribution is to resist data injection attack during data communication in a WBAN.

Recently, several related works on incentive mechanisms for different kinds of networks appeared in [16], [58], [65], [66] and [67]. In [16], Mahmoud et al., propose a light-weight secure cooperative incentive protocol that uses combination of public-key and hashing operations. They use Merkel hash tree to bundle the packets. In [67], a practical incentive protocol for DTNs is proposed. Here, source node attaches some incentive with a group of messages. With the fair incentive, the selfish DTNs nodes could be stimulated and it increases packet delivery ratio. In our work, we modified this incentive policy and provide security and privacy with network fairness. A simple, robust and practical incentive mechanism for DTNs is proposed in [68] using pair-wise-tit-for-tat. Extensive simulation results are given to show that the incentive mechanism can increase total delivered traffic in the whole DTNs network.

Lu et al. in [58] define the fairness principle for a reputation based ad hoc network. For the Vehicular Ad Hoc Networks (VANETs), an event-based reputation model is proposed in [65] to filter bogus warning messages. Based on the location of the vehicles, the model classifies incoming traffic into different roles. Event reputation value is calculated in considering the different roles. Considering the global security, individual privacy, and easy deployment in an VANETs environment, Lei et al. present as aggregate privacy-preserving

authentication protocol (APPA) in [69]. Their work aggregates multi-signatures into a single verifiable signature. Individual privacy is ensured by using public pseudo-identity that can be only traced by trusted authority.

5.3 Models and Design Goals

In this section, we formalize the system model and identify the design goal.

5.3.1 System Model

In our model, we consider patients or users are located in a rural area where network infrastructure is not available and they need long-term monitoring due to chorionic diseases. The model is also applicable at the urban area to minimize the overall service cost, where users are located at their own residence, old-home or care center. Fig.5.1 illustrates the architecture of the system model, which consists of four interactive components:

- Trust Authority (TA): It generates the public security parameters for RuralCare scheme. TA is fully trusted by the all participants in the proposed scheme and in-charge of the users and vehicles registration. It is also connected to the RSU backbone network. TA is responsible for providing proper incentive or reputation to the cooperative users or vehicles. Authorized health service providers (e.g., Hospital, urgent care) may work as TA. TA is assumed powered with sufficient computing and storage capabilities and infeasible for any adversary to compromise.

- Patients: They are the registered users and equipped with bio-sensors on, in, or around their bodies. Sensors deploy in a body form a Wireless Body Area Networks (WBANs), where PDA, or efficient-sensor works as a gateway. Patient is responsible to share a secret key among the body sensors.

- Road-Side Units (RSUs): RSUs are fixed units that can be deployed at road intersections or any area of interest (e.g., bus stations, parking lot entrances, shopping center etc.). A typical RSU also functions as a wireless access point which provides wireless access to users within its coverage. RSUs are interconnected (e.g., by a dedicated network or through the Internet via cheap ADSL connections) and form a RSU backbone network. RSUs are operated and maintained by the TA and considered as trustworthy by the network's users. Received data packets at RSUs are securely

forwarded to the corresponding health-care provider by using different mature Internet security protocols (such as, IPSec). So it is sufficient to transmit the data packet from rural area to any of the RSUs. In addition, RSUs also perform message authentication and certificate validation. In this article RSUs are distributed in the city area where network infrastructure is already exist.

- On-Board Units (OBUs): OBUs are installed on vehicles. A typical OBU can equip with a GPS module and a short-range wireless communication module (e.g., DSRC IEEE 802.11p [20]). Vehicles with OBUs also have sufficient processing capability and data storage. It can communicate with an RSU or other vehicles in vicinity via wireless connections. For simplicity, we refer to a vehicle as a vehicle equipped with an OBU in the rest of this paper. A vehicle can be malicious if it is an attacker or compromised by an attacker.

- Rural Access Point (RAP): In a rural area RAP is placed at social spots, such as major road intersection, gas station, shopping store etc. It can temporarily store the patient's medical data and using short-range wireless communication forward it to be relayed.

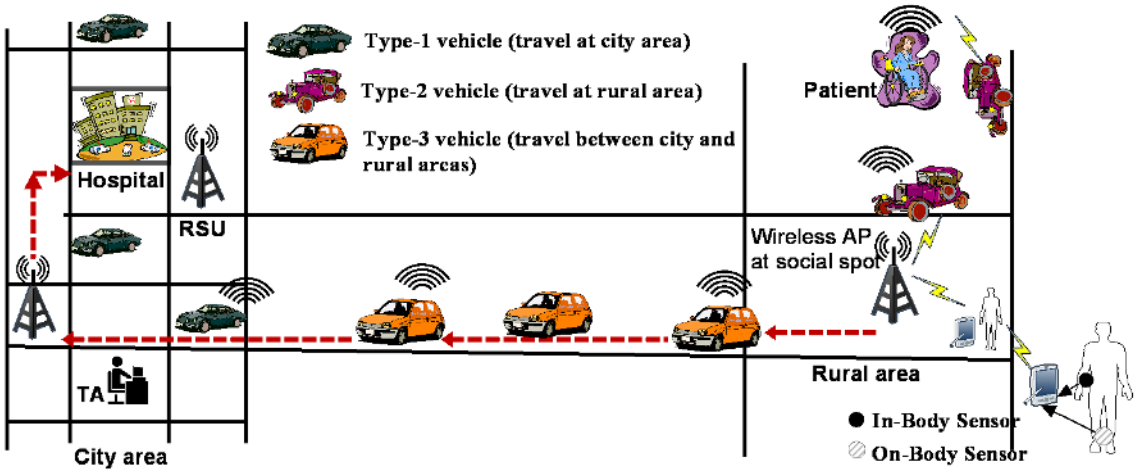

Figure 5.1: System model of proposed RuralCare scheme

In this paper, we divide the whole network into three phases; Phase-1) data communication in a WBAN; phase-2) data communication between users and corresponding Rural Access Point (RAP); and phase-3) communication among RAP, On Board Units (OBUs), and

Road Side Units (RSUs), or destination. Vehicles are categorized into three types: a) vehicles in the city (Type-1); b) vehicles in the rural area (Type-2); and c) vehicles traveling between city and rural area (Type-3). Based on the different types, mobility and location of vehicles are independent. Cooperative vehicles choose shortest path to route from one place to another.

Wireless transmission network

We adopt Bluetooth technology in our proposed RuralCare scheme as the communication standard in the WBAN environment. Different body sensors, such as accelerometer, blood pressure and oxygen saturation (SpO_2) and temperature sensors, frequently send the sensory data to the PDA using this short range, low power communication protocol. Globally used WiFi technology is used to carry the data packet at the RAP using opportunistic data forwarding. Wireless access in vehicular environment can also assist in transferring these data packets to the RAP end. However, communication between RAP and RSU is only performed by VANETs using WiFi standard (IEEE 802.11 [70]). Dashed line in the Fig.5.1 shows the network connectivity in the proposed RuralCare scheme.

5.3.2 Design Goals

Our design goal is to develop a delay-tolerant long-term patient health monitoring system, where the network performance is enhanced by providing proper incentive to the cooperative relay nodes, as well as data security and patient privacy is preserved. In our privacy model, we consider how to protect a user identity privacy, where the adversary has a complete view to eavesdrop all forwarding packets but RAP and RSUs are not compromisable. RuralCare aims at achieving message integrity and source authentication, so that patient's sensitive PHI can deliver unaltered.

Security and Privacy requirements

We aim at achieving the following security objectives.

1. *Message integrity and source authentication:* All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated by the health-care service provider.

2. *Prevention of Packet analysis attack:* Intermediate relay nodes have sufficient time to analyze the data packet. The scheme should provide proper encryption protocol so that eavesdropper can not be able to trace-out any valid, sensitive information about patient.

3. *Prevention of Ciphertext-only attack:* The scheme should be secured enough to prevent recover of the plaintext from a set of stored ciphertexts.

4. *Provide patient privacy:* Privacy is one of the important concerns from a patient perspective. Illegal disclosure and improper use of patient's PHI can cause legal disputes and undesirable damaging in patient's personal life. In all levels of the communication, the scheme must provide patient identity privacy.

5. *Resistant to intermediate nodes adding or dropping:* Due to gain more incentive or reward, some selfish nodes may modify or add false relay information by colluding group of users. The scheme should be able to detect this type of attack.

6. *Non-repudiation:* Non-repudiation prevents either sender or receiver from denying a transmitted message. To ensure the non-repudiation, the patient can not refute the validity of a PHI afterward. As the intermediate routing nodes will get some incentive, message non-repudiation must be ensured by the proposed scheme.

7. *Secure Routing:* In a multi-hop communication scenario, secure routing is required for the sensitive patient health information. Due to the heterogenous wireless environment, the scheme should provide secure and efficient routing of the sensitive data packets.

Incentive Strategy

Performance of any delay-tolerant network usually depends on the cooperation of network's participants. In our proposed scheme, users and vehicles are awarded based on their participation in the network. To ensure the fairness of the incentive protocol, the intermediate forwarding nodes (either users or vehicles) can receive credit if and only if the destination node receives the data packet (Case 1). Even though the packet is not delivered to the destination, the relaying nodes still get good reputation values for their cooperation (Case 2). Reputation function takes holding-time as a parameter and encourages to forward data-packet earlier to maintain higher reputation value. To ensure more participation from the network's users, the TA defines reputation-threshold so that users crossing the threshold

value will get some incentive as a bonus (Case 3). Processes of reward calculation is shown in Equ. 5.1.

$$Reward_i = \begin{cases} Dist_i.C_{IP} + Dist_i.R_{IP}, & \text{Case 1} \\ Dist_i.R_{IP}, & \text{Case 2} \\ Incentive_{Bonus}, & \text{Case 3.} \end{cases} \tag{5.1}$$

User can get a reward $Dist_i.C_{IP} + Dist_i.R_{IP}$ if the data packet P arrives at the destination. Here, $Dist$ is the distance that traveled by user/vechile, C_{IP} is unit incentive credit provided by the data packet's source, and R_{IP} is the fixed unit reputation provided by the trusted RAP/TA. Reputation value R_{IP} at any time T_n is formulated as
$R_{IP(n)} = e^{-\lambda T_i}.R_{IP(n-1)} + CPR_i$,
where packet holding time $T_i = T_n - T_{n-1}$. Reputation value decreasing rate is λ, and CPR_i is the cumulative participant ratio calculated by RAP/TA as $PF_j.\sum_{T=n'}^{T=n} \frac{1}{TPF_{T_j}}$. It is the ratio of the packet forwards (PF) by an individual user and total number of PF by all users at any time period $T_j = T_n - T_{n'}$. Reputation value decreasing rate,λ, can be dynamically readjusted based on network density, data type, device energy level etc.

5.4 The Proposed RuralCare Scheme

In this section, we present the proposed RuralCare, including system setting, data formation, secure patient health information transmission in different phases, incentive and reputation granting, and PHI receiving at care-giver's end. Patient's identity and location privacy, as well as secure transmission of sensitive PHI are considered to design our proposed scheme. We adopted bilinear pairing as a cryptographic technique to design the secure protocol and the basic review is described in chapter 2.

Before delving into the details of the proposed scheme, we first review the bilinear pairing which is used as a cryptographic technique and serves the basis of the proposed RuralCare scheme.

5.4.1 Notations and complexity assumptions:

Notations

If x,y are two strings, then $x||y$ is the concatenation of x and y. If S is a finite set, $s \in_R S$ denotes sampling an element s uniformly at random from S. $\{0,1\}^*$ denotes bit-string of variable length and that converts to a defined group element by the notation $\{0,1\}^* \rightarrow \mathbb{G}$.

Definition 1: Bilinear Parameters Generator ($\mathcal{G}en$): A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and output 5 tuple $(q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, g)$ as the bilinear parameters, where q is a prime number with $|q| = k$. $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are two cyclic groups of the same order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ is a non-degenerated and efficiently computable bilinear map.

Definition 2: Computational Diffie-Hellman (CDH) problem: The security of the proposed system depends on the hardness of computational Diffie-Hellman (CDH) problem, i.e., given $< g, g^a, g^b >$ for $g \in \mathbb{G}$ and unknown $a, b \in \mathbb{Z}_q^*$, there is no algorithm running in expected polynomial time, which can compute g^{ab} with non-negligible probability.

5.4.2 The RuralCare Scheme

In this subsection, we present our proposed scheme RuralCare, which is designed with major four parts, namely a) system initialization and registration; b) secure data communication in a WBAN environment; c) data communication between PDA and RAP; and d) transfer data packet to RSU using OBUs. Patient, also refer as user in RuralCare, uses WBAN that allows to continuous monitoring of physiological parameters (e.g., electrocardiogram (ECG), Electroencephalography(EEG), pulse rate, blood flow and oxygen levels, pressure, and temperature) with physical activities. The WBAN's gateway (e.g., PDA, SmartPhone) then forwards the sensed data to the RAP directly or uses relay nodes (other users/ vehicles) depends on the communication coverage. The forwarded data packet is then temporally stored in RAP and wait until there is an opportunity to forward the packet to RSUs at designated area using VANETs.

System Initialization

Let all users and the TA of RuralCare scheme's use the same security parameters (S) and public bilinear parameters $(q, g, e, \mathbb{G}, \mathbb{G}_{\mathbb{T}})$ that generated by the function $\mathcal{G}en(S)$. The proposed scheme then generates cryptographic hash functions $H : \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G} \rightarrow \{0,1\}^l$, where l is any predefined bit string length. The scheme then initializes $ENC()$ and $DEC()$ as public key cryptographic encryption and decryption protocols to be used in WBAN and $\mathcal{E}nc()$ and $\mathcal{D}ec()$ as symmetric encryption and decryption protocols, i.e., AES, or DES, to be used in phase-2 and phase-3 of data communication. TA picks up a random number $s \in \mathbb{Z}_q^*$ as a secret key, and computes the corresponding public key $P_{TA} = g^s$. Finally, TA publishes the public system parameters $(q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, g, P_{TA}, H)$. Both patients

and cooperative vehicles that relay data packets are considered as registered users of the proposed scheme.

TA in RuralCare defines acceptable holding time (HT) for city and rural areas at the initialization phase. This is the maximum acceptable time an authorized cooperative relay node can store data packet before forwarding to the next available relay hope. TA chooses this time based on the number of users, incentive rate, and distance between rural area and urgency of sensed-data.

Registration Processes

Individual user, vehicle, and body-sensor need to be registered to the system before being a part of the scheme. Registration processes have the following steps:

Step 1: Each RuralCare's registered user has a unique identity $U_i \in U$, $U = \{U_0...U_n\}$ is the set of users, and $V_i \in V$, $V = \{V_0...V_n\}$ is the set of registered vehicles. TA checks the individual identity and computes the pseudo-identity
$PID_{U_i} = H(sU_i)$ and $PID_{V_i} = H(sV_i)$ for the user and vehicle respectively. TA stores users identities and their corresponding pseudo-identities locally. Users' add their corresponding pseudo-identities (PID) in the data packets and their identity privacy is guarantee as others can not be able to know the real identities.

Step 2: TA chooses appropriate medical body sensors based on patient's requirement. It then generates a serial number (SN) for the sensor using the patient's identity and sensor's manufacture defined unique Media Access Control (MAC) address, $SN = H(U_i||MAC_{sensor})$. Generated sensor's serial number (SN) then stores in the registered user's PDA that will be used as gateway in WBAN environment.

Step 3: RuralCare's registered user chooses a random number $x_i \in_R \mathbb{Z}_q^*$ as its private key. The user then computes the corresponding public key as $PK_{U_i} = g^{x_i}$.

Step 4: TA/RAP creates personal reputation account (PRA) and personal credit account (PCA) for each registered user.

Secure Communication Processes

Here, we describe different communication phases. We first describe the secure communication processes between body-sensor and PDA. Thereafter, we present steps for communication between PDA and RAP, and RAP and RSU. We use 'node' in $phase-2$ and $phase-3$ to refer user and vehicle, respectively.

Phase-1: Communication between body-sensors and gateway (PDA)
Secure communication between body-sensors and PDA is described in Chapter 3. The secure communication is ensured by following a hybrid encryption policy. We use public-key cryptography to securely shared a secret key among the sensors, after that symmetric-key cryptography is used to encrypt the data.

Phase-2: Communication between Users and RAP
After receiving the data packet at the PDA using phase-1, the user needs to transmit the sensed data to the local wireless access point, RAP. Steps toward secure data communication between the user and RAP using cooperative vehicles or other users (equipped with mobile wireless devices) as relay nodes are described as below:

Step 1: User U_0 with private-public key pair $(x_0, PK_{U_0} = g^{x_0})$ computes first the shared key $K_{ud} = PK_d^{u_0} = g^{x_0 x_d}$, where $(x_d, PK_d = g^{x_d})$ is the private-public key pair of the destination RAP. User 'U_0' equipped with body sensors, aggregates the sensed data ('m') and encrypts as $E = \mathcal{E}nc_{k_{sd}}(m)$.

Step 2: Determine a proper incentive policy (IP). Based on the significance of the sensed data, user chooses a packet-valid-time (PVT) and generates the data packet $M_u = PID_{U_i}||L_{U_0}||D||IP||Session_{ID}||Packet_{ID}||PVT||TS$.
Here, L_{U_0} is the location information, D is the corresponding access point/destination identity, and TS is the time-stamp that indicates packet generating time.

Step 3: User then generates verifiable encrypted signatures Sig_s and Sig_0 as shown in equations 6.3 and 5.3. Later on, Sig_0 is replaced by the aggregated signature Sig_{agg} that generates by multiplying secure key of the intermediate nodes.

$$Sig_s = PK_d^{H(M_u||E)+u_0)} \tag{5.2}$$

$$Sig_0 = u_0 H(E||L_{U_0}||TS) \tag{5.3}$$

Step 4: Intermediate relay node, U_1, first checks the IP and take the routing decision based on the proposed incentive policy. If U_1 feels interested in routing the data packet, it then verifies the validity of Sig_0 with the equation $e(Sig_0, g)$
$\stackrel{?}{=} e(PK_{U_0}, H(E||L_{U_0}||TS))$ and calculates the difference between current time and received packet's TS. If the difference is less than PVT, U_1 sends acknowledgement (ACK) to the sender U_0.

Step 5: Let $U_0 \rightarrow U_1 ... U_i \rightarrow U_d$ be the current packet forwarding path. In each routing step, intermediate node calculates short signature, $Sig_j = u_j.H(PID_{U_j}||L_{U_j}||TS)$ and computes aggregate signature as
$Sig_{agg} \leftarrow Sig_j . \prod_{i=0}^{j-1} Sig_i$.

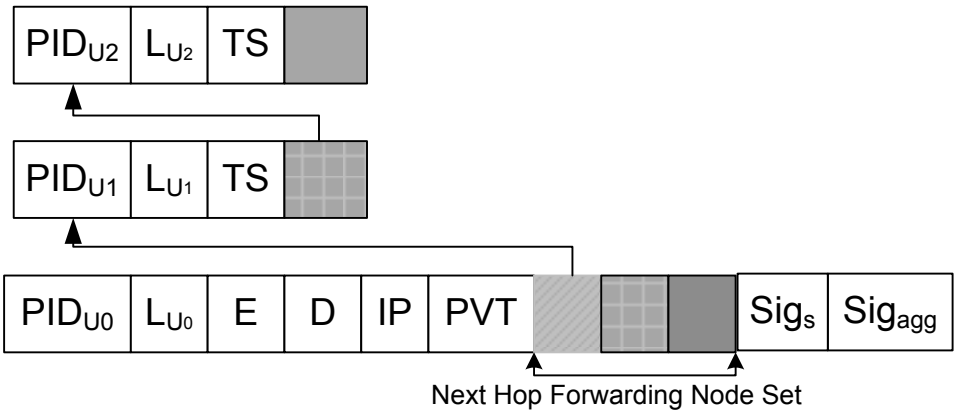

Figure 5.2: Data Packet architecture of RuralCare scheme

Intermediate node U_j verifies the aggregate signature as
$e(Sig_{agg}, g) \stackrel{?}{=}$
$e(PK_{U_0}, H(E||L_{U_0}||TS)) \prod_{i=1}^{j-1} e(PK_{U_i}, H(M_i))$
Here $M_i = PID_{PID_i}||L_{U_i}||TS_i$.

Cooperative intermediate nodes are also attached nodes' pseudo-identities, location information, and time-stamp (TS), as shown in Fig. 5.2. Cooperative intermediate nodes also store hashed value of the received data packet with their current location information as a receipt. In a non-cooperative environment, these receipts will be submitted to the TA to collect their individual rewards.

Step 6: Steps 4 and 5 will be repeated until the packet reached at RAP. It then obtains the aggregate signature as $Sig_{agg} \leftarrow Sig_0 \prod_{i=1}^{d-1} Sig_i$ and verifies the validity of Sig_s and Sig_{agg} as $e(Sig_s, g^{H(M_u||E)}.PK_{U_o}) \stackrel{?}{=} e(PK_D, g)$, and $e(Sig_{agg}, g) \stackrel{?}{=}$
$e(PK_{U_0}, H(E||L_{U_0}||TS)) \prod_{i=1}^{d-1} e(PK_{U_i}, H(M_i))$,
here $M_i = (PID_{U_i}||L_{U_i}||TS_i)$.

Step 7: RAP now removes the details of next hop forwarding node set and provides incentive, or updates reputation of the participated users in our proposed RuralCare scheme.

Phase-3:Communication between RAP and RSUs

In our system model, all RSUs are securely connected to the TA and located at the city area, so it is sufficient to deliver the packet to any RSUs using VANETs. Steps in phase-3 are same as Phase-2, except some identities are changed. Vehicles (type-2) in the rural area are cooperate as packet carrier and search for any vehicle going towards the

city, and vehicles (type-3) going towards city are treated as packet forwarder. The *RAP* follows packet forwarding $step-4$ and $step-5$ of the $phase-2$. Intermediate cooperative vehicles,$(V_{1...d-1})$, calculate short signature as
$Sig_i = v_i.H(PID_i||L_{V_i}||TS_i);\ i := 1..d-1$. Intermediate nodes verify the aggregate signature before forwarding it to the next cooperative node. When the packet reaches to any RSU, indicated as destination 'D', the RSU verifies the validity of the message as shown in $step-6$. It then decrypts the message 'm' as $m = \mathcal{D}ec_{k_{sd}}(E)$, and provides the incentive and rewards to the participated vehicles $(V_1...V_{d-1})$.

5.4.3 Signature Correctness

The correctness of Sig_s and Sig_{agg} are given as follows:

$$\begin{aligned} & e(Sig_s, g^{H(M_u||E)}.PK_{U_o}) \\ & = e(PK_d^{\frac{1}{H(M_u||E)+u_0}}, g^{H(M_u||E)}.g^{u_o}) = e(PK_d, g) \end{aligned} \tag{5.4}$$

$e(Sig_{agg}, g) = e(Sig_0 \prod_{i=1}^{d-1} Sig_i, g)$
$= e(u_0 H(E||L_{U_0}||TS).\prod_{i=1}^{d-1} Sig_i, g)$
$= e(PK_{U_0}, H(E||L_{U_0}||TS)).\prod_{i=1}^{d-1} e(PK_{U_i}, H(M_i))$

5.4.4 Incentive and Reputation Granting:

The TA/RAP provides incentive or reputation to the cooperative nodes as demonstrated in Algorithm 2.

5.5 Security Analysis

In this section, we analyses different security and privacy issues of the proposed RuralCare scheme. Notice that 'node' and 'user or vehicle' are used interchangeably.

Resilience to Packet Analysis Attack: In the proposed scheme, a source node U_0 has encrypted the sensitive message m into $E = \mathcal{E}nc_{k_{sd}}(m)$. The adversary can not recover m and knows user's physiological medical information without knowing both of the user's and RAP's secret keys. Computational Diffie-Hellman (CDH) hardness, described in section II, ensures that even the adversary knows the public keys, he can not generate

Algorithm 2 Incentive and Reputation Confirmation

Require: The RAP and TA obtain aggregate signature and verify the validity of the message.

1: Get the location information, $L_{V_0}, L_{V_1}, ...L_{V_{d-1}}$, measure each intermediate node relay distance $Dis_i = |L_{U_i} - L_{U_{i-1}}|$ and their routing direction with types.
2: **for** i=1 to $d-1$ **do**
3: **if** Data packet reaches destination and the total routing time $\leq$ PVT **then**
4: Provide incentive $C_i = Dis_i \times C_{IP}$, as described in the incentive-strategy subsection.
5: **else**
6: Provide reward $R_i = Dis_i \times R_{IP}$ and incentive if accumulated rewards exceed some predefined reputation-threshold.
7: **end if**
8: Store the C_i and R_i in the individual PCA and PRA account respectively.
9: **end for**

the shared key in an expected polynomial time. The adversary can get only the location (L_{U_0}) information, but this information does not has any link to the user's original identity. Moreover, any intermediate node is not allowed to hold relaying packet for an undefined time due to the packet validity time period (PVT). This parameter also reduces the probability of eavesdropping attack because the computation time needed to break the CDH hardness is far more than the PVT.

RuralCare ensures message integrity and source authentication: RuralCare ensures end-to-end message integrity. Users register their body-sensors at the initialization phase and TA generates public-private key pair and pseudo-identities for these devices. Sensor's pseudo-identity is a hashed value of respective user identity and sensor's Media Access Control (MAC) address. This pseudo-identity (PID_{SN}) is used for message encryption and signature during the communication between body-sensors and PDA. It ensures message integrity at the user's end. On the other hand, RuralCare uses sender's secret key to generate the signature Sig_s, and the receiver can verifies the signature by using the public parameters of the sender, shown in Equ. 4. This verification ensures corresponding source authentication. Hashed value of the encrypted message along with others system parameters are integrated with Sig_s and Sig_{agg}, which ensures message integrity with non-repudiation.

Resistent to intermediate-node removing or adding:
RuralCare scheme uses aggregate group signature, where secret key of each intermediate

relay nodes is multiplied with the original signature. If any selfish node removes previous relaying nodes' identities, the validity of the signature will be failed and encrypted message will be treated as invalid. Honest cooperative nodes in that case submit their received packet to the TA, and the TA can easily catch out the misbehaving nodes by checking the submitted users aggregate signatures. The TA will then remove this selfish node and thus resist intermediate-node removing or adding. Moreover, this resistent helps to grow up cooperative attitude among all authorized users of the proposed RuralCare scheme.

RuralCare provides user's identity privacy: We use users' pseudo-identities instated of their real identities to provide user's identity privay, and these pseudo-identities are periodically updated and maintained by the TA. Publicly available pseudo-identities are generated by using one way cryptographic hash function and computing real-identity from these pseudo-identities is impossible since keyed hash is one-way. To make these pseudo-identities more indistinguishable, the TA periodically update user's pseudo-identities.

RuralCare provides fairness: RuralCare user's only pays credits to the cooperative intermediate users/vehiles based on distance that they travel to relay the data packet. However, if the data packet will not reach at the destination, the user won't pay any credits and it is fair to the user's perspective. The intermediate users/vehiles who are not responsible for the non-cooperative packet drooping, will gain reputation values from the TA. The RSUs and RAP always give priority to the highly reputed users. Even, if their aggregated reputation values cross the pre-defined threshold, they will get some incentive from the TA for their cooperative behavior. Thus, intermediate users or vehicles feel fair to forward RuralCare's data packet and improve the network performance.

Resistent to the eavesdropping attacks: An eavesdropping attacker aims at accessing the private and sensitive patient's medical data. The CDH hardness (details in Basic of Bilinear Pairing subsection) ensures that the proposed scheme is resistant to this eavesdropping attack. Moreover, any intermediate node is not allowed to hold relaying packet for a undefined time due to the packet validity time period (PVT). This parameter also reduce the probability of eavesdropping attack because of computation time needed to break the CDH hardness is far more than the PVT.

5.6 Performance Evaluation

In this section, we evaluate the performance of RuralCare in terms of probabilistic model, cryptographic overhead, average delivery ratio, and delay.

5.6.1 Probabilistic Model

We conduct a probabilistic model to analyze the relation among the total number of users (n) in a given region, probability of having acceptable incentive rate (p_i) agreed by intermediate relay nodes, and the successful packet forward probability (P_f).

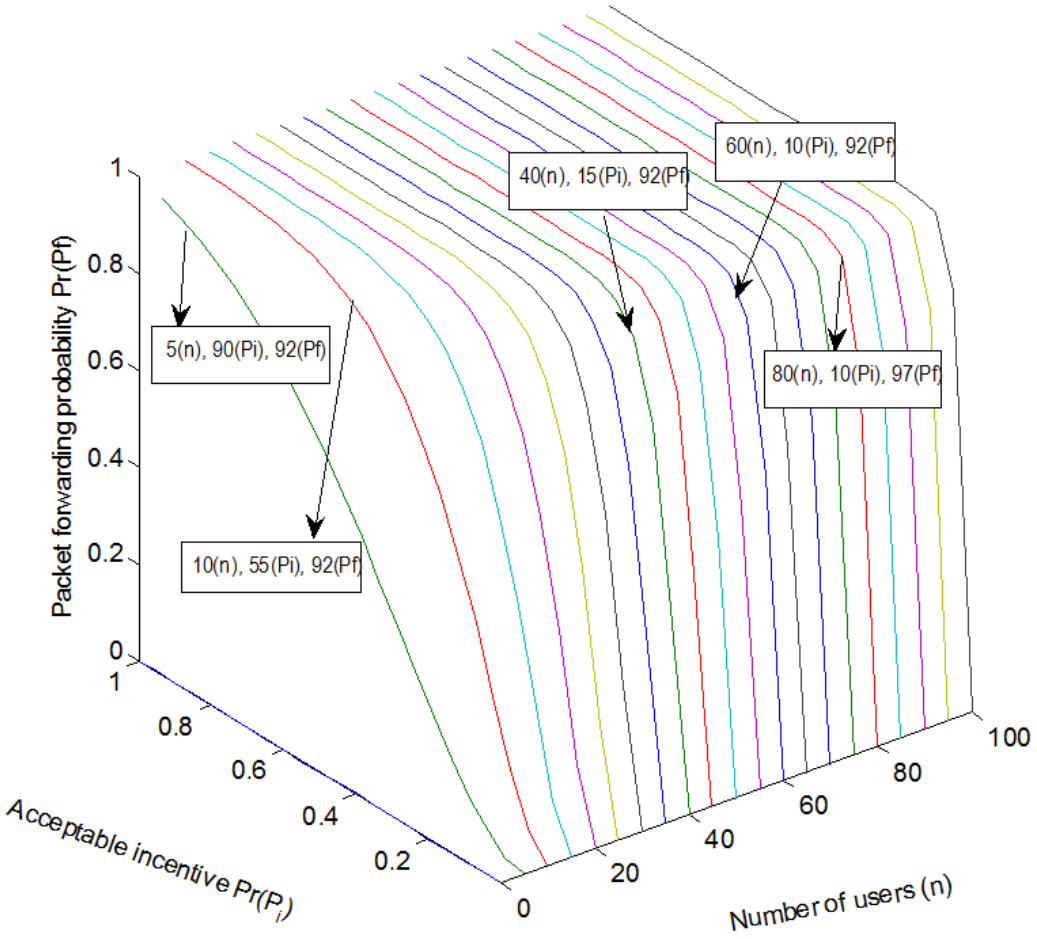

Figure 5.3: Relation among P_f, p_i, and n

Let $E(A_i)$ be the event that there are i cooperative nodes, and $n - i$ be the number of non-cooperative nodes in a specific area. Let $E(P_f)$ be the event that there is at least a node that agree with the incentive policy and will verify the message to relay to the

next-hop node. Using the equation of total probability, the relation among $Pr(P_f)$, n, and $Pr(P_i)$ can be represented as:

$$Pr(P_f) = \sum_{i=0}^{n} Pr(E(P_f)|E(A_i)).Pr(E(A_i)) = 1 + (1-p_i)^n - 2(1-\frac{p_i}{2})^n.$$

Here, $(1-p_i)^i$ is the probability that none of the i users agrees the incentive policy, $(1-(1-p_i)^i)$ is the probability that there is at least one cooperative node that accept the incentive policy, and $(1-(1-p_i)^{n-i})$ is the probability that there will be at least one non-cooperative node may feel interest to relay the message to the next-hop and accept the incentive policy. Hence, $Pr(E(A_i)) = \binom{n}{i}(1/2)^i(1-\frac{1}{2})^{n-i}$ and $Pr(E(P_f)|E(A_i)) = (1-(1-p_i)^i)(1-(1-p_i)^{n-i})$; each user position is independent and follows binomial distribution. Fig. 5.3 shows the relation among $Pr(P_f)$, $Pr(P_i)$, and n. It can be seen that $Pr(P_f)$ increases as either $Pr(P_i)$ or n increases. Fixing the packet forwarding probability, $Pr(P_f)$, more than 90%, we have to ensure either large number of users or higher incentive policy. For example, when $Pr(P_i)$ is 15%, we have to ensure number of user is greater than or equal to 40 to have 91% of $Pr(P_f)$. But for a low number of users $n = 10$, we have to confirm $Pr(P_i) \geq 55\%$ to have more than 90% of $Pr(P_f)$.

5.6.2 Cryptographic Overhead

In our layered packet architecture, the elements in $\mathbb{G}$ could be up to 160 bits [66]. We assume the Sig is 20 bytes, E is 120 bytes, and all other fields are 4 bytes. If there are n-intermediate nodes in the network, the communication overhead is around $140 + 24.n + 20 + |Sig_{agg}|$ bytes, $|Sig_{agg}|$ denotes the length of aggregate signature that minimize the packet length in a layered architecture [66].

Time Cost: We consider 20ms and 550ms as the computation time for the pairing using personal computer and personal digital assistant (PDA) that used as gateway in WBAN [71]. Computing cost of pairing at OBUs is expected to be same as personal computer. In [52], it is shown that a single pairing T_{pair} needs about 10 times more to compute than a multiplication T_{mul}. Proposed RuralCare's signature and verification processes need $T_{pair} + T_{mul}$ and $2.T_{pair} + T_{mul}$ operations, respectively. Based on the time analysis, we use 600ms and 20ms as the signing time for user and vehicle, respectively.

5.6.3 Simulation

We implement RuralCare scheme using a custom event-driven simulator built in Java, and consider three types of vehicles in the simulation scenario: type-1: only driving in the city

Parameter	Value Range
City area	$5000m \times 6000m$
Rural area	$10000m \times 6000m$
DTN nodes	N=60, 100
Velocity	50km/h, 80km/h
Packet interval	Every 20min
Communication range	
PDA	200m
RAP	350m
OBUs	100m
RSUs	350m
Simulation time	12-hrs
Incentive Rate (IR)	50,70,90

Table 5.1: Simulation Parameters

area, type-2: driving in rural area, and type-3: driving between city and rural areas.

At first, we evaluate the performance by changing number of deployed RSUs and acceptable packet-holding time (HT) at the city area. Here, HT is the valid time duration by which the data packet has to be forwarded to the next cooperative relay node. Considering the city area as $5km \times 6km$, we deploy RSU in every $30km^2$ refer as RSU-1, every $10km^2$ refer as RSU-3, and every $6km^2$ refer as RSU-5. Packet-holding time HT chooses as 45 min and 120 min. Simulation results demonstrate that deploying more RSUs have a good impact on the delivery ratio (Figs. 5.4 and 5.5) and by increasing the packet-holding time, intermediate relay nodes have got more chance to deliver data packets at the destination. But compare to RSU-1, RSU-3 and 5 have almost identical performance using long holding time (2hrs). Based on this observation, we deploy RSUs in every $10km^2$ (RSU-3) and prefer to use long packet-valid-time (PVT) for the rest of simulations.

We run the rest of simulations in an area of 15000×6000m for 12 hours (assumed PVT =12 hours), where road intersections are located at every 1km and 5km in the city and rural area, respectively. Other simulation parameters are summarized in Table 5.1.

In our simulation, we deploy 60% of nodes in the city area (type-1), 20% in the rural area (type-2), and the rest are traveling forward and backward between the city and rural areas (type-3).

Figs. 5.6 and 5.7 show the impact of vehicle's speed, incentive rate, and number of vehicles on the packet delivery ratio over a period of time. By increasing the vehicle's speed, we can achieve better packet delivery ratio compare to lower speed having the same

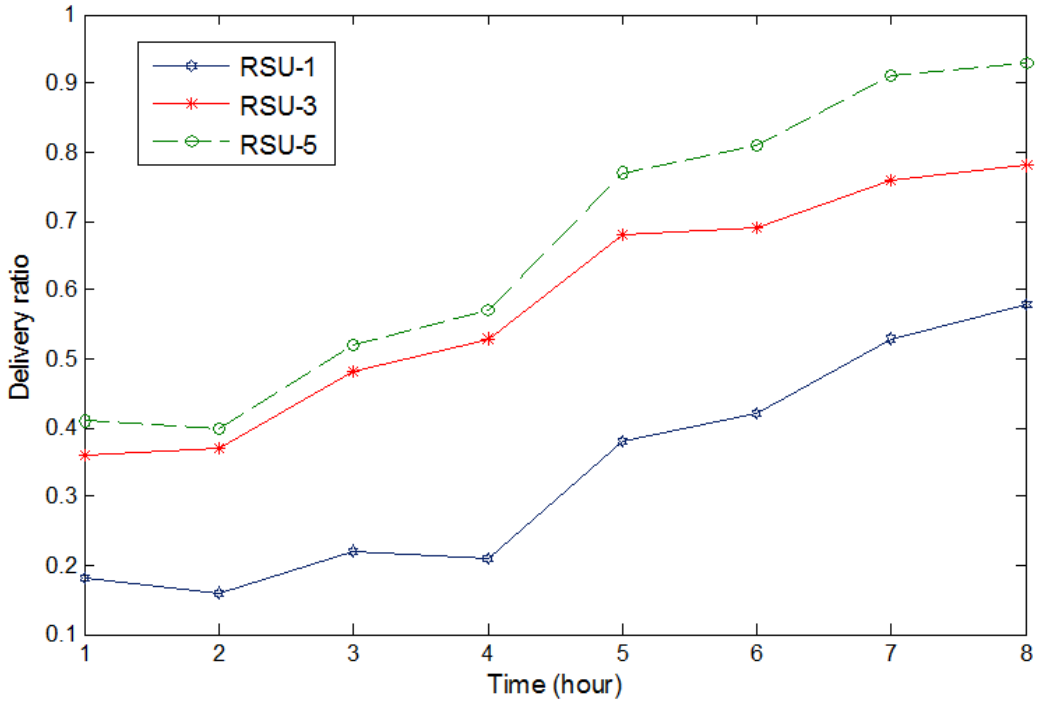

Figure 5.4: Packet delivery ratio with HT=45min

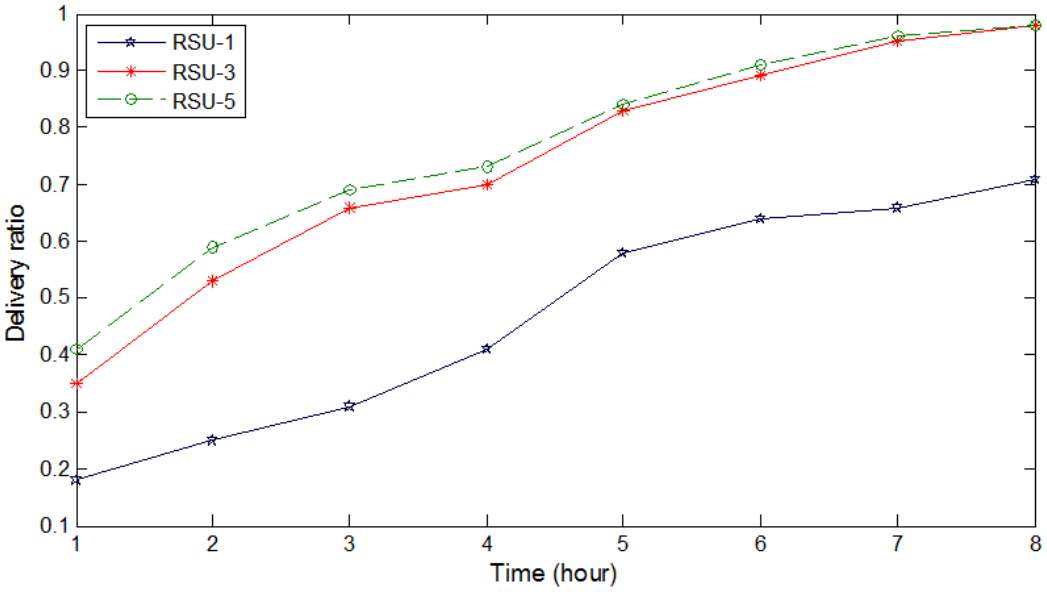

Figure 5.5: Packet delivery ratio with HT=2hrs

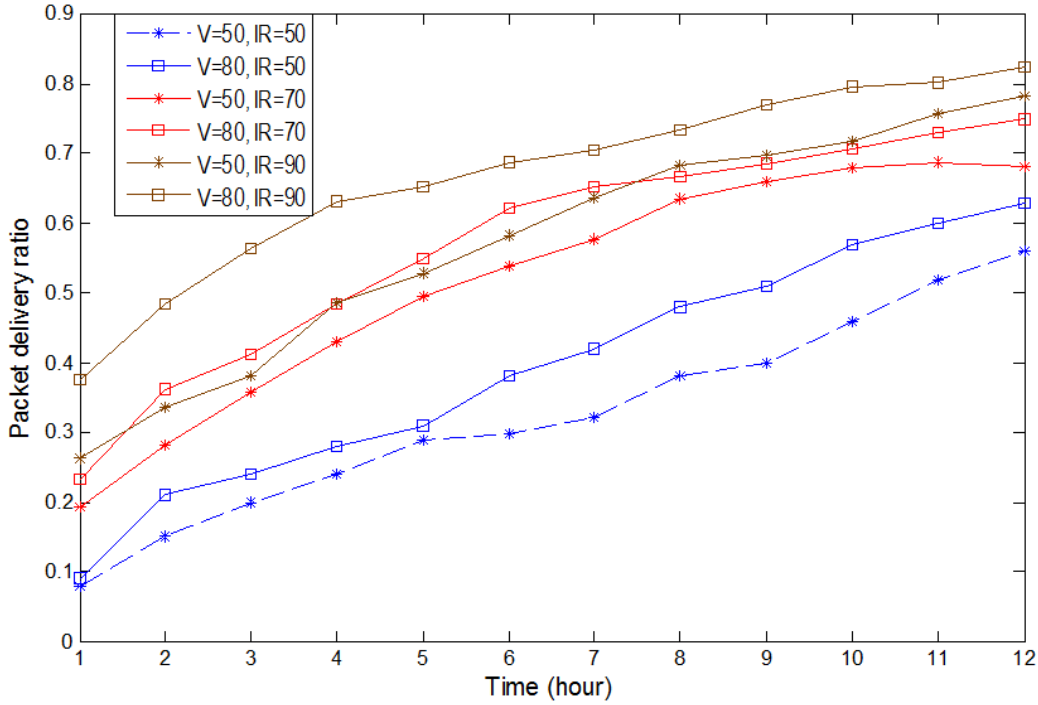

Figure 5.6: Delivery ratio with N=60

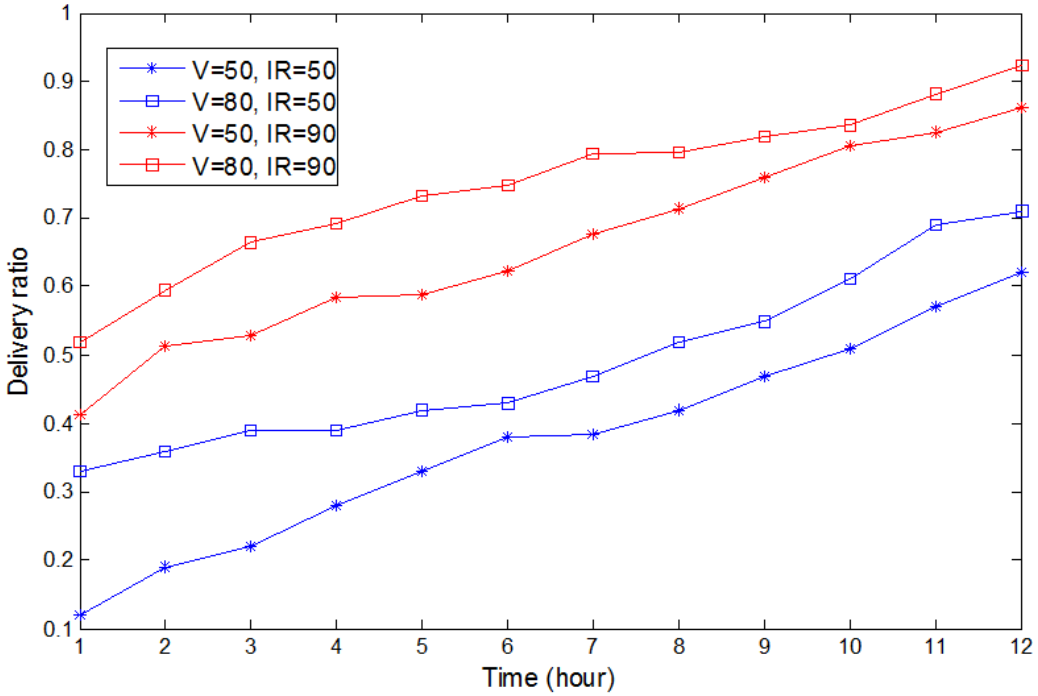

Figure 5.7: Delivery ratio with N=100

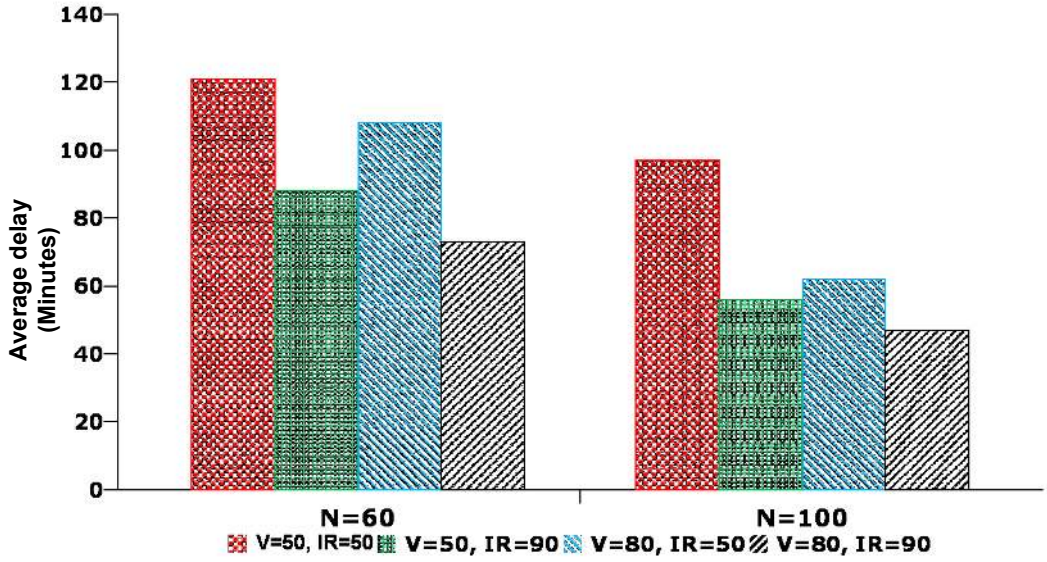

Figure 5.8: Average delay within 12 hours simulation with number of vehicles N=60 and 100

incentive rate. For example, around 20% more packet delivery ratio can be achieved by increasing vehicle's speed from 50km/h to 80km/h at the fourth hour of simulation with N=60 (Fig.5.6). Increasing incentive rate motivates participating vehicles to relay other data packet and it assists to increase the packet delivery ratio too. Simulation results demonstrate that we can achieve around 80% of packet delivery ratio having V=80,IR=90 and N=60 at the 9th hour. It is around 30% more compare to that of IR=50.

Fig.5.7 shows that higher packet delivery ratio can be achieved by increasing the number of participating users, N. For example, at the 4th hour, we can get around 30% packet delivery ratio having N=100, V=50, and IR=50, but with N=60 we can achieve only 20%. To ensure higher packet delivery ratio, we need to confirm either higher incentive rate or large number of participant users.

Fig.5.8 depicts the average end-to-end delay with 12 hours of simulation having variation in number of nodes (N) and incentive-rates (IR). We can see that increasing number of nodes and incentive-rate reduce the average delay and the average delay varies between 50-minutes and 120-minutes.

5.7 Summary

In this chapter, we have proposed a delay-tolerant secure long-term health care system, RuralCare, for monitoring patients located at rural area. RuralCare ensures secure and privacy preserving data aggregation using body sensors in WBAN environment. It describes data forwarding steps from the patient end to the care-giver's end that also achieves different security and privacy requirements. The fairness among all cooperative participants in RuralCare is guaranteed by adopting proper incentive and reputation policies. These policies also improve the network performance in terms of high delivery ratio and low average delay. Through extensive security and performance analyses, it has been demonstrated that RuralCare is highly effective to resist possible security attacks and efficient to provide emerging health care to patient resides at the rural area.

Chapter 6

Enabling Patient-centric Access Control of Aggregated Data in Cloud Computing

6.1 Introduction

In our previous chapters, we have described the high potentiality of eHealth care system in terms of improving quality of diagnosis, reducing medical costs and helping address the reliable and on-demand health care challenges posed by the aging society. We addressed different data aggregation solutions based on patient's residency and communication network availability. In addition to the secure data aggregation, the eHealth care system needs to ensure the availability of PHI in electronic form adheres to the same levels of privacy and disclosure policy as applicable to present-day paper-based patient-records accessible only from the physician's office. Instead of storing the PHI locally, the recent advancement of cloud computing allows us to store all PHI at the cloud storage and ensures availability with reduces the capital and operational expenditures [72]. In cloud storage (or data storage as a service), data is stored on multiple third-party servers where the storage can be administrated on demand. Migrating patients PHI into this cloud storage offers enormous conveniences to the eHealth care providers, since they do not have to care about the complexities of direct hardware management [7]. However, computerized PHI are open to potential abuse and security threats. Storing large amounts of patient's sensitive medical data in third-party cloud storage is vulnerable to loss, leakage, or theft [73]. In addition, patient's privacy with proper access control to cloud storage is a growing concern in the

eHealth care industry due to its direct involvement to human. Stored data confidentiality is considered as one of the biggest challenges raised by cloud storage environment. Especially in a public clouds environment, which are operated by commercial service providers and shared by various other customers, data confidentiality is a desired property.

Traditional data access schemes which are used to provide data confidentiality are mostly depend on the system itself to enforce authorization policies and rely on the system trusted infrastructure. Providing data confidentiality by server side data encryption is not also appropriate for the health application when the server is not fully trusted. In addition, patient's privacy with proper access control to cloud storage is a growing concern in the eHealth care industry due to its direct involvement to human. Patient generally wants to be sure that his sensitive health information can only be accessed by particular authorized users and his original identity will not be exposed. In order to assure the privacy of PHI, we propose efficient and secure patient-centric access control (ESPAC) scheme which allows data requesters to have different access privileges based on their roles, and then assigns different attribute sets to them.

To store PHI in a cloud storage with patient-centric access control privilege, we use ciphertext-policy attribute-based encryption [74] in ESCAP. Identity based encryption is adopted to ensure secure end-to-end communication among patient, eHealth care service provider, and cloud storage. Our contributions are in three-fold: a) provide an architectural model of eHealth care system, b) show how ESPAC provides a secure communication between remote patient and eHealth care provider, and c) present an patient-centric access control policy that helps ESPAC to has more reliability. To construct this access control policy, we assign different attribute sets to data requesters based on their relation to the patient. For example, general users may know some common attributes of a patient, e.g., location, gender; patient's relatives or health care givers may know more private information of a patient, likely medication details, patient date of birth, patient phone number, etc.; health insurance providers may have more privileges and can know patient health card number, Social Identification number, etc.

The remainder of this chapter is organized as follows. Section 2 contains a brief description of related work. System model and security requirements are presented in Section 3. Preliminaries such as bilinear pairing, security definition are introduced in Section 4. The proposed ESPAC scheme is presented in Section 5. Section 6 and Section 7 provide security analysis and performance analysis of the proposed ESPAC scheme respectively. Section 8 introduced M-ESPEC, the modified version of the ESPAC. The chapter is concluded in Section 8.

6.2 Related Works

Existing research works related to proposed ESPAC includes i) secure and privacy preserving eHealth care system ii) attribute-based encryption and iii) access control over untrusted cloud storage.

Hybrid security policy for WBANs with Quality of Services (QoS) have recently been proposed for secure eHealth care system in [56]. Public key cryptography is used for session key management and private key cryptography is used for regular data encryption in WBANs environment. Due to the nature of the real-time traffic, emergency health application traffic is given high priority compare to other applications traffic. Lu. et al. propose a mobile health care social network, where two patients can communicate each other if they have the same symptoms [75]. Performance analyzes demonstrate that emergency response time can be minimized by using proposed mobile health-care social network. Lin et al. present a privacy preserving scheme for health care that can effectively works against global adversary [76]. Both content and contextual privacy can be achieved by the proposed work.

Attribute-Based Encryption (ABE), a novel extension from identity based encryption by enabling expressive access policy to control the decryption process is first presented in [77]. Key Policy Attribute-based Encryption (KP-ABE) and Ciphertext Policy Attribute-based Encryption (CP-ABE) are the two main variants of ABE proposed so far. In both cases, user has a set of attributes that associate with user's private key. The attribute set is used to describe a user's credentials. In KP-ABE, user's private key is embedded with an access policy, whereas ciphertext is encrypted by an pre-defined access policy in CP-ABE [2, 74]. Liang et al. [78] present a patient self-controllable access policy so that patients would have the primary control of the access to their own personal health information.

Health records sharing and integrating in health care cloud is discussed in [79]. The article describes the security reference model for managing different security issues in healthcare clouds. Yu et al. propose a fine gained data access control in cloud computing based on KP-ABE [7]. Confidentiality of user access privilege and user secret key accountability can be achieved by the work. A mandatory access control model to protect patient's metadata with privacy is presented in [80]. It is shown that the use of fragmentation after encryption greatly improves overall security because potential attackers need to compromise more data file to gain access. Without disclosing the data contents, data owner delegates most of the computation tasks involved in fine-grained data access control to untrusted cloud server by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption. An efficient cloud storage sharing scheme is presented in [81]. The scheme works on hierarchical identity based encryption, where intended recipients can share the

file by using their private keys. G. Wang et al. combine hierarchical identity-based encryption and CP-ABE to achieve fine-grained access control in cloud storage services [82].

Most of the current works encrypt PHI before being stored at cloud with defined access policy at storage server. But this approach does not ensure patient centric access control and has a risk to have inside attack. Most of them use ciphertext-policy attribute based encryption (CP-ABE) [74] to construct the access policies and assign different attribute sets to data requesters based on their relation to the data owner [83] [84] [85] [86]. However, there are some common drawbacks existing on those works. If the data requester can submit all the attributes correctly, CP-ABE executes on the root node of the access tree and decrypt the encrypted PHI. This can open the door of potential privacy exposure, as the cloud can collide with data requester to get access to the PHI too. To perform user revocation, the cloud needs to re-encrypts all stored PHI with different access architecture. It costs a huge computation overhead to the cloud and increases the eHealth expenditure because cloud service provider (CSP) will demand more service cost to perform additional computation tasks. In addition, it is not practical to delegate all access control tasks to the third party CSP [87].

6.3 System Model and Security Requirements

In this section, we define the system model and then describe the security requirements of the proposed ESPAC scheme.

6.3.1 System Model

In our system model, we define the following entities:

1. Trusted Authority (TA): It generates the public and secret key parameters for the ESPAC. The trusted authority is responsible for attributes' keys issuing, revoking, and updating. It grants differential access rights to individual users based on their attributes and roles. Trusted authority also maintains an index-table, where it stores the location of distributed data storage server. Authorized health service providers (e.g., Hospital, urgent care) are denoted as trusted parties.

2. Cloud Service Provider: It provides data outsourcing services and consists of data servers and data service manager. The main responsibility of the data storage server

is to serve and retrieve data according to authorized users' request. Data service manager negotiates with health-care service provider to control the access from outside users to the stored encrypted data.

3. Registered User: Patient who is registered to the trusted authority is considered as registered user. A Registered User is responsible for defining attribute-based access policy and encrypting the sensitive PHI under the predefined policy before storing at the cloud-storage.

4. Data-access requester: Cloud users who request to access some specific PHI are called the data-access requester. The ESPAC scheme ensures that any data-access requester can only decrypts the encrypted data if and only if he can successfully completes the access-policy.

The encrypted data is stored in a centralized storage, health-cloud, for future access. Based on the major operations, the proposed scheme can be classified into four major steps, as shown in Fig 6.1.

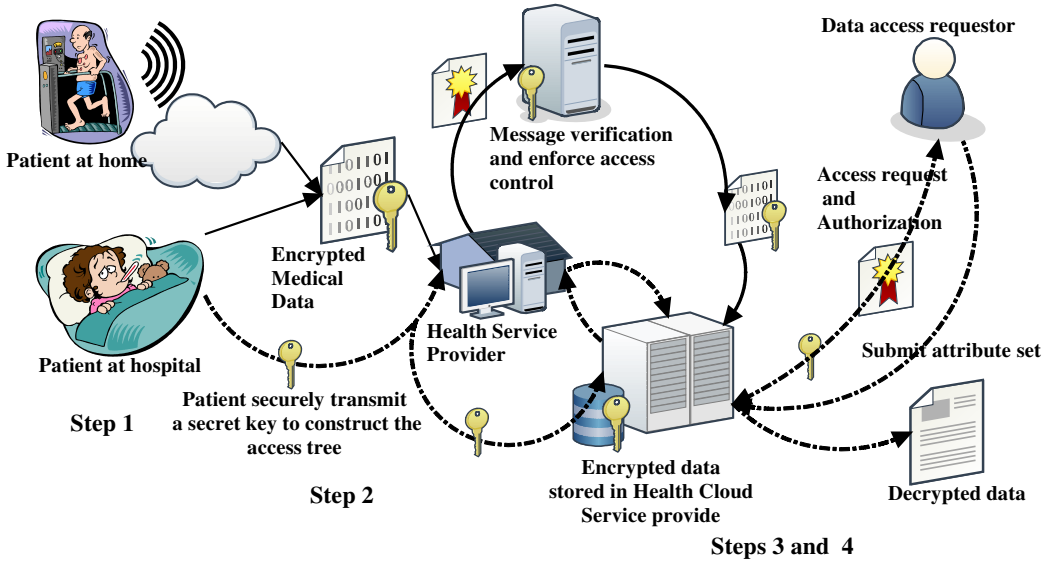

Figure 6.1: Major steps of the proposed ESPAC scheme

Step 1 (PHI collection): In this initial step, using different body sensors, PHI is sensed and ready to be transmitted to the trusted eHealth care service provider.

Step 2 (Secure data communication): In this step, public key cryptography is used to securely transfers collected PHI to the eHealth care service provider. Patient securely transfer a secret key to the trusted eHealth care provider, if he authorized the service provider to build-up the access tree.

Step 3 (PHI processing at eHealth care provider): After receiving the PHI securely, eHealth care service provider classifies the PHI based on the attributes set chosen by the patient. It then makes different privacy levels of data requesters based on their roles (e.g., level-1: general users, level-2: pharmacist, level-3: doctors, etc.) and assigns different set of attributes to these different levels.

Step 4 (Transfer PHI to the cloud storage and control access): After the data classification, encrypted data securely transfers to the cloud storage, shows as 'Health Cloud' in the Figure 6.1. eHealth care service providers may operate either real-time or periodically based on the existing infrastructures. Data-access requester sends request to the cloud storage with a data block identity. They may also request for the corresponding attribute sets. In this case, the cloud storage provider communicates with the eHealth care service provider and verifies the authentication of the requesters. The data requester, as a node in the access tree ($\mathbb{T}$), can decrypt a ciphertext if and only if other corresponding nodes (users) also cooperate with him, or he has all the attribute sets to complete the $\mathbb{T}$.

In our system model, we classify the data requester as health worker, physicians, researchers, insurance companies, and agencies, etc. Some of them only need the accumulated number of patients in a specific area, some need disease related syndromes, age and gender specific characteristics, while others may need medication details. Figure 6.2 shows possible access structures based on different privacy levels, where intermediate nodes work as a logic gates. For example, "2 of (location, gender, disease)" in the Figure 6.2(a) can be converted to "(location AND gender) OR (gender AND disease) OR (disease AND location)".

6.3.2 Security Requirements

We aim at achieving the following security objectives.

1. *Patient-centric access control:* The system should provide patient-centric access control, where a patient can decide who can get the access to his/her stored PHI.

2. *Message integrity, source authentication and non-repudiation:* All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated

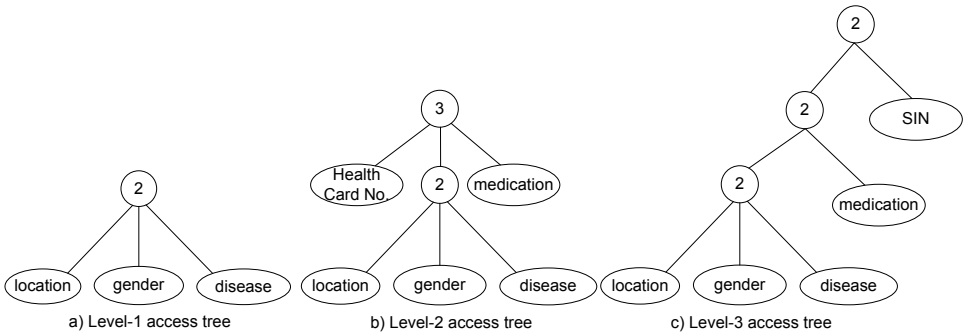

Figure 6.2: Access trees based on different data privacy level

by the eHealth care service provider. To ensure the non-repudiation, the patient can not refute the validity of a PHI afterward.

3. *Prevention of Ciphertext-only attack:* The system should be secured enough to prevent recover of the plaintext from a set of stored ciphertexts.

4. *Provide patient privacy:* Privacy is one of the important concerns from a patient perspective. Illegal disclosure and improper use of patient PHI can cause legal disputes and undesirable damaging in patient's personal life.

5. *Resistant to collusion attack:* If multiple users collude, generally they may be able to decrypt a ciphertext by combining their attributes. Users can not get any access to the encrypted data even by sharing information in a group.

6. *Resistant to Denial-of-Service (DoS) attack:* The DoS attack may be caused due to the large groups of legitimate users access the eHealth care service provider at the same time, or the attacker continuously launch false traffic with a high data rate. The system should ensure acceptable QoS level to resist the DoS attack.

6.4 Defination

Bilinear pairing and the attribute-based ciphertext policy (CP-ABE) work as the basis of our proposed scheme, we briefly review some related definitions of CP-ABE , which closely follow those in [30].

Definition (BDH Parameter Generator): An algorithm *Gen* is called a BDH (Bilinear Diffe-Hellman) parameter generator if *Gen* takes a sufficient large security parameter

$K > 0$ as input, runs in polynomial time in K, outputs a prime number q, the description of two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order q, and the description of a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

Definition (BDH Problem hardness): Given a random element $P \in \mathbb{G}_1$, as well as aP,bP,cP, for some random $a, b, c \in \mathbb{Z}_q^*$; there is no efficient algorithm to compute $e(P, P)^{abc} \in \mathbb{G}_2$ from $P, aP, bP, cP \in \mathbb{G}_1$. This implies the hardness of the BDH in the group $\mathbb{G}_1$ [30].

Definition (Access Structure [74]): Let $\{a_1, a_2, ..., a_n\}$ be a set of health attributes. The sets $\mathbb{A}$ ($\mathbb{A} \subset 2^{\{a_1, a_2, ..., a_n\}}$) are called the authorized attributes set, and the sets not in $\mathbb{A}$ are called the unauthorized sets. $\mathbb{A}$ is monotone if $\forall B, C : if B \subseteq \mathbb{A}$ and $B \subseteq C$ then $C \subseteq \mathbb{A}$.

In the access-tree construction, ciphertexts are labeled with a set of descriptive authorized attributes. Secret keys are identified by an access tree in which each interior node of the tree is a threshold gate and the leaves are associated with attributes.

Setup(1^t): The probabilistic polynomial time (PPT) setup algorithm takes as input a security parameter 1^t. It outputs the public parameters PK and a master key MK which is known only to the private key generator.

Encrypt$_1$(PKs, m, PKr) : The encryption algorithm takes the public parameters of the sender and receiver and encrypt the message 'm' by doing mapping and XOR operations. We use $Encrypt_2(PK, M, A)$ function to encrypt the message M and store in the health cloud. This encryption algorithm takes the system public parameters PK, a message M, and an access structure $\mathbb{A}$ over the universe of health attributes. The encrypted ciphertext CT can only be decrypted if and only if the user possesses the set of health attributes that satisfy the access tree structure.

Decrypt$_1$(PK, C, d) : The decryption algorithm takses as input the public parameter PK, ciphertext C, and the product of the receiver's secret key and sender PK's hash value. The health care provider uses this function to decrypt the encrypt message sent by the user for further processing. Another decryption function $Decrypt_2(PK, CT, SK)$ takes as input the public parameters PK, a ciphertext CT, which contains the access policy $\mathbb{A}$, and a secret key SK, which is a private key for a set S of health attributes. If the set S of attributes satisfies the access structure $\mathbb{A}$, the algorithm will decrypt the ciphertext and return the message M.

The set of algorithms must satisfy the standard consistency requirements: For $(PK, MK) \leftarrow Setup(1^t)$ (MK is the system Master Key), $(k, E) \leftarrow Encryption(PK, \gamma)$, $D_{\mathbb{A}} \leftarrow KeyGen(PM, MK, \mathbb{A})$

and $\mathbb{A}(\gamma) = 1$ (i.e. the attribute set γ satisfies the access structure $\mathbb{A}$), then we have $Pr[Decryption(PK, E(M), D_{\mathbb{A}}) = k] = 1$.

6.5 Proposed ESPAC Scheme

The four major categories that have described in the system model can be further integrated into two major phases, as shown in Fig 6.3.

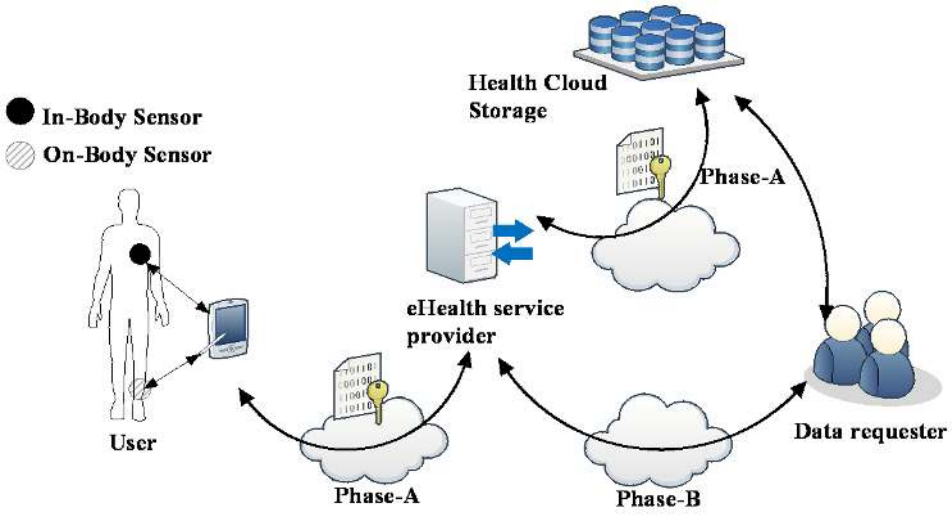

Figure 6.3: Two major phases of the proposed scheme

6.5.1 Phase-A: secure data communication:

In the phase-A, the scheme defines the secure and privacy preserving communication between different eHealth users. Here, we describe the secure communication steps between a remote user and an eHealth service provider; communication among others e.g., eHelath service provider and the cloud storage or data requesters will follow the same steps.

Step 1 (System initialization): Given the security parameter $S^{'}$, the bilinear parameters (q, G_1, G_2, e, P) are generated by the function $setup(S^{'})$. It is assumed that a unique ID is given to the health care provider (HCP) by a trusted authority and the health service providers will do the following initializations:

- Select a random number $\alpha \in_R Z_q^*$ and compute the public key $PK_{hcp} = \alpha.P$;

- Generate the hash function $H_1 : \{0,1\} \rightarrow \mathbb{G}_1^*$ and compute the key $K_{hcp} = H_1(ID)$ for message encryption and decryption;
- Generate the secure hash function $H_2 : \{0,1\}^* \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^* \rightarrow G_1^*$ and $H_4 : G_2 \rightarrow \{0,1\}^*$.
- Compute the remote user's pseudo-identity $(U_{PID}) = H_2(U_{ID})$, and store a copy of it for future verification;
- Securely distribute U_{PID}, H_2, H_3, and H_4 to its subscribers.
- For attribute-based Encryption and Decryption, the TA chooses two random number $\bar{\alpha}, \bar{\beta} \in \mathbb{Z}_p$, p is the prime order with generator g.
- Compute public key, $PK = \mathbb{G}, g, h = g^{\bar{\beta}}, f = g^{1/\bar{\beta}}, e(g,g)^{\bar{\alpha}}$. (details in [74])
- Compute master key, $MK = (\bar{\beta}, g^{\bar{\alpha}})$.

An individual user (U) will do the following steps:

- User Chooses a random number $r \in_R Z_q^*$ and computes the public key $PK_U = r.P$
- User selects a random number $\beta \in_R Z_q^*$, to calculate the session key $P_\beta = \beta.P$
- User computes the message token $T = H_2(m|U_{PID}|session\_id)$ and sends it to the receiver along with encrypted data and session key.

Step 2 (Secure message communication): After the system initialization, both parties use the data encryption and decryption algorithms to securely transmit their data. Here, we show how an user will encrypt the message 'm' ($Equ.6.1$) and decrypt the encrypted message by the corresponding eHealth care service provider. The user encrypts the message, m, based on the public key of the corresponding receiver using the identity based encryption [30].

$$v = Encrypt_1(PK_{hcp}, m, PK_U) = m \oplus H_4(g_U^r) \tag{6.1}$$

Here, $Q_U = H_3(U_{PID})$; $H_3 : \{0,1\}^* \rightarrow G_1^*$, a random oracle; $g_u = e(Q_U, PK_{hcp})$, and $H_4 : G_2 \rightarrow \{0,1\}^*$, a random oracle.

The encrypted message is decrypted using the $Dec(PK_U, v, d)$ function, where $d = \alpha H_3(U_{PID})$ and α is the secret key of the corresponding agent.

$$Decrypt_1(PK_U, v, d) = m \tag{6.2}$$

$Decrypt_1(PK_U, v, d) = v \oplus H_4(e(d, PK_U)$
$= v \oplus H_4(e(\alpha H_3(U_{PID})), rP)$
$= v \oplus H_4(e(H_3(U_{PID}), P)^{r\alpha})$
$= v \oplus H_4(e(H_3(U_{PID}), \alpha P)^{r})$
$= (m \oplus H_4(g_u^r) \oplus H_4(g_u^r)) = m$

Step 3 (Message Signature and Verification): To ensure data integrity, the receiver will verify the message signature after receiving it. By doing it, the eHealth service provider can verifies the data originated from the specific patient and can not be altered after signing it. We use the cryptographic digital signature ($Equ.(6.3)$), based on the bilinear pairing to provide data integrity. The patient first creates a session key $P_\beta = \beta P$, here $\beta \in_R Z_q^*$, and computes the message token T. He then computes the signature using the equation (6.3).

$$S = \frac{1}{v + \beta + r + T} P \tag{6.3}$$

The eHealth service provider verifies the signature by using the equation (6.4).

$$e(vP + P_\beta + PK_{U_{PDA}} + TP, S) = e(P, P) \tag{6.4}$$

$e(vP + P_\beta + PK_{U_{PDA}} + TP, S)$
$= e((v + \beta + r + T)P, (v + \beta + r + T)^{-1}P)$
$= e(P, P)^{(v+\beta+r+T)(v+\beta+r+T)^{-1}} = e(P, P)$

6.5.2 Phase B: Control of data requesters access

In a traditional public key cryptography system, the receiver and sender need each other public parameters to encrypt a message. But in the eHealth care system, the patient does not have any knowledge about the data requester or does not know who is going to access his PHI. Therefore, the security scheme by itself has to be capable to grant access control remotely. We use attribute-based ciphertext policy with privacy leveling to solve this challenge. Based on the different roles of the data requesters, an access tree is created and the requester needs to provide corresponding attributes (nodes of the tree) to have the secret key and thereafter he can use the secret key to decrypt the encrypted data (PHI). Providing falls attributes will stop the decryption processes immediately and the data requester learns nothing more than the attributes he/she is entitled. Details construction of the access tree with related key-generation, encryption, and decryption algorithms are described below.

Access Tree ($\mathbb{T}$): Let $\mathbb{T}$ represent an access structure. Each non-leaf node of the tree represents a threshold gate. If num_x is the number of children of a node x and k_x is the threshold value, then $0 \leq k_x \leq num_x$. When $k_x = 1$, the threshold gate is an OR gate, when $k_x = num_x$, it is an AND gate, finally when $1 \leq k_x \leq num_x$, it is a combination of AND and OR gates (Figure 6.2). The function $parent(x)$ returns the parent of node x. The function $att(x)$ is defined only if x is a leaf node and denotes the attribute associated with the leaf node x. The function $index(x)$ returns an ordering number associated with node x.

Let $\mathbb{T}$ be an access tree with root 'r'. Denote by $\mathbb{T}_x$ the subtree of $\mathbb{T}$ rooted at the node 'x'. Hence $\mathbb{T}$ is the same as $\mathbb{T}_r$. If a set of health attributes ω satisfies the access tree $\mathbb{T}_x$, we denote it as $\mathbb{T}_x(\omega) = 1$. We compute $\mathbb{T}_x(\omega)$ recursively as follows:

If 'x' is a non-leaf node, evaluate $\mathbb{T}_z(\omega)$ for all children z of node 'x'. $\mathbb{T}_x(\omega)$ returns 1 if and only if at least k_x children return 1. If 'x' is a leaf node, then $\mathbb{T}_x(\omega)$ returns 1 if and only if $att(x) \in \omega$.

Data formation and authentication: Before encrypting the data packets, the trusted eHealth care provider classifies the data set based on some privacy levels and assign some attributes on that message block (M). It then concatenates the message block (M), user pseudo identity U_{PID}, and the $session\_id$. After that the trusted eHealth care provider computes the token value $T = H_2(M|U_{PID}|session\_id)$. It then computes the signature using the equation 6.3. Local health care provider will store the block sequence and patient pseudo identity for future verification. Figure 6.4 shows the data packet structure. The health cloud service provider will check the message authenticity by verify the signature using the equation 6.4.

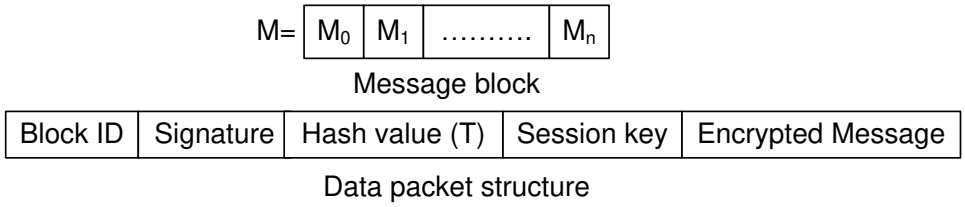

Figure 6.4: Data packet architecture

The health cloud service provider will generate the signature in the same way and store along with the encrypted messages for the data requester verification purposes.

Encrypt$_2$($\mathbf{PK}, \mathbf{M}, \mathbf{T}$) : The algorithm first chooses a polynomial q_x for each node x in the tree T. These polynomials are chosen in a top-down manner, starting from the root

node. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value of k_x. Starting with the root node 'R', the algorithm chooses a random $s \in \mathbb{Z}_p$ and sets $q_R(0) = s$. Then it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses d_x other points randomly to completely define q_x.Finally, the ciphertext is then constructed by giving the access tree structure $\mathbb{T}$ and compute

$$CT = (\mathbb{T}, C^{'} = Me(g,g)^{\alpha s}, C = h^s, \forall y \in Y : C_y = g^{q_y(0)}, C_y^{'} = H(att(y))^{q_y(0)}) \quad (6.5)$$

KeyGen(MK,S): The key generation algorithm takes as input a set of attributes S and outputs a key that identifies with the set. The algorithm first chooses a random $r \in \mathbb{Z}_p$, and then random $r_j \in \mathbb{Z}_p$ for each attribute $j \in S$, and outputs the key as

$$SK = (D = g^{\alpha+r)/\beta}, \forall j \in S : D_j = g^r.H(j)^{r_j}, D_j^{'} = g^{r_j}) \quad (6.6)$$

Decrypt$_2$(CT, SK) : The decryption procedure works as recursively and is defined by the function $DecryptNode(CT, Sk, x)$ that takes as input a ciphertext CT and a private key SK. If the node x is a leaf node, then the function works as follows:
$DecryptNode(CT, SK, x) = \frac{e(D_i, C_x)}{e(D_i^{'}, C_x^{'})}$
$= \frac{e(g^r.H(i)^{r_i}, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} = e(g,g)^{rq_x(0)}$

Here $i \in S$. If $i \notin S$, we define $DecryptNode(CT, Sk, x) = \perp$. When x is a non-leaf node, the algorithm is called by its all child nodes z. It then stores the output of $DecryptNode(CT, Sk, z)$ as F_z. Detail is shown in [74]. If the data requester can submit all the attributes correctly, the algorithm then executes on the root node 'R'. If the tree is satisfied by S, we set $A = DecryptNode(CT, SK, r) = e(g,g)^{rq_R(0)} = e(g,g)^{rs}$. The message 'M' can be decrypted by computing
$C^{'}/(e(C,D)/A) = C^{'}/(e(h^s, g^{(\alpha+r)/\beta})/e(g,g)^{rs}) = M$

6.6 Security Analysis

In this section, we evaluate the security and privacy issues of the proposed scheme.

The ESPAC scheme ensures user and eHealth agent's identity privacy: User and health agent use pseudo identity instead of their unique identity, and these pseudo identities are generated by a strong one-way hash function. The construction of the hash function is easy to sample and compute but hard to invert. Therefore, the privacy is ensured by the proposed scheme.

The scheme is secure to chosen ciphertext-only attack: Data transmissions from user to health agent, as well as from health agent to health cloud service provider are done with proper encryption schemes ($Encryption_1$ and $Encryption_2$). The processes are indistinguishable under chosen ciphertext attack based on the BDH problem hardness and this hardness ensures there is no probabilistic polynomial time algorithm that can decrypt the message from a set of chosen ciphertext.

The scheme is resistant to the eavesdropping and collusion attacks: An eavesdropping attacker aims at accessing the private and sensitive patient's medical data. This attack may be happened during the patient to eHealth care provider or eHealth care provider to the health cloud data communication. The BDH hardness ensures that the proposed scheme is resistant to this eavesdropping attack. To access the data at the health cloud server, an attacker needs to has sufficient attributes to complete the access tree. Here the random number 's' is divide into multiple shares based on the attributes set. For the non-privacy data set, he may get access and its allowed in our scheme. But he can't modified the data due to the verification bindings. However, for the patient sensitive data, a unique random number is embedded into both 'C' and 'D' of the equation shown in the $Decrypt_2(CT, SK)$ function. Without knowing that secret number, it is impossible to access the data in a probabilistic polynomial time. This hardness also demonstrates our scheme as a resistant to the collusion attack. Therefore, any attacker cannot successfully launch the eavesdropping or collusion attack to our proposed scheme.

The scheme ensures message integrity, non-repudiation, and source authentication: We use the patient's secret key and the session identity to generate the signature 'S' ($Equ.6.3$). The data receiver can verifies the signature by using the public parameters of the sender, shown in the Equ. 6.4. This verification ensures the corresponding source authentication. The scheme generates the message token value 'T' by computing the hash value of the concatenated message, patient's identity (P_{ID}), and a session sequence number. Only the patient and the eHealth care provider know the patient's original identity and the session sequence number. This token value is also used to generate the signature 'S'. Therefore the message integrity with non-repudiation can be provided by our proposed scheme.

ESPAC ensures backward and forward secrecy: The scheme prevents user to access the plaintext before providing the required attributes that satisfy the access policy. On the other hand, any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other attributes that he is holding satisfy the access policy. Thus, ESPAC ensures backwards and forward secrecy.

6.7 Performance Analysis

To evaluate the performance of the presented ESPAC, we first show the timing cost of operations used in ESPAC. We evaluate the computation timing cost by varying number of attributes. Finally, we analyze the performance of ESPAC to resist DoS attack, and conduct a simulation using NS 2.33.

Time cost: Based on the open source project CP-ABE [88], we evaluate computation time of attribute-based encryption and decryption in a Pentium-IV 3-GHz PC that has 1-GB of RAM. We varying the number of attributes from '2' to '40' and make different access-policies based on these attributes. Encryption and Decryption functions are executed on a 512-byte data-block. Simulation results show that computation time of $Encryption_2$ is increasing linearly with number of attributes, shown in Figure 6.5. $Decryption_2$ needs less computation time compare to $Encryption_2$. When the number of attributes is '2', $Encryption_2$ and $Decryption_2$ take 76 ms and 45 ms, respectively. These computation time reaches to 962 ms and 372 ms, when the number of attributes is altered to 40. Time cost of ESPAC operations is given in table 6.1.

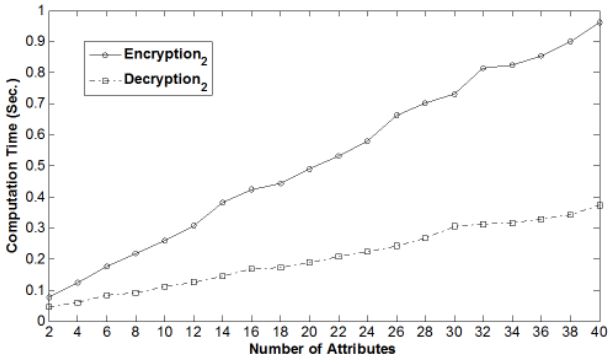

Figure 6.5: Computation time of encryption and decryption with different no. of attributes

Table 6.1: Time cost for ESPAC operations

Operation	Time	Operation	Time
Encryption1	C_e	Signature	C_m
Verification	C_e	Decryption1	C_e
Encryption2	$C_e + 2C_m$	Decryption2	$2C_e + C_m$

We denote by C_e a computation of the pairing, and C_m a scalar multiplication in G_1. Usually, pairing operations cost is much more than other computations. A single pairing

C_e needs about 10 times more time to compute than a scalar multiplication C_m [52], and our simulation shows a single pairing needs around 65ms to compute. We consider 550ms as the computation time for the pairing using a PDA [71] for further network analysis.

Analysis: The system blocking probability can be increased by high data rate traffic, or accessing the system by a large number of misbehaving users at a time. This increased rate of blocking probability is considered as a cause of DoS attack. In our analysis, we aim to minimize the blocking probability by restricting data rate and using multiple servers. We assume that the service provider serves multiple users. Users demand services according to a Poisson process and request independent and identical distributed exponential service time. We use M/M/1/K and M/M/m/K queuing model for analysis and assume that the blocking probability should be less than 30% to provide adequate Quality of Service (QoS) to the users. Blocking probability $P_1(K)$ and $P_m(K)$ of the M/M/1/K and M/M/m/K queue respectively can be written as follow:

$P_1(K) = \frac{1-\rho}{1-\rho^{K+1}}\rho^i$ and $P_m(K) = \frac{\rho^m/m!}{\sum_{i=0}^{K}\frac{\rho^i}{i!}}$; for $\rho = \frac{\lambda}{\mu} \neq 1$ and $0 \leq i \leq K$.

Derivation of above equations can be found in [89]. We consider the arrival rates λ for the normal and high data rate traffic are 3 and 6 per unit of time, respectively, while the service rate $\mu = 10$ is fixed. The number of users, K, varies from 0 to 50. For the M/M/m/K queue, the number of servers $m = 2$.

Figure 6.6 shows that high data rate (HDR) created by malicious users causes high blocking probability compared to normal data rate (NDR), and ineffective to maintain QoS level for more than 10 users. We can use multiple server with fixed upper bound of the data rate to resist the DoS attack, and to ensure the required QoS with an acceptable number of users.

eHealth care scenario: We consider two types of users, wired and wireless, are connected to the eHealth care service provider. The eHealth care provider is linked to the cloud server through a wired connection. We define two types of scenarios, normal scenario (NrS) and high-dense scenario (HdS), in our model. NrS consists of 5 mobile users and 3 users with wired connection. For the HdS, we just double the respective numbers.

Network simulation: Based on the theoretical analysis, we consider NrS, and HdS with single and duel server in our simulation. The performance metric used in our simulation is end-to-end delay, and all the wireless users are assumed to be in the access-point communication range. Table. 6.2 gives the different parameters used in our simulation.

Figure 6.7 shows the average end-to-end delay of the different scenarios using the ESPAC scheme.

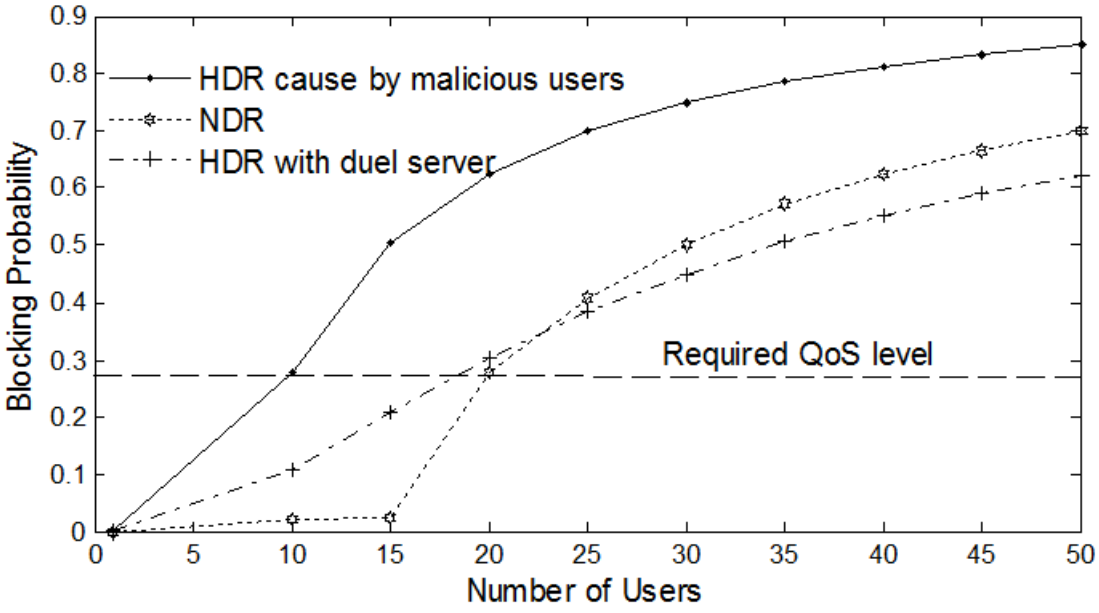

Figure 6.6: Queuing comparisons for the QoS requirements

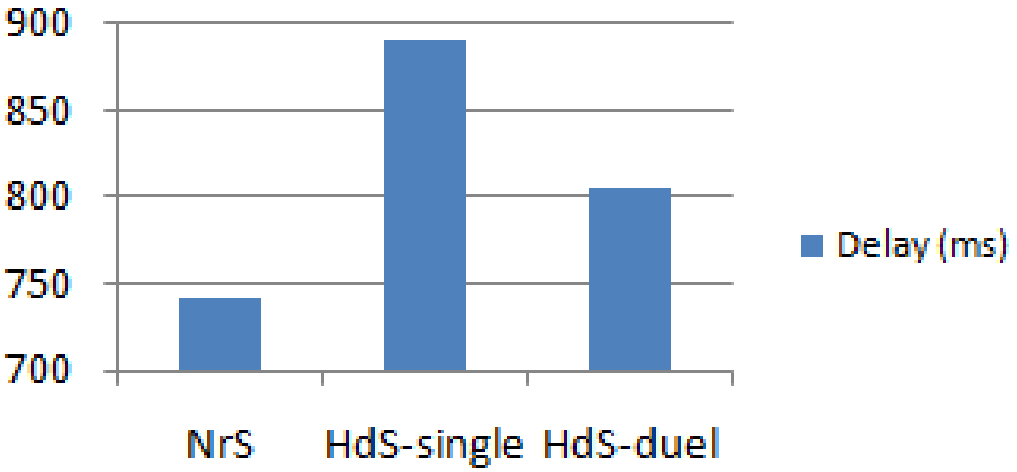

Figure 6.7: Comparison of average end-to-end delay

Table 6.2: Simulation Parameters

Simulation time	150 sec
Number of nodes	NrS [wireless 5, wired 3]
	HdS [wireless 10, wired 6]
Packet type	wireless-CBR, Wired-TCP
Packet size	512 bytes
Mobility	2-5 Km/hr [for wireless users]

Simulation results show that the average end-to-end delay of the proposed scheme is around 750 ms in a normal scenario and increases to 900 ms in a high-dense scenario, which is minimized to 800 ms by using the duel server. Based on the performance analyses, we can apply ESPAC scheme in a duel server mode to resist DOS attack and provide a high QoS level for users.

Key Storage Efficiency: Compared to the traditional access-control schemes, ESPAC's users do not need to store data requesters' IDs. In the initialization phase, TA computes the constant size PK and MK. Service providers or registered users only need to store the assigned attributes keys. Let, N is the average size of attributes and 'c' is the number of assigned attributes. Thus, the storage overhead is $\mathcal{O}(c\ logN)$. The proposed scheme ensures users' storage efficiency as they do not need to store data-requesters IDs for future access control. In a trusted environment, they may even release more storage space by storing the access-policy in the trusted service provider end.

6.8 M-ESPAC:Modified ESPAC for User Revocation and Audit

There is a drawback of our first proposed ESPAC scheme. If the data requester can submit all the attributes correctly, CP-ABE executes on the root node of the access tree and decrypt the encrypted PHI. This can open the door of potential privacy exposure, as the cloud can collide with data requester to get access to the PHI too. To perform user revocation, the cloud needs to re-encrypts all stored PHI with different access architecture. It costs a huge computation overhead to the cloud and increases the eHealth expenditure because cloud service provider (CSP) will demand more service cost to perform additional computation tasks. In addition, it is not practical to delegate all access control tasks to the third party CSP [87].

To solve the ESPAC's drawbacks as well as to incorporate cloud services to eHealth, we perform modification on ESPAC and propose a multi-parties proxy re-encryption scheme with CP-ABE named as M-ESPAC. In addition, proposed M-ESPAC ensures PHI owner, respective health service provider (HSP), and cloud service provider (CSP) participation to provide reliable, secure, and privacy preserving eHealth care system. In the modified proposed scheme, HSP can easily rebuild the PHI access architecture without doing any computation at the cloud site. As well as auditing of the stored PHI needs minimum computation.

6.8.1 Multi-parties Proxy Re-encryption Protocol

To ensure authentic patient-centric access control in a cloud environment where only a specific DAR can decrypt the encrypted PHI, we propose a multi-parties proxy re-encryption protocol. In our proposed protocol, the HSP and CSP are identified as multi-parties proxies and they share their secret keys to generate the re-encryption key. Re-encryption process performs such a way that neither HSP nor CSP can deny their involvement in the PHI access process, as well as only the specific DAR can decrypt the re-encrypted PHI. Fig. 6.8 shows the framework of proposed multi-parties proxy re-encryption protocol.

6.8.2 System Initialization

Given the security parameter S, the trusted authority HSP generates the bilinear parameters $(q, g, e, \mathbb{G}, \mathbb{G}_{\mathbb{T}})$ by the function $Gen(S)$. It also generates a secure hash function $H : (0,1)^* \rightarrow \mathbb{G}$. By using the available public security parameters, HSP and CSP choose random numbers $h \in_R \mathbb{Z}_q^*$ and $c \in_R \mathbb{Z}_q^*$ as there secret keys respectively and corresponding public keys are generated as $PK_{HSP} = g^h$ and $PK_{CSP} = g^c$. Each registered patient has a unique identity $U_i \in U$, $U = U_0..U_n$ is the set of patients enlisted to a HSP, and chooses a random number $x_i \in_R \mathbb{Z}_q^*$ as its private key. The patient then computes the public key as $PK_{U_i} = g^{x_i}$.

HSP computes patient pseudo-identity $PID_{U_i} = H(U_i)$ and constructs different access trees based on PHI privacy level. Fig. 6.2 shows possible access structure based on different privacy levels, where intermediate node work as a logic gate. For example, any DAR who knows location and gender, or gender and disease, or location and disease can get access to the privacy level-1 type of PHI as shown in Fig. 6.2(a). Patient chooses $\rho_{1..n} \in \mathbb{Z}_q^*$ as secret keys for different privacy levels' PHI and constructs respective access trees $\mathbb{A}_1..\mathbb{A}_n$, where

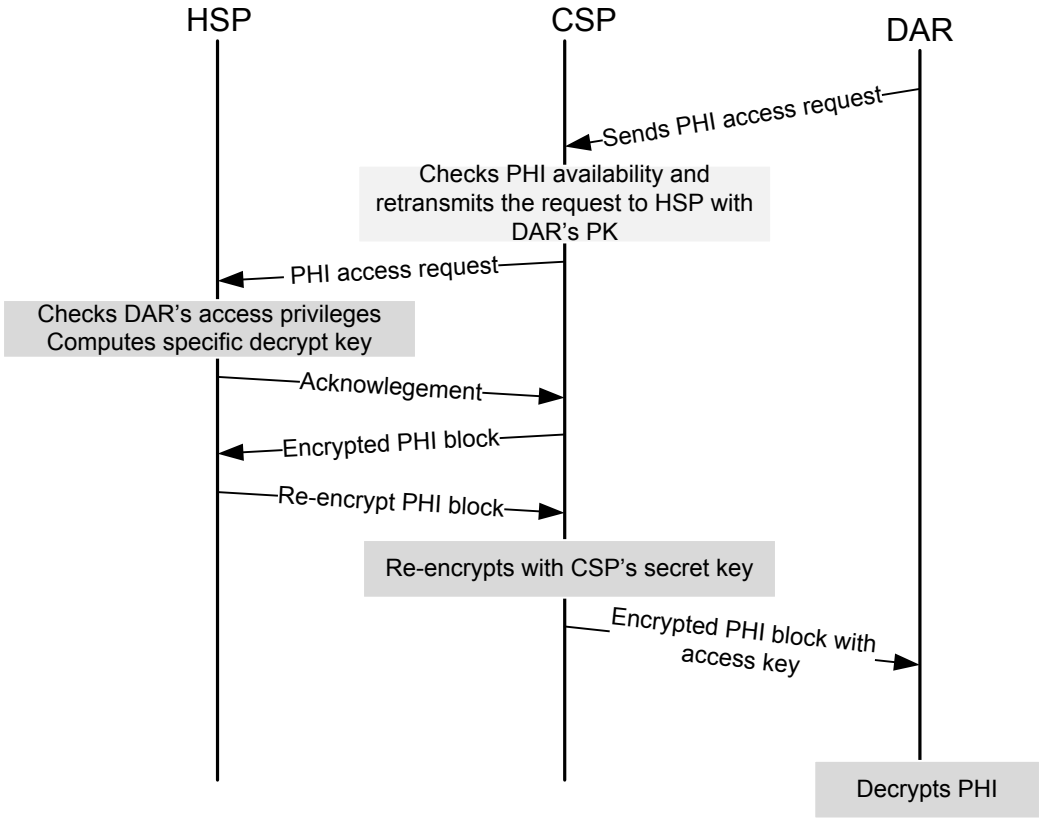

Figure 6.8: Framework of multi-parties proxy re-encryption protocol

the polynomial of the trees' root are set as $\rho_{1..n} \in \mathbb{Z}_q^*$. Secret keys are then encrypted by using the $Encrypt_2$ function described in ESPAC.

Trusted HSP maintains a secure records that contains patient's identity, pseudo identity, and secret keys for different privacy levels. In our proposed scheme, a set of PHI with different privacy levels form a PHI-block and the HSP signs on this block before sending to CSP for permanent storage. A sample PHI block structure is presented in Fig.6.9.

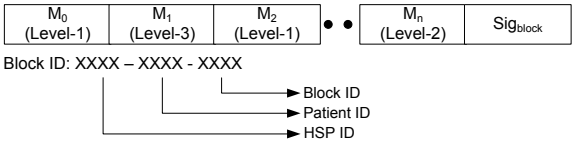

Figure 6.9: Sample PHI block architecture

6.8.3 Communication Between Patient and HSP

Step-1) Patient U_0 and HSP with private and public key pairs (x_0, g^{x_0}) and (h, g^h) compute first the shared key $K_{uH} = PK_{HSP}^{x_0} = PK_{U_0}^{h} = g^{hx_0}$. Patient U_0 encrypts the PHI 'm' as $E = m \times K_{uH}$ and signed the message as $Sig_E = PK_{HSP}^{\frac{1}{H(E||m||PID_{U_0})+x_0}}$. Patient then sends the encrypted PHI along with the digital signature to the specific HSP.

Step-2) After receiving the encrypted message E, and corresponding signature Sig_E, the HSP decrypts it as $m = E \times K_{uH}$ and check the validity of the signature as $e(Sig_E, g^{H(E||m||PID_{U_0})}.PK_{U_0}) \stackrel{?}{=} e(PK_{HSP}, g)$.

$$
\begin{aligned}
& e(Sig_E, g^{H(E||m||PID_{U_0})}.PK_{U_0}) \\
&= e(PK_{HSP}^{\frac{1}{H(E||m||PID_{U_0})+x_0}}, g^{H(E||m||PID_{U_0})+x_0}) \\
&= e(PK_{HSP}, g).
\end{aligned}
$$

6.8.4 PHI Encryption Based on Privacy

If the validity of the signature $Sign_E$ verified, the HSP encrypts the PHI 'm' according the patient's predefined privacy setting. Let HSP founds the decrypted PHI 'm' is a type of level-1. It then performs the following steps:

Step-3) Regenerates encryption key as $K = e(PK_{U_0}, g^{\frac{1}{h}})^{\rho_1} = e(g,g)^{\frac{\rho_1 \cdot x_0}{h}}$ and encrypts the PHI 'm' as $M_0 = K \times m$. HSP obtains the secret key ρ_1 from its secure record or obtains from the access tree.

Step-4) HSP signs the encrypted message M_0 as $Sig_M = PK_{CSP}^{\frac{1}{H(M_0||Message_{ID})+h}}$, here h is the secret key of the HSP and $Message_{ID}$ represents an unique identity of the message (adding message position with block ID).

Step-5) Stores $v_0 = H(M_0)$ temporally and sends M_0 and $Sign_M$ to the CSP. HSP performs step-3 and 4 for others PHI of a block.

Step-6) After successful transmitting of all the PHI of a block, HSP computes the block sign as $Sig_{block} = PK_{CSP}^{\frac{1}{v_0+V_1..+V_n+x_0+H(Block_{ID})}}$. Here, $V_0, .., V_n$ are the values of $H(M_0)..H(M_n)$ respectively.

6.8.5 Storing PHI at Cloud

CSP performs following steps before storing the patient's encrypted PHI at cloud.

Step-7) Checks the validity of the received encrypted PHI, M_0, by using the digital signature Sig_M as $e(Sig_M, g^{H(M_0||Message_{ID})}.PK_{HSP}) \stackrel{?}{=} e(PK_{CSP}, g)$
$e(Sig_M, g^{H(M_0||Message_{ID})}.PK_{HSP})$
$= e(PK_{CSP}^{\frac{1}{H(M_0||Message_{ID})+h}}, g^{H(M_0||Message_{ID})+h})$
$= e(PK_{CSP}, g)$.

Step-8) If the signature verified successfully, CSP computes $V_0 = H(M_0)$ and stores both M_0 and v_0 temporally. Steps 6 and 7 continue until all the encrypted PHI of a block $(M_0..M_n)$ are successfully received and verified.

Step-9) Check the validity of the Sig_{block} as $e(Sig_{block}, g^{V_0+..+V_n+H(Block_{ID})}.PK_{HSP}) \stackrel{?}{=} e(PK_{CSP}, g)$
$e(Sig_{block}, g^{V_0+..+V_n+H(Block_{ID})}.PK_{HSP})$
$= e(PK_{CSP}^{\frac{1}{v_0+V_1..+V_n+x_0+H(Block_{ID})}}, g^{V_0+..+V_n+H(Block_{ID})+x_0})$
$= e(PK_{CSP}, g)$.

Step-10) If step-9 performs successfully, CSP stores all the encrypted PHI and the corresponding Sig_{block} as shown in Fig.6.9.

6.8.6 PHI Access and Multi-parties Proxy Re-encryption

In this subsection, we define the steps those are needed by DAR, HSP, and CSP to get access to sensitive encrypted PHI.

Step-11) DAR sends access request to CSP with attributes set of a specific patient. CSP forwards attributes set along with DAR's public key to the HSP.

Step-12) HSP executes $AccessCheck()$ and $Decrypt_2()$ [83] to check the access privileges of the DAR. If the DAR can submit all the required attributes correctly, the function obtains the corresponding secret key ρ.

In our proposed scheme, HSP and CSP perform as multi parties proxies to re-encrypt the specific encrypted PHI which can only decrypt by the DAR.

proxy Re-encryption at HSP

HSP now computes a re-encryption key for the DAR, so that he can easily decrypt the re-encrypted PHI.

Step-13) Generates the re-encryption key as $\acute{K} = e(PK_{U_0}, PK_{DAR})^{\frac{\rho_1}{h}} = e(g,g)^{\frac{d \cdot x_0 \cdot \rho_1}{h}}$, here ρ_1 is the secret key of a specific PHI privacy level that obtains by the function $AccessCheck()$.

Step-14) HSP chooses a session key $s \in \mathbb{Z}_q^*$ and re-encrypts M_0 as $M = M_0 \times e(PK_{csp}, g)^s = M_0 \times e(g,g)^{c \cdot s}$

Step-15) Generates a shared key by using CSP's public key and HSP's secret key as described in step 1. Encrypts $\acute{K}$ and s using this shared key. HSP then signs on M as described in step-1.

Step-16) HSP transmits M, signature on M, encrypted $\acute{K}$, and s to CSP.

Proxy Re-encryption at CSP

In this stage, CSP first checks the validity of M (step-2)and generates the shared key using HSP's public key and CSP's secret key and decrypts the session key s (step-2).

Step-17) CSP re-encrypts M as $\acute{M} = \frac{M}{e(g,g)^{c \cdot s}}$. It then calculates shared key between CSP and DAR.

Step-18) By using the shared key, encrypts the key $\acute{K}$ and signs on $\acute{M}$ and transmits to DAR.

6.8.7 PHI access by DAR

Step-19) After receiving encrypted PHI $\acute{M}$ and signature, DAR checks the validity of the message as shown in step-2.

Step-20) DAR then decrypts the PHI as $\frac{M}{\acute{K}^{\frac{1}{d}}} = \frac{m \times e(g,g)^{\frac{\rho_0 \cdot x_0}{h}}}{e(g,g)^{\frac{d \cdot x_0 \cdot \rho_0}{h \cdot d}}} = m$

6.9 Audit of Stored PHI

In our proposed SPS scheme, trusted HSP can perform block or partial audit of stored encrypted PHI to ensure CSP performs as expected.

6.9.1 Partial Audit

HSP performs partial audit to minimize the computation and communication cost. In this case, HSP audits any PHI unit of a block and checks the validity with stored block signature Sig_{block}.

Step-1) HSP chooses a random PHI address from any data block. It then sends request message to the CSP to deliver the specific encrypted PHI, Hashed values of others PHI stored in the same block along with the block signature.

Let HSP asks for M_1 of a block. CSP computes $V_i = H(M_i)$, for all $i \neq 1$, where $i \in [0, n]$. Sends back computed hashed values, stored encrypted PHI M_1, and signature Sig_{block} to HSP.

Step-2) HSP now decrypts M_1, check the contents, encrypts again with the same privacy level's secret key and computes the hash value v_1. It then checks the validity of $sign_{block}$ as $e(Sign_{block}, \prod_{i=0}^{n} g^{v_i} \cdot g^{H(Block_ID)} \cdot g^{x_0}) \stackrel{?}{=} e(PK_{CSP}, g)$. If this challenge verified, HSP sends acknowledge message to CSP and terminates the partial auditing task.

Correctness:

$e(Sign_{block}, \prod_{i=0}^{n} g^{v_i} \cdot g^{H(Block_ID)} \cdot g^{x_0}) = e(PK_{CSP}^{\frac{1}{v_0+\ldots+V_n+H(Block_ID)+x_0}}, g^{v_0+..+v_n+H(Block_ID)+x_0}) = e(PK_{CSP}, g)$.

6.9.2 Block Audit

HSP requests for all encrypted PHI ($M_0..M_n$) of any random block. It then computes the hashed values $v_0..v_n$ and checks the validity of the block signature as shown in step-2 of partial audit subsection. By the block audit, HSP can assure correctness of the stored PHI block.

6.10 Summary

In this chapter, we have proposed a scheme,ESPAC, to achieve patient-centric access control with security and privacy by exploiting attribute-based encryption. Moreover ESPAC enables the eHealth care service provider to reduce the overall maintaining cost by moving data to a centralized storage or cloud storage for further processing and long-term storage. Moreover, storing PHIs in the cloud storage provides anytime, anywhere access to stored patient's health information. The proposed scheme also preserves user privacy with data integrity. Through detailed security and performance analyses, it has been demonstrated that the proposed scheme is highly efficient to resist various possible attacks and malicious behavior. We further modified ESPAC by introducing multi-parties proxy re-encryption and ensure participation of both HSP and CSP to grant access of encrypted PHI to a specific DAR.

Chapter 7

Conclusions and Future Work

In this chapter, we summarize our contributions in this thesis, propose our future research work, and give final remarks.

7.1 Conclusions

The major contributions of this thesis can be summarized as follows:

- First, we studied different PHI aggregation scenarios based on patient's location and summarized basic security and privacy requirements for eHealth applications. We then proposed a light-weight hybrid secure communication scheme for WBAN, where session key ensures body sensor reusability. Considering PDA as the gateway of WBAN, we then prioritized health care data packets and ensure QoS with acceptable security and privacy bindings.

- Second, we proposed a secure packet forwarding protocol,ASTP, based on mutual trust and integrated with trustworthiness to Agent, energy level, residential time, and priority to the same Agent's subscriber in a cooperative heterogeneous network. The proposed protocol works in a cooperative social environment, where other cooperative users help to establish a secure communication link between care giver and end user. The ASTP protocol can remarkably increase the average packet delivery ratio and achieve excellent efficiency to be used in an eHealth application. Power efficiency at the user level is maintained by computing major calculation at the Agent side. User privacy is ensured using pseudo identity. Fairness is achieved by providing incentive

to the cooperative intermediate routing nodes. Through detailed security analyses, it has been demonstrated that the ASTP is highly effective to resist various possible security attacks and malicious behavior.

- Third, we proposed a delay-tolerant secure long-term health care system, RuralCare, for monitoring patients located at the rural-area. RuralCare ensures secure and privacy preserving data aggregation using body sensors in WBAN environment and vehicles as cooperative relay nodes. It describes data forwarding steps from the patient's end to the care-giver's end and achieves different security and privacy requirements. The fairness among all cooperative participants in RuralCare is guaranteed by adopting proper incentive and reputation policies. These policies also improve the network performance in terms of high delivery ratio and low average delay. Through extensive security and performance analyses, it has been demonstrated that RuralCare is highly effective to resist possible security attacks and efficient to provide emerging health care to patient resides at the rural area.

- Fourth, we proposed secure and efficient PHI sharing schemes (ESPAC and M-ESPAC) in a cloud computing environment. Proposed schemes ensure patient-centric access control by exploiting attribute-based encryption. Moreover, overall maintaining cost is minimized by performing less computation at the cloud side. ESPAC and M-ESPAC preserve patient's identity privacy and data integrity. Proposed multi-parties proxy re-encryption protocol ensured participation from both HSP and CSP to grant access of encrypted PHI for a specific DAR. Stored PHI correctness is maintained by block-auditing that can be performed by the TA.

7.2 Future Work

Our research has already made significant progress in secure eHealth care applications. However, since cloud storage and delay tolerant network using vehicular social network are the promising platform for PHI storage and providing health care to rural area, there still exist several research direction to be explored to complement this thesis. Therefore, the following two research topics will be investigated as a continuation of my Ph.D. thesis work.

- Searching on encrypted stored PHI: In a continuous health monitoring system, a large amount of PHI are going to be stored at the cloud side frequently. Due to the sensitiveness of the stored PHI, care giver would like to encrypt the PHI to ensure

access restriction. However, this large amount of data is very much valuable to the health workers, researchers, pharmacist, or care givers. They would like to perform different search queries and the system should allow them to have an advancement in health care industry. Therefore, as one of our future research work for cloud storage, we will propose an access policy with general search option on encrypted PHI.

- Supporting reputation-based trust in Vehicular Social Networks: In a Delay tolerant network, participant vehicles could maintain a blacklist which is helpful for selecting nearby trusted peers. In addition, the vehicles are more likely to share their blacklists with others in vehicular social networks. Then, the black-list can be considered as trust value and minimize the number of malicious relay nodes.

7.3 Final Remarks

In this thesis, we have presented a suite of security and privacy-preserving protocols for secure eHealth care system. In addition, we have also identified two future research topics to complement of this thesis. To facilitate our research accomplishments and findings to benefit the real world situations, we will carry out experiments to further confirm our research findings.

Author's Publications

Journal and Magazine Papers

1. **M. Barua**, X. Liang, R. Lu, and X. Shen, "RCare: Extending Secure Health Care to Rural Area Using VANETs, ACM Mobile Networks and Applications (MONET), to appear

2. K. Zhang, X. Liang, **M. Barua**, R. Lu, and X. Shen, "PHDA: A Priority Based Health Data Aggregation with Privacy Preservation for Cloud Assisted WBANs", Information Sciences (Elsevier) to appear.

3. X. Liang, X. Li, **M. Barua**, L. Chen, R. Lu, X. Shen, and H. Luo, "Enable Pervasive Healthcare through Continuous Remote Health Monitoring", IEEE Wireless Communications, Vol. 19, No. 6, pp. 10-18, 2012.

4. X. Liang, **M. Barua**, R. Lu, X. Lin, and X. Shen, "HealthShare: Achieving Secure and Privacy-preserving Health Information Sharing through Health Social Networks", Computer Communications (Elsevier)- special issue on Smart and Interactive Ubiquitous Multimedia Services, Vol. 35, Issue 15, pp. 1910-1920, 2012.

5. X. Liang, **M. Barua**, R. Lu, and X. Shen, "Privacy-preserving Wireless Data Transmission for e-Healthcare Applications", IEEE COMSOC MMTC E-Letter - Special Issue on 3D DATA EVALUATION, RETRIEVAL AND PRIVACY, Vol. 6, No. 11, pp. 39-41, 2011.

6. **M. Barua**, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in Cloud Computing", Int. J. of Security and Networks (IJSN). Vol. 6, Nos. 2/3, pp. 67-76, 2011.

Conference Papers

1. **M. Barua**, R. Lu and X. Shen, "SPS: Secure Personal Health Information Sharing with Patient-centric Access Control in Cloud Computing", Proc. IEEE Globecom'13, Atlanta, GA, USA, Dec. 9-13, 2013.

2. **M.Barua**, M. Mahmoud, and X. Shen, "Agent-based Secure and Trustworthy Packet-Forwarding Protocol for eHealth, IEEE GLOBECOM, Houston, Texas, USA, Dec. 5-9, 2011.

3. **M.Barua**, R. Lu, and X. Shen, "Health-Post: A Delay-Tolerant Secure Long-Term Health Care Scheme in Rural Area, IEEE GLOBECOM, Houston, Texas, USA, Dec. 5-9, 2011.

4. M. Mahmoud, **M. Barua**, and X. Shen, "SATS: Secure Data-Forwarding Scheme for Delay-Tolerant Wireless Networks, IEEE GLOBECOM, Houston, Texas, USA, Dec. 5-9, 2011.

5. **M. Barua**, X. Liang, R. Lu, and X. Shen, "PEACE: An Efficient and Secure Patient centric Access Control Scheme for eHealth Care System, Proc. IEEE INFOCOM11-SCNC, Shanghai, China, April 10-15, 2011

6. **M. Barua**, Md. S. Alam, X. Liang, and X. Shen, "Secure and Quality of Service Assurance Scheduling Scheme for WBAN with Application to eHealth, Proc. IEEE WCNC11, Cancun, Quintana-Roo, Mexico, March 28-31, 2011.

Bibliography

[1] J. H. U. Partners for Solutions and the Robert Wood Johnson Foundation, "Chronic conditions:making the case for ongoing care." http://www.partnershipforsolutions.org/DMS/files/chronicbook2004.pdf, 2004.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, CCS '06, (New York, NY, USA), pp. 89–98, ACM, 2006.

[3] R. J. Romanow, "Building on values: the future of health care in canada - final report." http://publications.gc.ca/collections/Collection/CP32-85-2002E.pdf, 2003.

[4] "The publication population projections for canada, provinces and territories, 2005 to 2031." http://www.statcan.gc.ca/daily-quotidien/051215/dq051215b-eng.htm, 2005.

[5] R. Madan, N. Mehta, A. Molisch, and J. Zhang, "Energy-efficient decentralized cooperative routing in wireless networks," *Automatic Control, IEEE Transactions on*, vol. 54, pp. 512 –527, march 2009.

[6] K. Wang and M. Wu, "Cooperative communications based on trust model for mobile ad hoc networks," *Information Security, IET*, vol. 4, pp. 68 –79, june 2010.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*, (San Diego, CA, USA), pp. 1 –9, march 2010.

[8] S. Ting, S. Kwok, A. Tsang, and W. Lee, "Critical elements and lessons learnt from the implementation of an rfid-enabled healthcare management system in a medical

organization," *Journal of Medical Systems*, pp. 1–13, 2009. 10.1007/s10916-009-9403-5.

[9] "Health insurance portability and accountability act." http://www.hhs.gov/ocr/privacy/, 1996.

[10] "The american recovery and reinvestment act and health information technology for economic and clinical health act." http://www.ahima.org/advocacy/arrahitech.aspx#difference, 2009.

[11] S. Ramli, R. Ahmad, M. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (wban)," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pp. 998–1001, Jan 2013.

[12] H. Wang, H. Fang, L. Xing, and M. Chen, "An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks (wban)," in *Communications (ICC), 2011 IEEE International Conference on*, pp. 1–5, June 2011.

[13] J. Chaudhry, U. Qidwai, R. Rittenhouse, and M. Lee, "Vulnerabilities and verification of cryptographic protocols and their future in wireless body area networks," in *Emerging Technologies (ICET), 2012 International Conference on*, pp. 1–5, Oct 2012.

[14] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ecc algorithm for patient's medical information in healthcare system," in *Information Networking (ICOIN), 2014 International Conference on*, pp. 453–457, Feb 2014.

[15] C. soon Jang, D.-G. Lee, and J.-W. Han, "A proposal of security framework for wireless body area network," in *Security Technology, 2008. SECTECH '08. International Conference on*, pp. 202–205, Dec 2008.

[16] M. Mahmoud and X. Shen, "Esip: Secure incentive protocol with limited use of public-key cryptography for multi-hop wireless networks," *Mobile Computing, IEEE Transactions on*, 2010.

[17] M. E. Mahmoud and X. Shen, "Stimulating cooperation in multi-hop wireless networks using cheating detection system," in *INFOCOM'10: Proceedings of the 29th conference on Information communications*, (Piscataway, NJ, USA), pp. 776–784, IEEE Press, 2010.

[18] Z. Wang, C. Li, and Y. Chen, "Local cooperative relay for opportunistic data forwarding in mobile ad-hoc networks," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 5381–5386, June 2012.

[19] X. Liang, X. Li, T. Luan, R. Lu, X. Lin, and X. Shen, "Morality-driven data forwarding with privacy preservation in mobile social networks," *Vehicular Technology, IEEE Transactions on*, vol. 61, pp. 3209–3222, Sept 2012.

[20] D. Zhao, H. Ma, S. Tang, and X. Li, "Coupon: A cooperative framework for building sensing maps in mobile opportunistic networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2014.

[21] K. Kinsella and W. He, "An aging world:2008, u.s. census bureau." http://www.census.gov/prod/www/abs/p95.html, 2008.

[22] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22, pp. 847–859, May 2011.

[23] J.-S. Wang, C.-H. Liu, and G. Lin, "How to manage information security in cloud computing," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*, pp. 1405–1410, Oct 2011.

[24] Z. Chen, F. Han, J. Cao, X. Jiang, and S. Chen, "Cloud computing-based forensic analysis for collaborative network security management system," *Tsinghua Science and Technology*, vol. 18, pp. 40–50, Feb 2013.

[25] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *Network and Service Management, IEEE Transactions on*, vol. 11, pp. 60–75, March 2014.

[26] H. Wang, S. Wu, M. Chen, and W. Wang, "Security protection between users and the mobile media cloud," *Communications Magazine, IEEE*, vol. 52, pp. 73–79, March 2014.

[27] G. Yan, D. Wen, S. Olariu, and M. Weigle, "Security challenges in vehicular cloud computing," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 14, pp. 284–294, March 2013.

[28] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *Communications Surveys Tutorials, IEEE*, vol. 15, pp. 843–859, Second 2013.

[29] R. Lu, X. Li, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *Vehicular Technology, IEEE Transactions on*, vol. 61, pp. 86–96, Jan 2012.

[30] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, (London, UK), pp. 213–229, Springer-Verlag, 2001.

[31] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography* (K. Nyberg and H. Heys, eds.), vol. 2595 of *Lecture Notes in Computer Science*, pp. 310–324, Springer Berlin Heidelberg, 2003.

[32] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," *Journal of Cryptology*, vol. 21, pp. 149–177, 2008. 10.1007/s00145-007-9005-7.

[33] M. Al Ameen, J. Liu, and K. Kwak, *Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications*. Springer Netherlands.

[34] D. Vergados, D. Vergados, and I. Maglogiannis, "Ngl03-6: Applying wireless diffserv for qos provisioning in mobile emergency telemedicine," in *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, pp. 1 –5, nov. 2006.

[35] J. Iqbal, Nizamuddin, N. Amin, and A. Umar, "Authenticated key agreement and cluster head selection for wireless body area networks," in *Information Assurance (NCIA), 2013 2nd National Conference on*, pp. 113–117, Dec 2013.

[36] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and security in wireless body area network infrastructures," in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pp. 3837–3840, 2005.

[37] K. M. Sharmilee, R. Mukesh, A. Damodaram, and V. Subbiah Bharathi, "Secure wban using rule-based ids with biometrics and mac authentication," in *e-health Networking, Applications and Services, 2008. HealthCom 2008. 10th International Conference on*, pp. 102–107, July 2008.

[38] S. Sridharan and G. Kiran, "Secure authentication model for online health monitoring system," in *Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on*, pp. 1–5, July 2013.

[39] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in *INFOCOM*, pp. 2838–2846, 2010.

[40] Z. Qin, Z. Jia, and X. Chen, "Fuzzy dynamic programming based trusted routing decision in mobile ad hoc networks," in *5th IEEE International Symposium on Embedded Computing (SEC '08)*, pp. 180 –185, oct. 2008.

[41] A. Pushpa, "Trust based secure routing in aodv routing protocol," in *IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, pp. 1 –6, dec. 2009.

[42] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *INFOCOM*, pp. 632–640, 2010.

[43] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *Selected Areas in Communications, IEEE Journal on*, vol. 27, pp. 387 –399, may. 2009.

[44] J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *Wireless Communications, IEEE*, vol. 17, pp. 66 –73, feb. 2010.

[45] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *Selected Areas in Communications, IEEE Journal on*, vol. 27, pp. 365 –378, may. 2009.

[46] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic, and S. Khan, "Timestamp authentication protocol for remote monitoring in ehealth," in *2nd International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth 2008)*, pp. 73 –76, jan. 2008.

[47] B. De Decker, M. Layouni, H. Vangheluwe, and K. Verslype, "A privacy-preserving ehealth protocol compliant with the belgian healthcare system," in *Public Key Infrastructure* (S. Mjlsnes, S. Mauw, and S. Katsikas, eds.), vol. 5057 of *Lecture Notes in Computer Science*, pp. 118–133, Springer Berlin / Heidelberg, 2008.

[48] L. B. Oliveira, D. F. Aranha, C. P. Gouva, M. Scott, D. F. Cmara, J. Lpez, and R. Dahab, "Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer Communications*, vol. 34, no. 3, pp. 485

– 493, 2011. Special Issue of Computer Communications on Information and Future Communication Security.

[49] L. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, "Tinytate: Computing the tate pairing in resource-constrained sensor nodes," in *Network Computing and Applications, 2007. NCA 2007. Sixth IEEE International Symposium on*, pp. 318 –323, july 2007.

[50] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '02, (London, UK, UK), pp. 354–368, Springer-Verlag, 2002.

[51] "Intel px27x processor electrical, mechanical, and thermal specification." http://www.intel.com/design/pca/applicationsprocessors/manuals/278780.htm.

[52] R. Zhu, G. Yang, and D. Wong, "An efficient identity-based key exchange protocol with kgs forward secrecy for low-power devices," *Internet and Network Economics*, vol. 3828, pp. 500–509, 2005.

[53] X. Lin, R. Lu, and X. Shen, "Mdpa: multidimensional privacy-preserving aggregation scheme for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 10, pp. 843–856, 2010.

[54] "List of battery sizes." http://en.wikipedia.org/wiki/List_of_battery_sizes, 2011.

[55] K. R. M. N. Halgamuge, M. Zukerman and H. L. Vu, "An estimation of sensor energy consumption," vol. 12, pp. 259–295, 2009.

[56] M. Barua, M. S. Alam, X. Liang, and S. Shen, "Secure and quality of service assurance scheduling scheme for WBAN with application to ehealth," in *IEEE WCNC 2011 - Network*, (Cancun, Mexico), 3 2011.

[57] M. Yoshitomi, T. Takagi, S. Kiyomoto, and T. Tanaka, "Efficient implementation of the pairing on mobilephones using brew," *IEICE - Trans. Inf. Syst.*, vol. E91-D, no. 5, pp. 1330–1337, 2008.

[58] R. Lu, X. Lin, H. Zhu, C. Zhang, P.-H. Ho, and X. Shen, "A novel fair incentive protocol for mobile ad hoc networks," in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, 31 2008.

[59] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling security and patient-centric access control for ehealth in cloud computing," *International Journal of Security and Networks*, vol. 6, pp. 67–76, Nov 2011.

[60] D. Niyato, E. Hossain, and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 412 –423, May 2009.

[61] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *Selected Areas in Communications, IEEE Journal on*, vol. 27, pp. 365 –378, may 2009.

[62] M. Masi, R. Pugliese, and F. Tiezzi, "A standard-driven communication protocol for disconnected clinics in rural areas," in *IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, pp. 304 –311, june 2011.

[63] A. Doorenbos, A. Kundu, L. Eaton, G. Demiris, E. Haozous, C. Towle, and D. Buchwald, "Enhancing access to cancer education for rural healthcare providers via telehealth," *Journal of Cancer Education*, vol. 26, pp. 682–686, 2011.

[64] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in *INFOCOM, 2012 Proceedings IEEE*, pp. 388 –396, march 2012.

[65] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, pp. 1 –6, 2010.

[66] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 8, pp. 4628 –4639, 2009.

[67] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 4, pp. 1483 –1493, 2010.

[68] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in dtns," in *Network Protocols, 2008. ICNP 2008. IEEE International Conference on*, pp. 238 –247, 2008.

[69] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Appa: Aggregate privacy-preserving authentication in vehicular ad hoc networks," in *Information Security* (X. Lai, J. Zhou, and H. Li, eds.), vol. 7001 of *Lecture Notes in Computer Science*, pp. 293–308, Springer Berlin/ Heidelberg, 2011.

[70] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *IEEE Vehicular Technology Conference*, pp. 2036 –2040, may 2008.

[71] A. Ramachandran, Z. Zhou, and D. Huang, "Computing cryptographic algorithms in portable and embedded devices," in *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*, (Orlando, Florida), pp. 1 –7, May 2007.

[72] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Proceedings of the 14th international conference on Financial cryptograpy and data security*, FC'10, (Berlin, Heidelberg), pp. 136–149, Springer-Verlag, 2010.

[73] M. Johnson, "Data hemorrhages in the health-care sector," in *Financial Cryptography and Data Security* (R. Dingledine and P. Golle, eds.), vol. 5628 of *Lecture Notes in Computer Science*, pp. 71–89, Springer Berlin / Heidelberg, 2009.

[74] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP '07. IEEE Symposium on*, pp. 321 –334, May 2007.

[75] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," in *Mobile Networks and Applications*, pp. 1–12, Springer Netherlands, 2010.

[76] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *Selected Areas in Communications, IEEE Journal on*, vol. 27, pp. 365 –378, May 2009.

[77] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology EUROCRYPT 2005* (R. Cramer, ed.), vol. 3494 of *Lecture Notes in Computer Science*, pp. 557–557, Springer Berlin / Heidelberg, 2005.

[78] X. Liang, R. Lu, X. Lin, and X. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *AHIC 2010*, (Kitchener, Ontario, Canada), pp. 1–5, 2010.

[79] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 268 –275, july 2010.

[80] J. Luna, M. Dikaiakos, M. Marazakis, and T. Kyprianou, "Data-centric privacy protocol for intensive care grids," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 14, pp. 1327 –1337, nov. 2010.

[81] Q. Liu, G. Wang, and J. Wu, "Efficient sharing of secure cloud storage services," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pp. 922 –929, july 2010.

[82] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, (New York, NY, USA), pp. 735–737, ACM, 2010.

[83] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling security and patient-centric access control for ehealth in cloud computing," *International Journal of Security and Networks*, vol. 6, pp. 67–76, Nov 2011.

[84] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[85] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214–1221, 2011.

[86] Z. Wan, J. Liu, and R.-H. Deng, "Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743–754, 2012.

[87] P. K. Sinha, G. Sunder, P. Bendale, M. Mantri, and A. Dande, *Electronic Health Record: Standards, Coding Systems, Frameworks, and Infrastructures*. Wiley-IEEE Press, 2012.

[88] J. Bethencourt, A. Sahai, and B. Waters, "Advanced crypto software collection, ciphertext-policy attribute-based encryption." http://acsc.cs.utexas.edu/cpabe/, 2011.

[89] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. NY,USA: Springer, 2010.