Design of a Secure Framework for the Implementation of Telemedicine, eHealth, and Wellness Services

Master Thesis

Script number: 557

Drake Patrick Mirembe

July 11, 2006

Radboud University Nijmegen
Security of Systems
Supervisors: Dr. Martijn Oostdijk
Dr. Perry Groot

I dedicate this work to my beloved parents, fiancee, and siblings.

Abstract

In both developing and developed countries, the costs of delivering health care are increasingly taking a large proportion of the national gross domestic product (GDP). GDP, is one of several measures of the size of a regions' economy. While developed countries have a good doctor to patient ratio, in developing countries the ratios are alarming (e.g., in Uganda it is about 1 doctor to 24.725 patients). Thus, with the advent of Information Communication Technologies (ICT), researchers are working on ways of using ICT to deliver health care services at low costs. This has led to the development of proprietary Telemedicine, Ehealth, and Wellness (TEW) systems. Because most developments are proprietary, standards are fluid and this rises questions about interoperability. Besides, the application of ICT to remotely collect and disseminate information in a sensitive domain like health care, rises a number of security related issues especially for TEW systems that rely on wireless sensor networks (WSNs) for data acquisition and transmission (i.e., questions about data confidentiality, system reliability, user authentication, and data integrity arise). Therefore, in this thesis we investigate a number of TEW systems, analyse their technologies and security implementations. Our investigation led us to conclude that most of the wireless sensor based TEW developments have focused on engineering issues of making the technology work at the expense of security. We learn that even those systems that have implemented good security mechanisms may not have modeled appropriate threats. Hence, we present a threat model of TEW-WSNs and propose a polynomial based key management scheme to secure TEW wireless sensor networks. We give conclusions about the application of TEW systems in developing countries and the future trends.

Acknowledgements

I would like to thank Dr. Martijn Oostdijk and Dr. Perry Groot for their direction, assistance, and guidance. Indeed, without them this thesis would not have been possible. Special thanks go to Dr. Dick van Leijenhorst for the great insights in the fields of complexity theory and cryptography. I also wish to register my appreciation to Nicole el Moustakim, Drs. G.F.M. Paulussen, and the staff of external relations office for all the encouragement and assistance. A word of thanks also goes to my student colleagues who helped me in many ways.

I register my gratitude to NUFFIC and the coordinators of the ICT capacity building project in Uganda and in The Netherlands for giving me the opportunity of realising my dream.

Finally, words alone cannot express the thanks I owe to Martha Hope, for being there for me whenever I needed a word of encouragement.

Contents

1 Introduction **3**

1.1 Motivation . . . 4

1.2 TEW system security requirements . . . 4

1.3 Typical application scenario . . . 5

2 Related work **7**

2.1 General framework . . . 7

2.2 The Ipath telemedicine platform . . . 8

2.2.1 Ipath services . . . 9

2.2.2 Architecture of Ipath . . . 9

2.2.3 Ipath technologies . . . 10

2.2.4 Ipath security implementation . . . 10

2.3 OpenEMed telemedicine system . . . 10

2.3.1 OpenEmed services . . . 11

2.3.2 OpenEmed architecture . . . 11

2.3.3 OpenEmed technologies . . . 12

2.3.4 OpenEmed security implementation . . . 12

2.4 TeleCardio-FBC . . . 13

2.4.1 TeleCardio-FBC architecture . . . 13

2.4.2 TeleCardio-FBC technologies . . . 13

2.4.3 System security implementation . . . 14

2.5 Wireless Body Area Sensor Network . . . 14

2.5.1 WBASN architecture . . . 14

2.5.2 WBASN technologies . . . 14

2.5.3 WBASN security . . . 15

2.6 CodeBlue system . . . 15

2.6.1 CodeBlue architecture . . . 16

2.6.2 CodeBlue technologies . . . 16

2.6.3 CodeBlue security . . . 16

2.7 Medintegra Web suite . . . 17

2.7.1 Medintegra Web architecture . . . 17

2.7.2 Medintegra Web technologies . . . 17

2.7.3 Medintegra Web security . . . 18

2.8 Conclusions . . . 18

3 Wireless Sensor Networks 21
3.1 Motivation 21
3.2 General overview 21
3.3 WBASN approach 22
3.4 CodeBlue approach 24
3.5 General WSN security approaches 25
3.6 Conclusions 27

4 A secure and optimal KMS for TEW-WSNs 29
4.1 Motivation and problem 29
4.2 Related work 30
4.2.1 Conclusions 32
4.3 TEW-WSNs threat model 33
4.3.1 Home monitoring threats 33
4.3.2 Mobile monitoring threats 34
4.3.3 Threat model discussion 34
4.4 Proposed TEW-WSNs KMS 36
4.4.1 TEW-WSN KMS requirements 36
4.4.2 Polynomial solution justification 37
4.4.3 Key material 38
4.4.4 Key agreement and distribution 38
4.4.5 Key revocation 40

5 Theoretical performance estimates 43
5.1 Theoretical resiliency estimates 43
5.1.1 Related work 43
5.1.2 TEW-WSNs KMS resiliency estimates 44
5.2 Resource requirement estimates 44
5.2.1 Memory requirement estimates 45
5.2.2 Computational estimates 46
5.2.3 Communication estimates 46

6 Reflections and conclusions 49
6.1 Reflections 49
6.2 Conclusions 51

Bibliography 55

List of Figures

1.1 Thesis structure 6

2.1 TEW system general framework 8

2.2 Ipath architecture 10

2.3 OpenEMed Architecture *(Adopted from [Forslund, 2006])* 12

2.4 WBASN architecture *(Adopted from [Otto* et al.*, 2006])* 15

3.1 The structure of a generic sensor 22

3.2 A generic wireless sensor network topology 22

3.3 The WBASN Zigbee compliant protocol 23

3.4 CodeBlue operation 25

4.1 Attack topology 34

4.2 TEW-WSN KMS attack tree 35

5.1 Zigbee compliant packet structure 45

List of Tables

2.1 TEW systems services 19

2.2 TEW Technologies 19

2.3 TEW systems security implementations 20

2.4 TEW systems remarks 20

Summary

In this thesis we explore the current technological and security developments in Telemedicine, Ehealth, and Wellness (TEW) systems. We review a number of TEW systems and highlight their technologies, services, deployment architectures, and security implementations. From the review we construct a framework that can be used to describe any TEW system. In our framework, we categorise TEW systems into two: Patient Record management Systems (PRSs) and Patient Health remote monitoring Systems (PHSs).

We focus our research on PHSs because of their unique features (i.e., new technologies, lack of standards, stringent user requirements, varying degrees of threats, and resource constraints on some components). We seek to answer a number of questions: (1) What are the challenges of securing TEW systems that rely on wireless sensors for data acquisition and transmission? (2) What are the different approaches and standards that are being adopted? (3) What is the appropriate threat model for TEW wireless sensor networks? (4) How can TEW systems be adopted to the infrastructure of developing countries?

We present an overview of wireless sensor networks (WSNs) in general and in the context of TEW systems i.e., PHSs. We discuss the current approaches to securing WSNs and highlight a number of challenges that still require further exploration. We observe that, although security is a very important component of TEW systems in general and TEW-WSNs in particular, most of the current developments have focused on making the technology work at the expense of security. Hence, a number of issues like channel congestion, secure and optimal key management, secure routing, system reliability, and optimal threat modelling still needs more attention. Therefore, we present a realistic threat model for TEW-WSNs home and mobile applications and propose a secure and optimal polynomial based key management scheme.

Our scheme provides a mechanism of revoking compromised keys based on a reputation of a sensor as determined by its neighbours and the personal server. Based on theories of performance measurement, we estimate the security guarantee and resource requirements of our scheme. Also, we give conclusions about the application of TEW services in developing countries and the future work.

1

Introduction

Telemedicine, Ehealth, and Wellness (TEW) services are a means to providing medical and wellness services remotely by using Information Communication Technologies (ICT). These systems can be used in all phases of the primary health care process: from prevention and tele-diagnosis to treatment and tele-homecare. Besides, in countries where the ratio of doctor to patient is one-to-thousands, or health centres and hospitals are hundreds of miles from patient's homes, these systems come in handy as they allow timely access to quality health services like tele-monitoring, tele-diagnosis, and e-prescription at low costs leading to improved quality of life of citizens and greater economic productivity.

The recent advances in wireless, semiconductor, integrated circuit, and sensor technologies have stimulated the interest of ICT researchers to define ways of applying these technologies in the medical field to improve service delivery at lower costs. For the case of developed countries, TEW systems have captured the interest of the government as a cost-saving means of improving access to quality healthcare. Examples of these projects include: the Ipath project[1], the Yale Telemedicine centre[2], OpenEMed[3], CodeBlue[4], Wireless Body Area Sensor Network (WBASN)[5], Mobile telemedicine India[6], MIThril[7], and Biotronik home monitoring system.[8] Although these systems can have a positive impact on the quality of health service delivered to a patient, some people justifiably are not at ease with the remote collection, access, and transmission of patient

[1] http://www.ipath.ch/site

[2] http://www.yale.edu/omnibus/Dec95/telemedicine.html

[3] http://www.openemed.org

[4] http://www.eecs.harvard.edu/ mdw/proj/codeblue/

[5] http://www.ece.uah.edu/ jovanov/whrms/

[6] http://www.telemedicineindia.com/index.htm

[7] http://www.media.mit.edu/wearables/mithril/

[8] http://www.biotronik.com/content/detail.php?id=1799

data over electronic networks. Besides privacy concerns, some sceptics of these technologies have moral and ethical concerns as well. In this thesis we focus on privacy concerns.

1.1 Motivation

In our preliminary investigation, we observed that most TEW initiatives have mainly focused on developing efficient applications for delivery of health care services at the expense of designing robust secure systems. This has led to "let the technology work first" syndrome. Nevertheless, we believe, security should be core to the design of any TEW system. We also learnt from the literature that, most of the current security developments have focused on the needs of in hospital patient systems at the expense of remote monitoring systems. Therefore, there is a need to understand the security threats that mobile and home TEW applications face and design means to mitigate these threats. It is also clear to us that most of the TEW advancements has focused on the needs of developed countries and given the infrastructure imbalances. Adopting these technologies to serve the needs of developing countries requires more research, hence, this thesis. Our work seeks to answer a number of questions which include:

- In TEW systems, patient data is remotely collected electronically transmitted over wireless communication channels and the Internet. These operations raise questions of how authentication of users is done and how integrity and confidentiality of data are maintained.
- What are the challenges of securing TEW systems that rely on Wireless Sensor Networks (WSNs) for data acquisition? and given the numerous research initiatives, what are the different approaches and standards being adopted?
- What is the appropriate threat model for TEW-WSN based systems for home and mobile applications?
- The ICT infrastructure development in most developing countries still lags behind that of the developed world. Thus, how can we adopt secure TEW systems to this infrastructure?

1.2 TEW system security requirements

In general, any health system must comply with a number of local and international standards. The used standards used most often are HL7[9] and HIPAA.[10] By complying to these standards, the following security services will have implicitly been delivered by the system: (1) *Data confidentiality*, the protection of data from unauthorised readers. (2) *Data integrity*, the assurance that the data received is the exact data that was sent by a legitimate sender. (3) *Authentication*, the assurance that the communicating entity is the one that it claims to be. (4) *Non-repudiation*, an assurance that entities cannot deny having participated in the communication. (5) *Message freshness*, an assurance that the current message is not an older message relayed by an adversary.

[9] http://hl7.org

[10] http://hipaa.org

1.3 Typical application scenario

In a typical TEW application scenario, a patient wears a few on-body sensors, which collect and relay their data in real time or near real time to the Personal Server (PS), which is implemented on a smart phone or Personal Digital Assistant (PDA). The PS aggregates this data and forwards it to the care provider's medical server via the Internet or a mobile communication network (e.g., GSM). The care provider accesses this data in real time using a PDA or a smart phones or off-line using normal end user terminals like a Personal Computer (PC).

This application may be extended to include a group-ware tool to enable medical personnel to consult each other or even experts in the field on the given case. The group-ware capability illustrates the exchange of data among medical personnel as another application scenario.

Hypothetical case 1 *To put this scenario into perspective, we present a hypothetical case study of a stroke patient under rehabilitation, whom we shall call Jack. Jack is recovering from a stroke and his physician has prescribed to him a routine behaviour pattern involving moments of rest and exercises. Jack lives with his family of five people in an apartment located in a busy neighbourhood. Jack is required to wear a few tiny sensors for at least 15 hours a day to enable his physician to receive up to the minute updates on his health via his smart phone. As part of his routine exercise, Jack normally takes an evening walk every day around his busy neighbourhood. On weekends, Jack joins his family for weekend shopping and other family activities. At times, Jack uses public transport to visit his friends and siblings in a nearby city on his own. Jack's mobility and public life places his ambulatory system at risk of both logical and physical attacks.*

This research focuses on the privacy and security features of the various technologies integrated in the current TEW systems. We seek to uncover the various standards in the field and how the current TEW systems deliver the different security services i.e., authentication of users, confidentiality of patient's data, integrity of data, availability of service, and non-repudiation of users. As a contribution to the field of security in TEW systems, we define a threat model for home and mobile TEW applications and propose a polynomial based Key Management Scheme (KMS) for the TEW Wireless Sensor Network (TEW-WSN).

The rest of the work is organised as follows (Figure 1.1). In Chapter 2 we give an overview of some TEW systems in terms of their services, architecture, technologies, and security implementation. In Chapter 3, we review the current research in sensor network security and make deductions about areas that need further research. In Chapter 4, we discuss the pros and cons of the different approaches to key management in sensor networks, define an optimal threat model for our ambulatory system and discuss the application of symmetric bivariate polynomials to key management [Blundo *et al.*, 1992]. In Chapter 5, we present a theoretical analysis of the scheme in Chapter 4 and give our reflections on the application of TEW systems in both developing and developed countries, the future trends in medical sensor networks, and the challenges that lie ahead in Chapter 6.

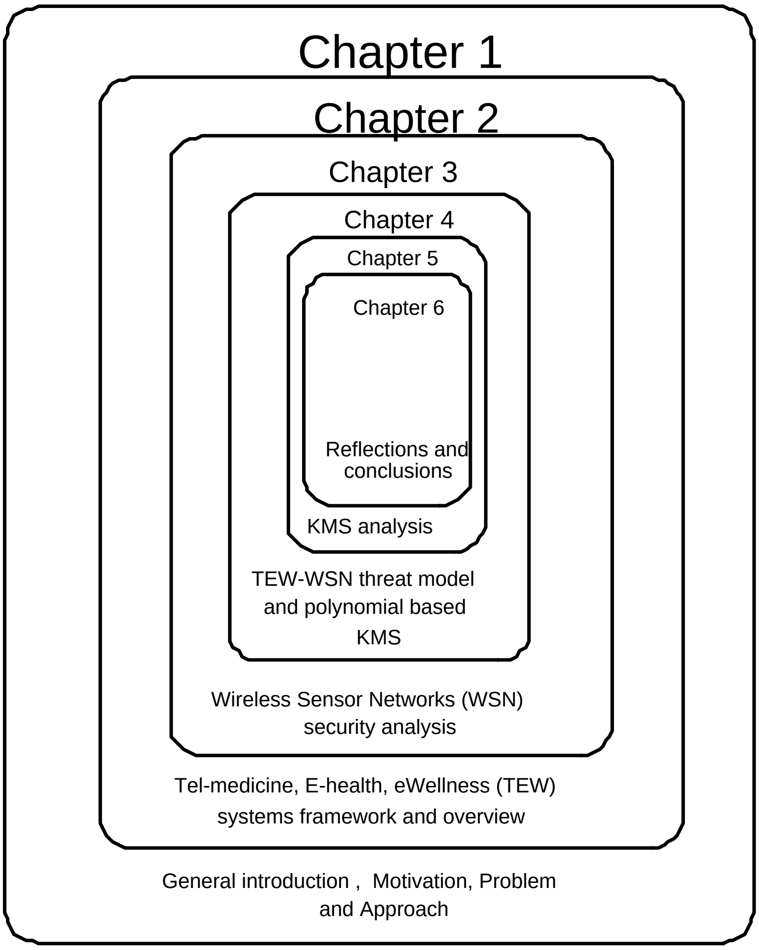
Chapter 1
Chapter 2
Chapter 3
Chapter 4
Chapter 5
Chapter 6
Reflections and conclusions
KMS analysis
TEW-WSN threat model and polynomial based KMS
Wireless Sensor Networks (WSN) security analysis
Tel-medicine, E-health, eWellness (TEW) systems framework and overview
General introduction , Motivation, Problem and Approach

Figure 1.1: Thesis structure

2
Related work

2.1 General framework

From our work, we assert that, any TEW system can be partly or wholly described by a three tier client-server framework. We observe that, any TEW system involves collection of data, either remotely by sensors worn by a patient or by a medical practitioner at a fixed location. The collected data is transmitted to the central server via the Internet or other communication channels available such as GSM and 2G. The transmission of data may be done in real-time or near real time. Medical personnel retrieve this data via a graphical user interface on their office terminals, mobile devices, or other supported user terminals. Figure 2.1 illustrates the general structure of this framework. Tier one encompasses a network of sensors that perform the actual sampling of signals, tier two encompasses data aggregation devices like a PDA or smart phone in patient monitoring TEW systems or local medical care provider PC in case of patient records management systems. Tier three is made up of the intergrated telemedicine centre which is the heart of the TEW system. Based on the type of service offered by a TEW system, mode of data collection, technologies integrated, deployment architecture and target user group, we categorise TEW systems into two categories: Patient Record management Systems (PRSs) and Patient Health remote monitoring Systems (PHSs).

PHSs: are systems that focus on convenience of service delivery to patients (i.e., patient oriented) and that deploy technologies that enable remote collection of patient data and remote delivery of health care services. The architecture of these systems spans all of the three tiers of our framework, which we refer to as a modular multi-tier client-server architecture. These systems rely on sophisticated sensor and communication technologies such as ActiS sensors, Zigbee, GPRS, Bluetooth, and smart phones to remotely collect and integrate data on the patients health status [Shnayder *et al.*, 2005, Jovanov *et al.*, 2005]. This data is transmitted in real time or near real time. The user interfaces for devices used to support human device interaction support all forms of data types as text, video, graphics, multimedia, and audio. Examples include, CodeBlue, and Medintegra Web.

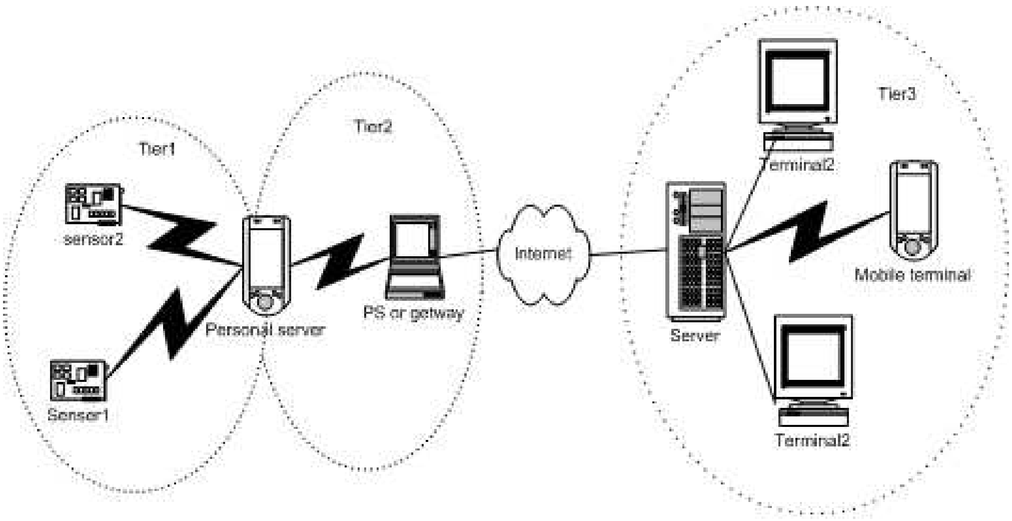

Figure 2.1: TEW system general framework

PRSs: are systems that focus on patient record management (i.e., on the needs of care provider) and link medical professionals to one another, but not patients to medical professionals. These systems are relatively more mature compared to PHSs since they rely on mature off-the-shelf technologies. Our claim is substantiated by rate of adoption of these systems in the field. Examples include, Ipath and OpenEMed [Brauchli *et al.*, 2005, Forslund, 2006]. We stress that PRSs can be regarded as subsystems of PHSs, since all PHSs incorporate the functionalities of PRSs.

In the following sections, we give an overview of the systems we studied leading to the framework described in Section 2.1. We describe the services, technologies, architecture, and security implementations of Ipath, OpenEMed, TeleCardio-FBC, CodeBlue, Wireless Sensor Body Area Network (WSBAN), and Medintagra Web. The selection of which system to study was based on the following guidelines:

- The availability of sufficient literature of a system. This explains why little study was done on commercial systems.
- Also our selection was guided by our bias on systems that can find application in developing countries where an ICT infrastructure is still poor compared to developed countries.
- Besides, our choice was influenced by our interests in security of wireless sensor technologies.

2.2 The Ipath telemedicine platform

Ipath is an open source telemedicine system running on six servers across the globe. The server in Norway serves a health network in Western Africa and the server in Dresden functions as a centre of field study about breast carcinoma organised by the German state of Sachen [Brauchli *et al.*, 2004]

Ipath development began in 1991 and was started by the department of pathology at the University of Basel, Switzerland with the objective of facilitating remote diagnosis of intraoperative frozen sections at a hospital in Samedan, Switzerland. After 10 years of development, in 2001, Ipath was rewritten and released as an open source telemedicine platform mainly supporting pathology consultation among medical practitioners. Given the 15 years of development, Ipath is relatively mature and has a higher user base than most of the telemedicine systems developed [Brauchli *et al.*, 2005, Brauchli *et al.*, 2004].

2.2.1 Ipath services

From Basel in Switzerland, to the Solomon Islands in the Pacific Ocean, Ipath has enabled remote consultations by pathologists. For example, medical personnel in the Solomon Islands can easily consult a group of distant experts through e-mail and other applications. The system also allows groups of specialists working in isolation to share knowledge and experiences with their remote colleagues. Besides enabling remote consultations, Ipath is used in academia to study the application of web technologies in the health domain of low resource communities. Besides user services, Ipath offers system services like security in order to protect the privacy of patient data.

2.2.2 Architecture of Ipath

The architecture of Ipath can be described as a multi-modular client server architecture, since it is composed of three main subsystems namely, the Ipath-server, the communication channel, and the Ipath-client. The server and client rely on the following modules to deliver their services: the database, content management, interface, web service, and security. While Ipath-client relies on the client interface and security. We observe that this architecture spans tier two and tier three of our general TEW framework.

Since the main objectives of the system is provision of reliable and user-friendly services, the Ipath-server is positioned within the Internet without access restriction from any firewall. This design is to guarantee easy access for authorised users from any location in the world at any time.

The client interface of the Ipath-client subsystem forms a client application, which can be a remote microscope session controller, a standard web browser, or simply a mail client. The security module of the Ipath-client provides secure session establishment and confidentially of the transmitted data [Brauchli *et al.*, 2004].

The Ipath-server provides system services like user authentication and authorisation, and data confidentiality by the security module, data definition by the database, data management by the content management system, and web services by the web server module.

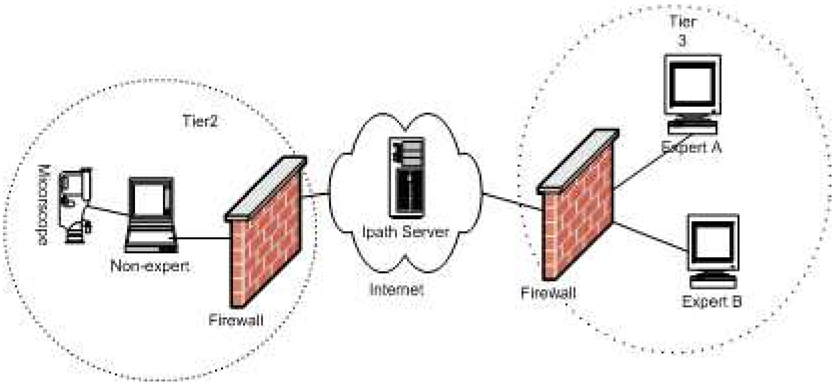

Figure 2.2: Ipath architecture

2.2.3 Ipath technologies

Technically Ipath is a web-based system developed in PHP and mySQL. The system relies mainly on Internet and Web technologies (like browsers, HTTP, HTML, SSL, etc) and high-speed communication links such as optical fibre, satellite, wireless technologies, and others to deliver its services [Brauchli *et al.*, 2005]. It also integrates advanced digital photography technologies embedded in standard digital cameras like the Nikon CoolPix 990 to take pictures of specimens.

2.2.4 Ipath security implementation

In Ipath, patient data resides on the Ipath server and on local medical personnel's personal computers. Thus, any security implementation must cover three scenarios: (1) data on users local computers, (2) data in transit, and (3) data on the central Ipath server. To access data on the Ipath server, users authenticate themselves using passwords and are authorised by the moderator of a community of a usergroup. The assumption is that patient's data on a pathologist local computer is part of the Ipath system and that the local user implements all the necessary standard security controls governing processing of medical records as required by law. Confidentiality of data in transit is maintained by end-to-end encryption provided by SSL and digital certificates for key exchange. In the current version of Ipath, integrity is through a non-edit policy, i.e., users can only comment on cases but they cannot modify the entries. In addition, patient privacy is maintained by use of pseudonyms i.e., users do not submit patient personal identifiable details to the Ipath server. We note that, the architecture of Ipath makes the system prone to denial of service attack [Brauchli *et al.*, 2005, ipath, 2006].

2.3 OpenEMed telemedicine system

OpenEMed is a modular open-source telemedicine platform with group-ware capabilities. It grew out of the Telmed system, which was initially developed by Los Alamos National Laboratory (LANL), University of California in 1994 as part of their Science Serving Society mission. In recent years, a number of telemedicine pilot projects in the US have implemented OpenEMed or integrated its functionalities into their systems. E.g., the medical surveillance system called B-SAFER

[Warren *et al.*, 2005] and immunisation registry system [Forslund, 2006]. These implementations highlight the level of maturity of OpenEMed technologies and their deployment in health care systems especially in America. We note that,the system encompasses tiers one and two of our general framework (Figure 2.1).

2.3.1 OpenEmed services

As one of its services, OpenEMed integrates patient records with detailed radiographic data, and facilitates secure remote sharing of these records through its sophisticated multimedia interface. This service improves clinical diagnosis and reduces the cost of health care by eliminating the time-consuming and costly activity of data gathering.

Besides enabling the integration and exchange of patient data among medical personnel, the system facilitates research and continuing education through its virtual patient record concept implemented in the Person Identification Service (PIDS) module, which enables access to case data without the need for patient identifying details [Forslund, 2006]. Also OpenEMed is used for self-training in diagnostic techniques and physicians use it to explain to a patient the courses of their illness. Besides the user services, OpenEMed also offers system services like user authentication, data encryption, and integrity checking using off-the-shelf technologies.

2.3.2 OpenEmed architecture

OpenEMed is made of eight modules, which are the Authentication module, Patient-ID Server, Medical Data Server, Secure web server, Relational Database Management System, Java client, the communication channel and Objection-Oriented Database Management System. This architecture spans tiers two and three of our framework and can therefore be characterised as PRS.

The Authentication module provides a general authentication service to users while authorisation is performed by individual servers. The authentication module is implemented as a PIDS, which is basically an identity management service. The current implementation relies on what the user knows (e.g., Username, password) and what the user has (e.g., iBUTTONS device, PIN) to deliver this service.

The Patient ID server performs authentication, authorisations, and audit. It delivers these services relying on its subcomponents Clinical Observation Access Service (COAS) and Resource Access Decision (RADS). The RADS component is a distributed need-to-know facility that provides finer grained access control than a role based access control system. The COAS is really a content access service, which simply manages the history of information about the entities identified with PIDS.

The medical server maintains medical records and the web-server replies user queries over a secure Internet connection. The Java client module provides a user-friendly interface that enables users to interact with the system and access its services [Forslund, 2006].

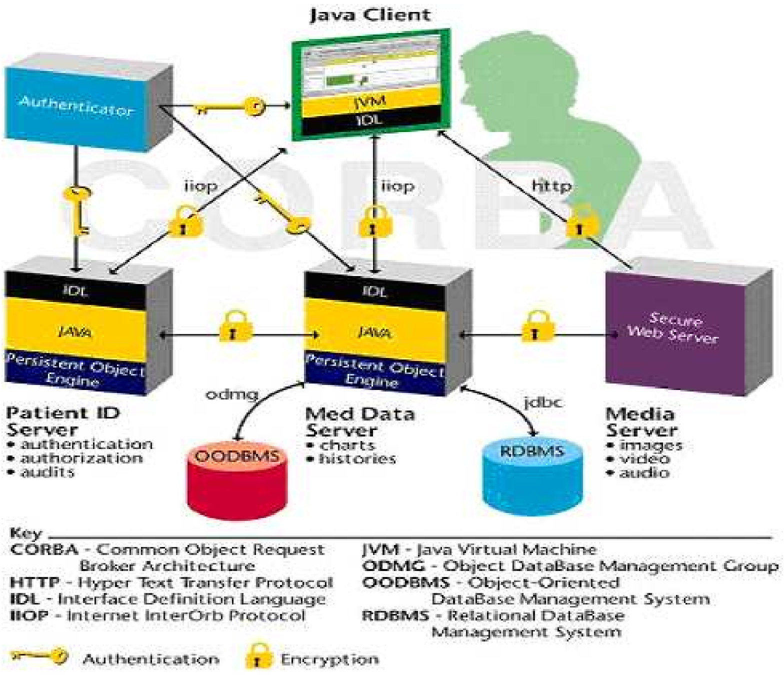
Java Client
JVM
IDL
Authenticator
iiop
iiop
http
CORBA
IDL
JAVA
Persistent Object Engine
IDL
JAVA
Persistent Object Engine
Secure Web Server
Patient ID Server
• authentication
• authorization
• audits
odmg
OODBMS
Med Data Server
• charts
• histories
jdbc
RDBMS
Media Server
• images
• video
• audio
Key
CORBA - Common Object Request Broker Architecture
HTTP - Hyper Text Transfer Protocol
IDL - Interface Definition Language
IIOP - Internet InterOrb Protocol
JVM - Java Virtual Machine
ODMG - Object DataBase Management Group
OODBMS - Object-Oriented DataBase Management System
RDBMS - Relational DataBase Management System
Authentication
Encryption

Figure 2.3: OpenEMed Architecture *(Adopted from [Forslund, 2006])*

2.3.3 OpenEmed technologies

OpenEMed is a web-based system built on the JavaTM platform and the Common Object Request Broker Architecture (CORBA). The JavaTM platform enables a single software to run on different kinds of computing platforms e.g., PC, smart phone, and Personal Digital Assistant (PDA). CORBA is used because it supports interoperability which is very important for TEW systems. Hence, these technologies come in handy in a field, where standards are still being developed and many preparatory devices exist in the market place.

Like other PRSs, OpenEMed depends on Internet and Web technologies like SSL, HTML, standard web browsers, and wireless technologies for service delivery. In order to support simultaneous access to data in the database, OpenEMed implements relational database management and object-oriented database management systems using SQL, XML, and flat files [Forslund, 2006].

2.3.4 OpenEmed security implementation

In OpenEMed, security at the server level is provided by two security modules implemented in CORBA: RADS and PIDS. RADS controls user access rights to patient information (authorisation) and PIDS, which is an identity management module, performs authentication of users. The RADS module performs authorisation after PIDS has authenticated the users.

The confidentiality of data is maintained by use of end-to-end SSL encryption using the

RSA algorithm and digital certificates for key exchange. To enforce the non-repudiation policy and comply with HIPAA legislation, the current version of OpenEMed relies on COAS, which manages the history of information about the entities identified with PIDS (audit trails). To further enhance the privacy of patients, OpenEMed assigns patients a unique pseudonym, which enables quick and anonymous use of patient case details [Moteiv, 2006]. For example, the care provider uses RADS to control the amount and kind of patient data that can be accessed by researchers who only need datasets without the need to provide patient identifying details to complete their tasks [Forslund, 2006]. Integrity of data over the communication channels is provided by SSL.

2.4 TeleCardio-FBC

The TeleCardio-FBC telemedicine system was developed to enable cardiologists at Fundao Bahiana de Cardiologia (FBC) University Hospital in Brazil to cooperate with cardiologists and physicians in remote locations on managing cardiovascular diseases. In 2002, Bludau et al. [Bludau & Koop, 2002] proposed an extension of the system to mobile platforms hence, the TeleCardio Mobile project. TeleCardio Mobile consists of two platform-independent systems: M-TeleCardio and WapCardio that enables access of TeleCardio-FBC functionalities via mobile computational platforms e.g. PDAs and smart phones. The system offers services similar to Ipath and OpenEMed, although the services are specific to cardiology.

2.4.1 TeleCardio-FBC architecture

The architecture of the TeleCardio-FBC system mirrors that of Ipath (Figure 2.2) and the two systems only differ in the number of interfaces they support. For example, TeleCardio-FBC supports mobile computing platforms like cell phones while Ipath is still a fixed system relying on personal computers. We note that the system spans tiers two and three of our general framework (Figure 2.1) and can therefore be characterised as a PRS.

2.4.2 TeleCardio-FBC technologies

Like Ipath and OpenEMed, TeleCardio-FBC relies heavily on Internet and Web technologies including web browsers, HTML, TCP/IP, SSL, and HTTP for communication, interface, and security. The core system is implemented using Microsoft Active Server Pages (ASP) technology and the relational database is developed in SQL. As the system is platform dependent, it lacks interoperability capability with emerging technologies for mobile devices (e.g., 2G, 3G, Bluetooth, and GPRS) for PDAs and cell phones.

Thus, its extension to mobile devices codenamed, TeleCardio-FBC mobile, exploits these technologies together with CDMA, GSM, WAP, JavaTM Servlet and Enterprise Java Beans (EJB) [Bludau & Koop, 2002]. JavaTM Servlet and Enterprise Java Beans technologies are used because they support a component-based, platform, and server independent method of developing applications. Besides offering capabilities of platform independence, EJB specifications create an infrastructure that takes care of the system-level programming, such as security, threading, naming, object-life cycle, resource pooling, remote access, and persistence.

2.4.3 System security implementation

We note from the available literature, that security was not one of the main design objectives of the Telecardio-FBC system which may explain why there are few published articles if any, that describe the security properties of TeleCardio-FBC. However, from our own analysis of this design, we conclude that TeleCardio-FBC relies on passwords for user authentication and authorisation while the standard Internet, Web, and wireless technologies maintain confidentiality and integrity of data over communication links.

2.5 Wireless Body Area Sensor Network

At the University of Alabama in Huntsville (UAH), Department of Electrical and Computer Engineering, researchers have implemented a fully integrated Wireless Body Area Sensor Network (WBASN) system. This system spans the entire framework of Section 2.1. The system enables remote delivery of health care services, facilitates sharing of patient records among care providers, facilitate research, and maintains privacy of patient data.

2.5.1 WBASN architecture

The system encompasses a network of sensors that connect to the PS, which in turn connects to a medical server via the Internet. Tier one is made up of a network of sensors which include: (1) Motion sensors, which monitor the patients overall activity, (2) heart rate monitor, (3) Blood pressure monitor, and (4) oxygen level monitor for on-body sensors. While the environmental sensors include: humidity, light, and temperature sensors.

Tier two encompasses the PS, which monitors the wireless sensor network and provides a graphical user interface (GUI) to support human-device interaction and links tier one devices to tier three devices. In this system, the PS is implemented on a PDA, cell phone or a PC. Connectivity between tier two and tier three is provided by the Internet, GPRS, 2G, 3G, and Wi-Fi.

Tier three encompasses a number of servers and end user terminals which enable care providers to access patients' data, consult, or deliver healthcare services like new exercise prescriptions (Figure 2.4).

2.5.2 WBASN technologies

The prototype system uses two ActiS sensors in which each sensor node includes a custom application specific board and Tmote sky platform from Moteiv [Moteiv, 2006]. Actis sensors run TinyOS, which is a middleware platform that incorporate “TinySec”, a module which offers a security service enabling sensors to authenticate data requesters and to establish a secure connection with the PS [TinyOS, 2006].

The Zigbee compliant protocol provides communication between sensors and the PS, while GPRS, Bluetooth, WLAN technologies, mobile communication technologies (e.g., 2G, 3G, GSM,

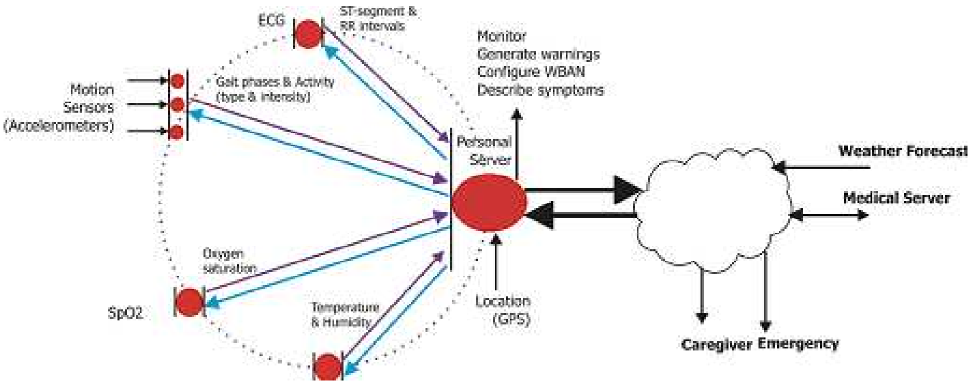

Figure 2.4: WBASN architecture *(Adopted from [Otto* et al.*, 2006])*

and VSAT), and the Internet provide the connection between the PS or/and the user's internet gateway and the care provider systems. Within the service providers infrastructure, Internet and web technologies such as HTTP, standard web browsers, HTML, and SSL are also integrated [Otto *et al.*, 2006, Warren *et al.*, 2005].

The PS used in the prototype system is a Dell AXIM X50v running on Windows CE and its applications are developed in Visual basic .NET 2003 while the local database on the PS is built in Microsoft Access.

2.5.3 WBASN security

In order to authenticate communications between sensors and the PS, sensors are uniquely associated to the PS using either sensor activity or serial numbers during initialisation. Confidentiality of data over communication channels between tiers two and three is maintained by standard encryption schemes such as SSL [Karlof *et al.*, 2004].

WBASN subscribers authenticate themselves on their PSs while the medical server performs authentication and authorisation of care provider personnel. Currently, authentication is based on passwords or biometrics. Logging of sessions is done to help audit security breaches and enforce the non-repudiation policy at all tiers [Warren *et al.*, 2005].

To further enhance privacy of patients, all records are stripped of all personal identifiable details before being integrated into the research database used by researchers. Also, the use of short-range wireless communications between the sensors and the PS also improves security of the system.

2.6 CodeBlue system

At Division of Engineering and Applied Sciences of Harvard University, researchers are exploring applications of WSN technology to a wide range of medical applications, including pre-hospital and in-hospital emergency care, disaster response, and patient rehabilitation. This group has identified five critical requirements for successful deployment of medical sensor networks: Wearable sensor platforms, reliable communications, multiple receivers, device mobility, and security [Shnayder *et al.*, 2005].

CodeBlue is designed to deliver a number of services which include: Device discovery, the establishment of multihop routing protocol, maintaining privacy of data, and user-friendly access to patient data. Like other systems in the PHS category, CodeBlue enables care providers to remotely monitor the physiological and environmental status of a patient. And through its groupware facilities, CodeBlue enhances the sharing of knowledge among care providers, thereby, supporting continuous education for medical personnel. It is also being used in academic research to explore the application of new technologies in the medical field [Shnayder *et al.*, 2005, Lorincz *et al.*, 2004].

2.6.1 CodeBlue architecture

Like WBASN, the architecture of CodeBlue spans all the three tiers of our framework (Figure 2.1) and mirrors that of WBASN (Section 2.5). The current focus of the CodeBlue project is however, on tier one.

2.6.2 CodeBlue technologies

Unlike WBASN, which relies on off-the-shelf sensors, the CodeBlue system relies on proprietary sensors (*Pulse Oximeter, Electrocardiograph (ECG), and Motion sensor*). The Pulse Oximeter uses infrared and near-infrared technologies to detect the amount of light absorbed by haemoglobin in the blood. The ECG is based on the Telos Mote platform. Motion sensors integrate motion analysis technologies like accelerometers, gyroscopes, and surface electrodes [Shnayder *et al.*, 2005, Lorincz *et al.*, 2004]. These sensors run TinyOS middleware and use Zigbee compliant protocols for communication with user devices like PDAs and PCs. The graphical user interface which supports human device interaction is built in Java.

2.6.3 CodeBlue security

We observe that the current implementation of CodeBlue lacks substantial security. According to its authors, work is still ongoing to integrate a link layer security in form of TinySec [TinyOS, 2006, Karlof *et al.*, 2004]. TinySec is a security module of TinyOS, which is open-source software for embedded systems which supports end-to-end encryption using a share-key encryption and a public-key protocol for key exchange. In situations where CodeBlue deployment involves transfer of data over a public network like the Internet, standard security technologies like SSL and IPSec are recommended. The current implementation lacks reliable communication and hence the inability of the system to guarantee availability of service [Shnayder *et al.*, 2005].

2.7 Medintegra Web suite

Medintegra Web is a proprietary PHS category telemedicine system developed by the Apollo group of hospitals to offer health services to rural Indian communities. Medintegra Web has a number of telemedicine applications that ensure its adaption to different kinds and levels of medical establishments. Its services include: (1) Telemonitored surgery in which a surgeon in a rural hospital performs surgical operations with the help of a distant specialist via videoconferencing, (2) Second opinion, in which doctors in low resource settings seek opinions from specialists in other locations (e.g., through e-mail, videoconferencing) about managing a given case, (3) Disaster management and continuous medical education through mobile health and e-learning modules. However, being a proprietary system, few technical or academic literature is available about the Medintegra Web system and our analysis is based on the literature and press releases found on Apollo hospital telemedicine websites [Apollohospitals, 2006].

2.7.1 Medintegra Web architecture

We describe its architecture as multi-tier client server which is the case with most PHSs. However, the system does not monitor patients at their homes but at their local clinics and hospitals. We note that this system encompasses all the levels of our general TEW framework (Figure 2.1).

Tier one encompasses data collection medical equipment for example ultra sound, electrocardiogram (ECG), digital cameras, or digital microscope.

Tier two encompasses an on-line PC with a web based client module enabling the medical personnel to build a case description. Tier one devices are connected to tier two devices via data cables and research is still going on to explore integration of low power wireless technologies like Bluetooth and Zigbee [Apollohospitals, 2006].

Tier three, which is the most complex level of the system, encompasses the telemedicine centre infrastructure that consists of a medical server, web server, and other devices that support Medintegra mobile on a GSM network.

2.7.2 Medintegra Web technologies

Medintegra integrates a number of communication and data processing technologies in order to deliver its services. The software platform is built in Java and relies on the Internet, LAN, WAN, POTS, ISDN, DSL, VSAT, cable and and Wireless network technologies like CDMA, GSM and Wi-Fi to provide connectivity between the main telemedicine centre and the remote hospitals or clinics. Other web technologies like HTTP, SSL, and standard web browsers are also used. Digital photography and video conferencing technologies are also used in service delivery [Apollohospitals, 2006].

2.7.3 Medintegra Web security

Medintegra is HIPAA compliant and supports both role-based access and user-based access control with user authentication based on fingerprints. To enforce the non-repudiation policy as required by the HIPAA standard, the system maintains data logs for security audits. To ensure confidentiality of data over communication lines, the system relies on 128-bit end-to-end encryption mechanism [Apollohospitals, 2006]. From the available literature, we note that, tier two and three seem to implement sound security controls. However, we are uncertain of how tier one implements security controls.

2.8 Conclusions

In this chapter, we have investigated a number of TEW systems which are mainly non-commercial because of lack of literature on commercial systems. During our study, we identified systems with similar features and services and thus we have categorised the various TEW systems into two major categories: PRSs and PHSs. *PRSs*, offer services of a content management system with group-ware capabilities. They enable medical personnel to share knowledge over the Internet and GSM network. We note that, patients do not interact with these systems directly and their data is entered into the system by medical personnel or devices like an on-line microscope in Ipath at the medical personnel's premises [Brauchli *et al.*, 2005, Forslund, 2006, Bludau & Koop, 2002].

PHSs, are more complex than PRSs and we refer to their architecture as modular multi-tier client-server with three levels (Section 2.1). We note that most of the PHSs are in early stages of their development and there are receiving alot of attention from researchers. Although, there are standards describing the individual components of PHSs, there is not single standard describing the entire system.

Our study has also revealed the requirements for acceptance of TEW systems. We note that, these requirements depend on the specific application and the deployment environment. However, some requirements are global to all systems. For example, all TEW systems must be reliable, user friendly, and secure.

Of all the requirements highlighted above, we note that security is the least focused on. Most developers have focused more on the engineering issues of making the technology work. Yet issues of patient protection and system availability are of equal importance in the medical domain.

We note that given the complexity of PHSs and stringent user requirements, defining and implementing robust security still remains a big challenge even though most of the technologies integrated are off-the-shelf with proven security properties. We assert that, it is the challenge of defining appropriate attack models, stringent usability requirements, and optimisation of resources (especially on sensors) that makes the design of secure PHSs a challenge. We note that even those that have implemented proven security technologies, may not have optimally modeled their threats. It is our belief that implementing strong security does not depend entirely on strong cryptographic primitives, but also on modelling realistic threats.

Authors of the majority of the systems we have studied highlight the need to explore ways of enhancing security of their systems especially at tier one (Figure 2.1). Issues of key distribution, channel congestion, service availability, traffic analysis, and optimal ciphers still juggle the research community. In the subsequent chapter we therefore focus on security of WSNs.

System	**Services**
Ipath	Second opinion, data privacy, research and continuing education
OpenEMed	Record management, secure remote consultation, research and continuing education
TeleCardio-FBC	Remote consultation, record management, and security of data
WBASN	Remote real time monitoring, e-prescription, data security, facilitates data sharing, support continuing education and research
CodeBlue	Real time monitoring, record management, education, and research.
Medintegra Web	Remote consultation, record management, continuing education.

Table 2.1: TEW systems services

System	**Technologies**
Ipath	PHP, mySQL, web technologies(browsers, HTTP,HTML, e.t.c), Internet technologies (TCP/IP, etc) and digital photography technologies
OpenEMed	JavaTM, CORBA, Web, and Internet technologies
TeleCardio-FBC	ASP, SQL, Java Serlet, Java beans, Web, Internet, and wireless (GSM, Wi-Fi, WAP, CDMA, etc) technologies
WBASN	Windows CE, VB .NET, Microsoft Access, Wireless, Internet, and Web technologies.
CodeBlue	Java, Internet, Web, BlueTooth, Zigbee, Infrared, and motion (accelerometers, gyroscopes, etc) technologies.
Medintegra Web	Java, Web, Internet, and Wireless technologies

Table 2.2: TEW Technologies

System	**Security**
Ipath	Standard security for local records, end-to-end encryption by SSL and user based authentication and authorisation
OpenEMed	RADS for authorisation, PIDS, for authentication, COAS for security audit and SSL for end-to-end encryption
TeleCardio-FBC	Standard security practises
WBASN	TinySec (for tier1), SSL (for tier 2 and 3), biometrics (authentication)
CodeBlue	Standard security practises, redundant transmission, and biometrics
Medintegra Web	Biometrics and passwords for authentication, SSL for end-to-end encryption and relies on both role and user based access policy

Table 2.3: TEW systems security implementations

System	**Remarks**
Ipath	Mature and classified as PRS, already deployed in low resource settings
OpenEMed	Classified as PRS, mature, and integrated in a number of health care systems
TeleCardio-FBC	Classified as PRS
WBASN	Classified as PHS and in early stages of development
CodeBlue	Still in early stages of development and classified as PHS
Medintegra Web	Classified as PHS

Table 2.4: TEW systems remarks

3
Wireless Sensor Networks

In this chapter, we focus on security properties of Wireless Sensor Networks (WSNs). We begin by giving a general introduction to WSNs in Section 3.2 highlighting their application areas, limitations, security implementations, and deployment topologies. Secondly, we review in detail the features of WBASN in Section 3.3 and CodeBlue WSN in Section 3.4 . In Section 3.5 we discuss other approaches to WSN security and conclude with a list of problems that require more research in Section 3.6.

3.1 Motivation

Our motivation to focus on WSNs was guided by the fact that PHSs hold the real promise of smart homes of the future. Also, our choice was influenced by the fluidity of standards of these systems and the availability of literature. Besides, our choice was guided by our own interests in wireless communication technologies given their unique features as described in Section 3.2.

3.2 General overview

A generic wireless sensor can be viewed as a block of 3 layers: Data acquisition, pre-processing, and communication layers. The data acquisition layer encompasses algorithms that perform the actual sampling of signals *(data acquisition)*. However, the discussion of these algorithms is beyond the scope of this research, interested readers are refereed to [Shnayder *et al.*, 2005]. The pre-processing layer performs *data structuring and filtering* while the communication layer is charged with *sending and receiving of data packets* (Figure 3.1).

WSNs have wide application areas, from battle field reconnaissance missions to process control in manufacturing and now in medical monitoring applications. Like conventional networks, these networks are made up of two types of entities: the master and the slave entity. This master-slave

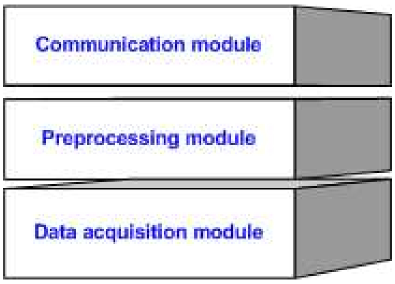

Figure 3.1: The structure of a generic sensor

relationship helps to maintain order in the network and provide secure means of communication among sensor nodes. In general, individual sensors form the untrusted part of the network (slave) while the base stations form the trusted computing base (master) upon which the security of the entire network depends (Figure 3.2). We observe that WSNs are deployed in two topologies: the flat topology which does not involve routing and the hierarchy topology with involves clustering of sensors and routing [Shnayder *et al.*, 2005, Jovanov *et al.*, 2005, Oliveira *et al.*, 2005].

Despite the promises WSNs hold, they suffer from a number of limitations which include: limited processing resources hence, implementation of the conventional cryptographic primitives becomes infeasible, hostile deployment environment and the inherited vulnerabilities of wireless communication. It is these limitation coupled with opportunities the technology can offer that has attracted our attention.

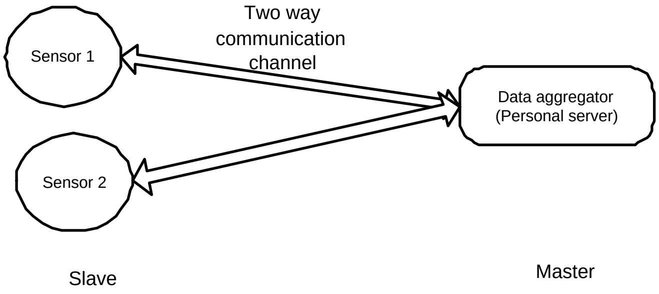
Two way communication channel
Sensor 1
Data aggregator (Personal server)
Sensor 2
Slave
Master

Figure 3.2: A generic wireless sensor network topology

3.3 WBASN approach

According to Otto et al. [Otto *et al.*, 2006], the WBASN prototype relies on the Zigbee compliant protocol (IEEE 802.15.4) [Zigbee-Alliance, 2006] to provide communication between individual sensors and the PS. The PS is the network controlling entity according to Figure 3.2, it aggregates and coordinates flow of data between sensors and itself. The PS establishes sessions, assigns sensor IDs, distributes keys, assigns communication slots to sensors, and manages the global time synchronisation protocol. Time synchronisation in this network is crucial for message correlation in order to minimise collisions and save energy. To address this challenge, the WBASN system uses the modified version of Flooding Time SynchronisationProtocol (FTSP)[Maroti *et al.*, 2004].

We note that, WBASN sensors operate in three states: Calibration, Transmission, and Dormant or Idle. The message sequence in Figure 3.3 illustrate a typical operation of WBASN Zigbee compliant protocol.

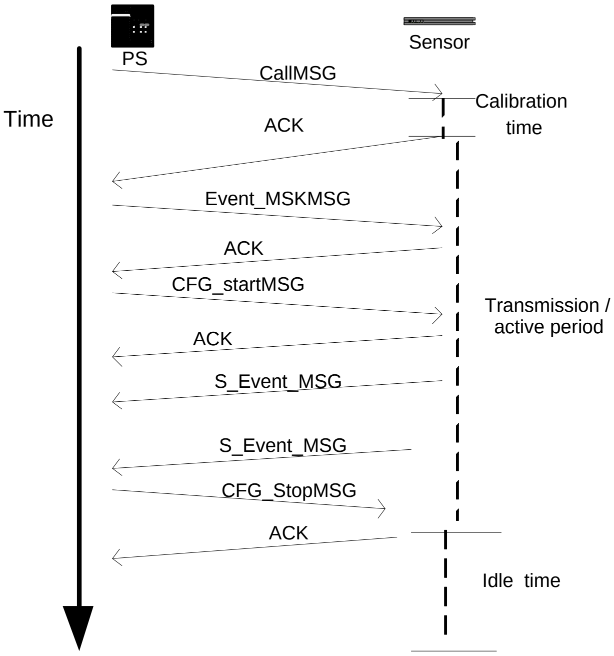

Figure 3.3: The WBASN Zigbee compliant protocol

- During *calibration* a sensor is marked using the S-EVENT-MASKMSG message sent by the PS. This message also sets the signal processing parameters on the sensor. Two types of calibration are currently supported: Sensor and session calibration. The sensor calibration, aims at accommodating sensor-to-sensor variations and the session calibration is used to define default values for the sensor parameters, e.g., a motion sensor needs initial calibration of the default body orientation. If a sensor supports encryption, keys are exchanged between the PS and the sensors during this stage.

- The second state is the *transmission* state. In this state, the sensor is continuously sampling and transmitting its data to the PS. The data transmitted by the sensor might be processed and encrypted or simply raw waveforms, which are unencrypted.

- The third state is the *dormant.* In this state, the sensor node is inactive, i.e., its not transmitting any packets.

We note that WBASN protocol (Figure 3.3) adopted a star topology of Zigbee standard and utilises the super frame mode of network access to eliminate collisions [Otto *et al.*, 2006, Zigbee-Alliance, 2006]. The super frame in the prototype system is of length 1 second and partitioned into 20 partitions of 50ms slots each. Sensors transmit only when their time slots are available. This is why time synchronisation is very important.

For secure communication, WBASN utilises hardware encryption supported by the ChipCon 2420 Zigbee compliant RF transceiver [Otto *et al.*, 2006, ChipCon, 2006]. The AES hardware encryption uses a 128-bit encryption key per session. We note that, the threat model of WBASN focuses on external attacks and assumed a stable deployment environment yet inside attacks in volatile environment are very much a possibility. Issues of network scalability and user friendliness do arise since the key distribution scheme requires the pre-distribution of keys before deployment. Also, relying on hardware encryption means increasing the size of the sensor which rise usability concerns. Also, little is discussed about the structure and optimality of the key material as well as mechanism of detecting compromised keys.

3.4 CodeBlue approach

CodeBlue defines a multicast routing protocol and device discovery protocol for the sensor nodes. According to Shnayder et al. [Shnayder *et al.*, 2005], the authors focused on making the technology work at the expense of security. The system relies on IEEE 802.15.4 complaint protocol to link Sensors and user devices. CodeBlue sensors can relay their data through a number of sensor nodes, hence the hierarchical topology. CodeBlue WSN was designed to cater for multiple data requests (i.e., a sensor can talk to multiple PSs) hence, the multicast routing approach. By abstracting from CodeBlue technical details, we envision CodeBlue sensor at any one time to be in one of the following state initialisation, transmission, and dormant.

In the *initialisation* state, sensors run a device discovery protocol based on Adaptive Demand-Driven Multicast Routing (ADMR) to discover identities of neighboring nodes and their capabilities. This is possible because sensors broadcast their Meta data *(details that describe a sensor in the network, e.g., serial number, functions, etc)*. Besides discovering neighbouring nodes, CodeBlue sensors build the routing tables, which are consulted when forwarding data to requester [Shnayder *et al.*, 2005].

In the *transmission* state, CodeBlue sensors are continuously transmitting data on the communication channel. This data could be sampled by the transmitting sensor or simply the sensor is relaying it from its neighbours.

In the *dormant* state, sensors are idle or inactive and this could be due to power failure, lack of data to transmit or due to out of reach radio channel. Figure 3.4 is an abstract message sequence illustrating an interaction between CodeBlue sensors and an end-user device *(PS)*.

From the published material, it is clear that CodeBlue, lacks substantial security and a sound

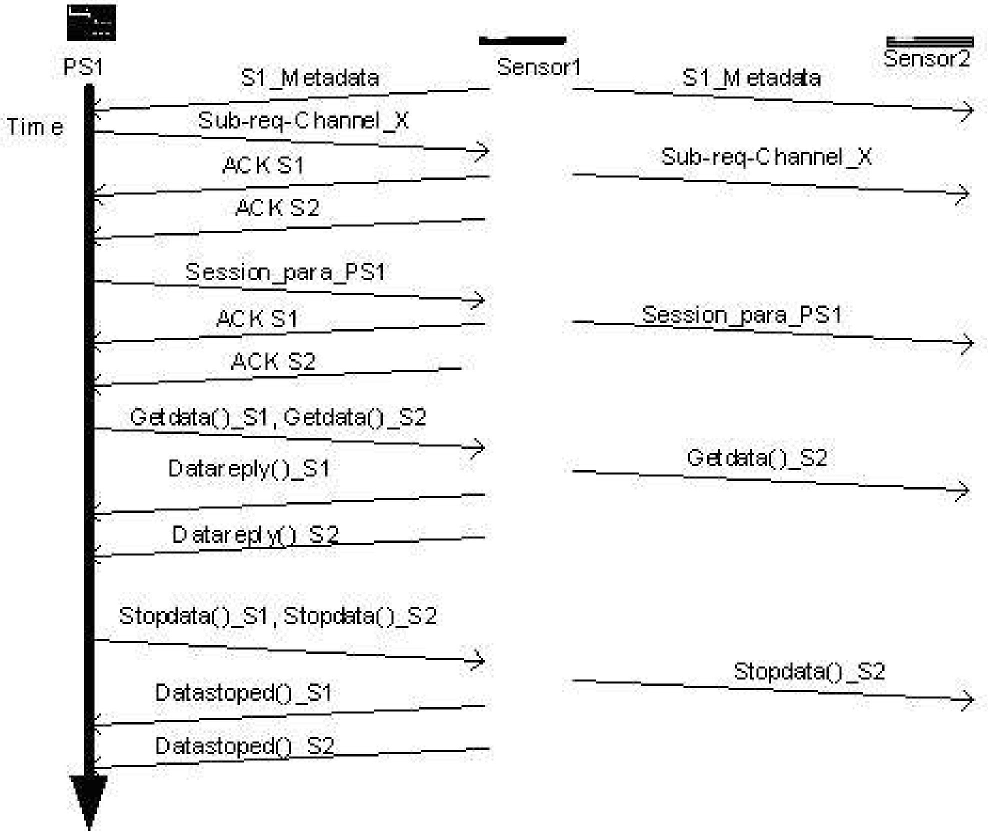

Figure 3.4: CodeBlue operation

mechanism to counter collisions in the sensor network which affects the reliability of the system. We observe that, unlike in WBASN where there is secure association of sensors to the PS, CodeBlue lacks this association and thus, it is easy for any adversary to install sensors and publish garbage data or even subscribe to download data from a legitimate sensor. Besides, no clear threat model is defined for this system, although standard security practises are recommended.

3.5 General WSN security approaches

Because of the unique features of WSNs, the design of optimal security mechanism for WSNs in general has attracted great attention as shown by the amount of published literature on the subject. In the proceeding sections, we present some of these approaches.

One of the most comprehensive approaches to WSNs security is SPINS *(Security Protocol for Sensor Networks)*, a suite of security protocols proposed by Perrig et al. [Perrig *et al.*, 2002]. SPINS offer the following security services: data confidentiality, data authentication, data integrity, and data freshness. In SPINS, base station(s) form the TCB of the network and act as a key distribution centre. SPINS is built from two smaller protocols: TESLA (*micro Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol)*, providing authenticated streaming broadcast and SNEP *(Secure Network Encryption Protocol)* providing data confidentiality, two-party data authentication, and data freshness. TESLA and SNEP are bootstrapped with a shared secret key between sensor and the base station. SPINS uses the concept of *semantic security* (i.e., a property of an encryption scheme which ensures that an eavesdropper has no information about a plaintext even when he sees multiple encryptions of the same plaintext) instead of conventional encryption to ensure that a reoccurring message encrypted under the same key generates different ciphered data. This is made possible by maintaining a counter at both ends of the communication channel so that session keys are a concatenation of shared keys and the current counter value.

SPINS is indeed a sound security construction with greater emphasis on optimal utilisation of scarce computational and communication resources. However, the design of SPINS relies on a generic threat model and its authors ignored the dynamic nature of WSNs. Besides, the design does not address security of compromised nodes, denial of service attacks, and traffic analysis. And also, issues of scalability remain since keys has to be pre-loaded into sensors before deployment and the authors do not discuss the composition of the initial key material.

Karlof et al. [Karlof *et al.*, 2004], proposed TinySec a link layer security construction, based on the knowledge of 802.11 and GSM networks. Currently, TinySec is an integral module of the TinyOS operating system for embedded systems [TinyOS, 2006]. TinySec defines and implements protocols for access control, data confidentiality, data integrity, and replay attack protection. TinySec being based on concepts of GSM and 802.11 networks overcomes inherent initialisation vector reuse problem by use of counter values and cipher block chaining. We note that TinySec does not address the security of captured sensors and lacks a sound key distribution mechanism. The design also does not offer an end-to-end security solution.

Oliveira et al. [Oliveira *et al.*, 2005] proposed LHA-SP a suite of security protocols for ad hoc WSNs. Their approach envisioned mitigating only attacks castigated by outsiders just as in SPINS and TinySec. In this approach, the network is organised into clusters with cluster leaders performing more roles than ordinary cluster members. Their main contribution to the field of WSN security is the development of a heterogeneous hierarchical communication scheme, which uses components of SPINS as the building blocks.

Zia et al. [Zia & Zomaya, 2006], propose a framework for securing WSNs. We note that this work is much related to the work of Oliveira et al. [Oliveira *et al.*, 2005]. Zia et al. made three contributions to the field of securing WSN: defined algorithms for dynamic cluster formation, cluster leader election, and secure routing. They proposed a key distribution scheme based on concepts of SPINS. In this framework, sensors maintain three keys, two preloaded and one dynamically generated. The preloaded keys enable the sensor to maintain association with the base station (*PS in case of PHSs*) in case of failure of the cluster leader and the dynamic key used to secure communication between the sensor and a cluster leader [Zia & Zomaya, 2006]. However, we observe that, this protocol has no mechanism to mitigate traffic analysis and it is vulnerable to inside attacks like compromised cluster leaders. Besides, the optimality of their key distribution scheme requires further research.

3.6 Conclusions

In this chapter we have presented a review of the different approaches to securing WSN both in the general context and in ambulatory WSNs in Sections 3.3 and 3.4. In general, there are standards covering individual components of the WSNs such as Bluetooth and Zigbee which define the physical layer of the Open Systems Interconnection (OSI) model *(communication channel)*, CORBA which handle object management over a networked environment[1] and the ISO/IEEE 11073[2] which defines the upper layer of the OSI application, presentation layer, and session layers. However, there is not single standard that is covering the entire WSN given the unique user requirements and deployment environment.

Despite the promise these technologies hold, wireless sensors and WSN in general have a number of limitations which include: (1) limited processing and energy resources hence, making implementation of the conventional cryptographic primitives (PKI, digital signatures, etc) infeasible, (2) hostile deployment environment, and (3) the inherited vulnerabilities of wireless communication. For medical WSNs, requirements of user-friendliness and guarantee of availability of service even in emergency situations make the problem of securing WSNs more difficult [Shnayder *et al.*, 2005]. It is these constraints coupled with opportunities the technology can offer that have attracted our attention and the attention of numerous researchers. Despite this attention, a number of security issues still need more research and below we list some.

- Central to the challenge of securing a WSN is the need to design an optimal, secure and scalable Key Management Scheme (KMS). This scheme should cover key generation, distribution, update, detection of compromised keys and their eventual revocation.

- Also, there is need to define efficient secure routing protocols that can mitigate traffic analysis and minimise the risk of denial of service attacks especially for safety critical TEW-WSNs.

- There is need to investigate which cryptographic primitive can offer greater resiliency at constrained resources, and which primitives are suitable for which application scenarios? For example is RC5 a better solution in military application than elliptic curve cryptography.

- We note that, designing resilient WSN does not depend entirely on strong cryptographic primitive but also on defining appropriate threat models. Hence, the need to model threats for different application scenarios. For example, mobile users of TEW-WSNs face different threats from stationary users (e.g., in-hospital or home monitoring).

- Besides the technical issues, their are organisational and social issues as well that have to be looked into if TEW-WSNs has to gain acceptance in society.

[1] http://java.sun.com/developer/onlineTraining/corba/corba.html

[2] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=36347

Hence, in the subsequent Chapter we focus on developing a realistic threat model for TEW-WSNs incorporated in PHSs and discuss the application of polynomial based key management scheme to secure this network.

4 A secure and optimal KMS for TEW-WSNs

In this chapter we review some approaches to key management in WSNs in Section 4.2. In Section 4.3 we formulate a threat model for TEW-WSNs, detailing the application scenario assumptions and attacker capabilities. From the threat model, current KMSs, and TEW-WSN requirements, we present an optimal and secure polynomial based KMS in Section 4.4. Unlike most of the current proposals which give generic solutions [Eschenauer & Gligor, 2002, Perrig *et al.*, 2002], our propose takes into account the contingency factors of TEW application scenario like deployment architecture, the degree of hostility of operational environment, and usability constraints as encoded in our threat model.

4.1 Motivation and problem

As we have already mentioned in the preceding chapters, WSNs rely on secrecy of keys and sound cryptographic primitives to deliver the security services of authentication, confidentiality, integrity, and non-repudiation. However, their limited energy supply and computational resources make the implementation of robust cryptographic primitives, like the public key infrastructure and the Diffie-Hellman key exchange algorithm infeasible [Stallings, 2003].

Hence, an intriguing research question “how does one securely set up and manage secret keys among communicating sensors?”. This problem is part of a wider problem which in literature is referred to as *the key agreement problem* [Stallings, 2003, Pfleeger & Pfleeger, 2003].

A number of proposals to address this problem have been published. However, most of these proposals assume generic threat models which are either too complex or unrealistic for our TEW-WSN applications. As noted earlier in Section 3.6, designing robust schemes requires the modeling of optimal threat models. Consequently, we find the existing KMSs inadequate for our patient remote monitoring application (which we discuss in Section 4.2). Hence, the need to explore new ideas in threat modeling and the application of polynomial based KMS in TEW-WSNs since little is done in literature when compared to the probability and key bootstrapping approaches.

4.2 Related work

Three generic key agreement schemes are prevalent upon which the wider KMSs are built: the key pre-distribution, the self-enforcing, and trusted-server schemes. In the key pre-distribution scheme, keys are bootstrapped into sensors before deployment. This has an advantage of secure delivery of keys at limited energy consumption, however, it suffers from lack of scalability and user-friendliness. The self-enforcing scheme relies on asymmetric cryptography, such as the Diffie-Hellman key agreement. This is one of the most attractive options of agreeing shared keys, however, constrained computation and energy resources of sensors make this option infeasible. The trusted-third party scheme, depends on a trusted server for key agreement between communicating entities, e.g., kerberos [Stallings, 2003], which is scalable and holds the promise of a robust KMS. A number of proposals based on these generic schemes have been published, which we discuss below.

Perrig et al. [Perrig *et al.*, 2002] propose SPINS. In SPINS during network initialisation, the base station (in our case the PS) distributes a master key which it shares with the individual sensors. From this master key, other keys used during network operation are derived using a one-way function. One limitation of this scheme is that it does not enable secure sensor-to-sensor communication, hence routing may not be secure. We observe that SPINS has no mechanism of detecting compromised keys. Also, given the fact that the master key has to be bootstrapped into sensors before deployment, this rises scalability concerns.

To enable secure routing, Eschenauer et al. [Eschenauer & Gligor, 2002] propose a probabilistic key pre-distribution scheme where individual sensors receive a random ring of keys from a pool generated off-line before deployment. For two sensors to agree on a key, they have to find a common key within their individual key ring. We note that the scheme avoids having to include a central trusted base station as a single point of failure. However, this scheme has a number of shortcomings: firstly, given the memory constraints on the sensor nodes, it means the sensor can hold only a few keys, hence, for large sensor networks, this scheme lacks the scalability that is needed. Secondly, during the shared-key discovery phase, key identifiers are broadcast in clear text enabling an adversary to perform traffic analysis during the key exchange. Thirdly, sensor nodes are trusted in this approach, which in practise cannot be the case since sensors have limited processing resources to perform strong cryptographic primitives. Also the size of sensors and their and deployment environment makes trusting sensors a design flaw. Fourthly, attackers who compromise a sufficient number of nodes could also reconstruct the complete key pool and break the entire scheme.

Chan et al. [Chan *et al.*, 2003] extend the work of Eschenauer et al. by proposing three key pre-distribution schemes. In their design, they observed that sensor nodes cannot be trusted since they are not tamper resistant and even their deployment environment is hostile. This assumption improves the work of Eschenauer et al., which assumes that sensors trust each other not to misbehave. Chan et al. made the following contributions: firstly, they defined the $q - composite$ random key pre-distribution, which remains secure under small scale attacks while trading off increased vulnerability in the face of a large scale physical attack on network nodes. Secondly, they defined a multi-path key reinforcement scheme, which increases the security of key setup in a sense that an attacker has to compromise a great number of nodes to gain a high probability of compromising a single communication link. Thirdly, they defined a random-pairwise keys scheme, which assures that only compromised nodes are affected while the rest of the network remains secure.

Pietro et al. [Pietro *et al.*, 2003] focused on optimisation of Eschenauer and Gilmar probability scheme. They incorporated two protocols: direct and cooperative. These protocols establish a pairwise communication link between sensors by assigning a set of random keys to individual sensors. This idea amounts to pseudo random generation of keys at minimum energy compared to the previous probabilistic based KMSs. Given the memory constraints on sensors, it means they can hold at any one time a few keys, hence, for large networks it might not be an optimal solution. Also this scheme is only k-secure, i.e., compromising k out of n sensors in the network, one can reconstruct pairwise keys for $t = n - k$ non-compromised sensors. Finding the upper bound of k remains a research challenge.

Anderson et al. [Anderson *et al.*, 2004] departed from the concept of bootstrapping key material and propose a novel KMS based on a weak threat model for less critical sensor networks codenamed “key infection”. In this scheme, Anderson et al. assume that the time required for key agreement during sensor initialisation is very short, hence, only adversaries with prior knowledge of sensor deployment can succeed in monitoring a small percentage α of the network. In this scheme, during network initialisation, sensors listen for transmissions to discover their neighbours. After discovering neighbours, they exchange keys with each other in clear text. After the keys have been exchanged, individual nodes run the *secrecy amplification algorithm* to strengthen the security of the shared key. Their work made two main contributions to the problem of key management: firstly, it opened up a new dimension of research in key agreement which does not rely on bootstrapping secret information. Secondly, their work emphasised the idea of contingency consideration in threat modeling. However, as initial keys have to be distributed in clear text, it means that, this scheme may not be appropriate for TEW-WSNs.

In their attempt to address scalability limitations in previous KMSs in WSNs, researchers at the University of Sydney [Zia & Zomaya, 2006] have proposed a secure hierarchical key management scheme in a clustered sensor network. Their idea is to use three keys: two generated by the base station (i.e., K_n the network key and K_s the sensor key) and one key generated by the cluster leader (K_c). The keys generated by the base station are pre-loaded into the sensor before deployment and therefore suffers from the inherent limitations of key bootstrapping. We also note there is a potential design flaw about the deployment of the key K_s and there is no mechanism of detecting compromised keys and their eventual revocation.

Oliveira et al. [Oliveira *et al.*, 2005] focused on minimising the key agreement cost and propose a purely symmetric KMS which does not depend on probability theory. In their proposal, prior to deployment, individual sensors are preloaded with two symmetric keys, a network-wide key, and a pairwise key shared with the base station only. The network key is used to set up pairwise keys to secure links between sensors and is dropped when links are setup. The second key shared with the base station is used to adapt new sensors or authenticate rejoining ones. This scheme suffers from the inherent limitations of key bootstrapping. Also, the scheme assumes that the value of ciphered data decreases to zero as the life time of the key draws to a maximum, but the value of our medical data remains constant throughout the lifetime of a patient. This assumption introduces a potential design flaw.

Yang et al. [Yang *et al.*, 2005] observed that, node compromise is the most severe threat to sensor networks. They note that despite this threat, most of the key management proposals in literature rely on threshold schemes which remain secure if τ or less nodes are compromised, but completely break down when more than τ nodes are compromised, where τ is a fixed threshold. Thus, to mitigate limitations of threshold based schemes, Yang et al. propose a new key scheme based on two location technique: *location binding keys* and *location based key assignment*. The general idea in this approach is to localise keys, so that any compromise of a node in a given locality does not spread to other regions allowing the rest of the network to function without the danger of complete breakdown.

4.2.1 Conclusions

Perrig et al. proposes a sound KMS in SPINS. However, SPINS has no mechanism of detecting compromised keys and it was designed based on a generic threat model. Thus, secure routing may not be guaranteed in TEW-WSNs. While probability based schemes [Eschenauer & Gligor, 2002, Chan *et al.*, 2003, Pietro *et al.*, 2003], which originated from the work of Eschenauer et al., have scalability limitations due to constrained storage resources on the sensors. Above all, the resiliency of these approaches depends on a threshhold value, i.e., in a network of n sensors, if an adversary compromises k sensors out of n, k sufficiently large, then an adversary can reconstruct the shared pairwise keys between the $n - k$ non-compromised sensors. But determining the optimal size of k still remains a research question.

Anderson et al. [Anderson *et al.*, 2004] departed from the concept of bootstrapping key materials on sensors and propose a novel concept codenamed “the key infection” which relies on the assumption that network initialisation takes a very short time sufficient to exchange the key material in plaintext without the adversary eavesdropping. However, given the sensitivity of medical information and TEW-WSN deployment environment, we find key infection not an adequate solution.

We not that most of the previous key management proposals have a number of limitations. Firstly, there are built based on a generic threat model which does not take into account the unique requirements of TEW-WSN. Secondly, most of the proposals have no mechanism of detecting compromised keys and their eventual revocation.

4.3 TEW-WSNs threat model

In prior work, most researchers have assumed a generic threat model with a highly motivated adversary who can deploy bogus sensors to inject traffic into the network or even gain physical access to legitimate sensors. In our work, we scale down this model to reflect the contingency factors in our application scenarios. We envision two deployment scenarios: home remote monitoring and mobile remote monitoring. We observe that in both applications, the goal of attacking the KMS is to get the key used to secure the communication between sensor and the PS. Figure 4.2 illustrates the attack tree which is derived from a list of stakeholders, deployment architecture, and communication protocols.

Stakeholders: We observe that patients are the main stakeholders in this scheme. Their interest is to maintain individual privacy as well as the privacy of their medical data. The second group is made up of medical care providers, whose interests are system availability, ease of use, transparency to patients, and maintaining the privacy of patients' medical data as required by law. The third category encompasses the informal care providers, like relatives and friends of the patient. Although, their stakes are hard to quantify, we note that ease of use would rank top on their requirements since this reduces the amount of time they would have to spend attending to the patient (Section 4.4.1).

Hypothetical case 1 *(continued): To put our threat model into perspective, we re-cap the hypothetical case study of a stroke patient under rehabilitation of Section 1.3. In this case, Jack initialises his keys once a day, but he can replace malfunctioning sensors on the fly. In public and on his own, Jack's ambulatory system is highly vulnerable to both logical and physical attack. While at home and in the company of his family, he enjoys improved physical security provided by his family, however, his curious children and neighbours pose a logical security threat. Because of the varying degrees of hostility in our deployment environments and attack advantages, we believe a single threat model may be inadequate for a design of a sound KMS. Therefore, in the Subsections 4.3.1 and 4.3.2 we give some assumptions for our threat model to hold in the two deployment scenarios.*

4.3.1 Home monitoring threats

In a home setting, the TEW-WSN is more or less static and can be highly predictable. The adversary can deploy robust computational resources since energy is not a problem. Below are some assumptions we make regarding threats from a stable environment.

- It is easy and cheap for an attacker to deploy bogus sensors and smart phones to sniff packets from WSNs.
- We assume that under some conditions, an attacker can have physical access to sensors even though they are worn by the patient as part of his cloth or jewelry or installed in their homes and offices.
- We assume that the adversary has a high probability of monitoring all communications from network initialisation to shutdown given the small number of sensors involved and the predictability of network operation.

- We also assume that the adversary can mount active attacks at any time during the operation of the network.

- We do not trust the informal care providers like patient relatives and friends, who can gain both physical and logical access to sensors and the personal server.

4.3.2 Mobile monitoring threats

Mobile patients face a slightly different challenge, their mobility presents new threats as well as new defence opportunities (Section 1.3).

- Because of patient's mobility, the adversary has a very low probability of monitoring the network during initialisation, but he still has opportunities of monitoring as well as injecting new traffic in the network during operation.

- In mobile situations, the attacker has limited computational resources unlike in the home monitoring application.

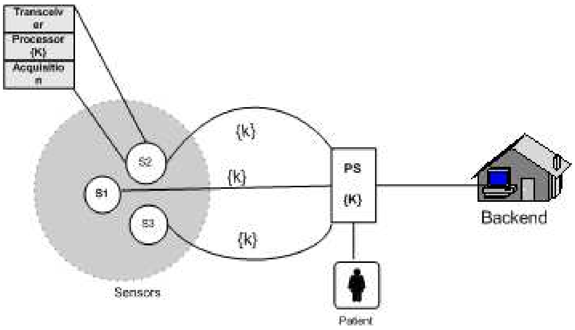

Figure 4.1: Attack topology

4.3.3 Threat model discussion

From a list of stakeholders (Section 4.3) and asset configuration (Sections 4.3.1 and 4.3.2), we present our threat model in the form of an attack tree (Figure 4.2). We note that a symmetric key k shared between a sensor and personal server at any time t, can be located on the sensor, personal server, or over the wireless communication channel (Figure 4.1), and any effort by an adversary to recover this key can be launched from the care provider infrastructure (*system back-end*), by compromising of user's physical security (Figure 4.1), or by exploitation of a system vulnerability (Figure 4.2).

In order to exploit a system vulnerability, the adversary has to deploy surveillance equipment within the communication range of the network and this device has to remain in place for as long as possible to obtain sufficient material to perform crypto-analysis. Although, this attack may seem to be too expensive for an adversary compared to social engineering of processed data, it is

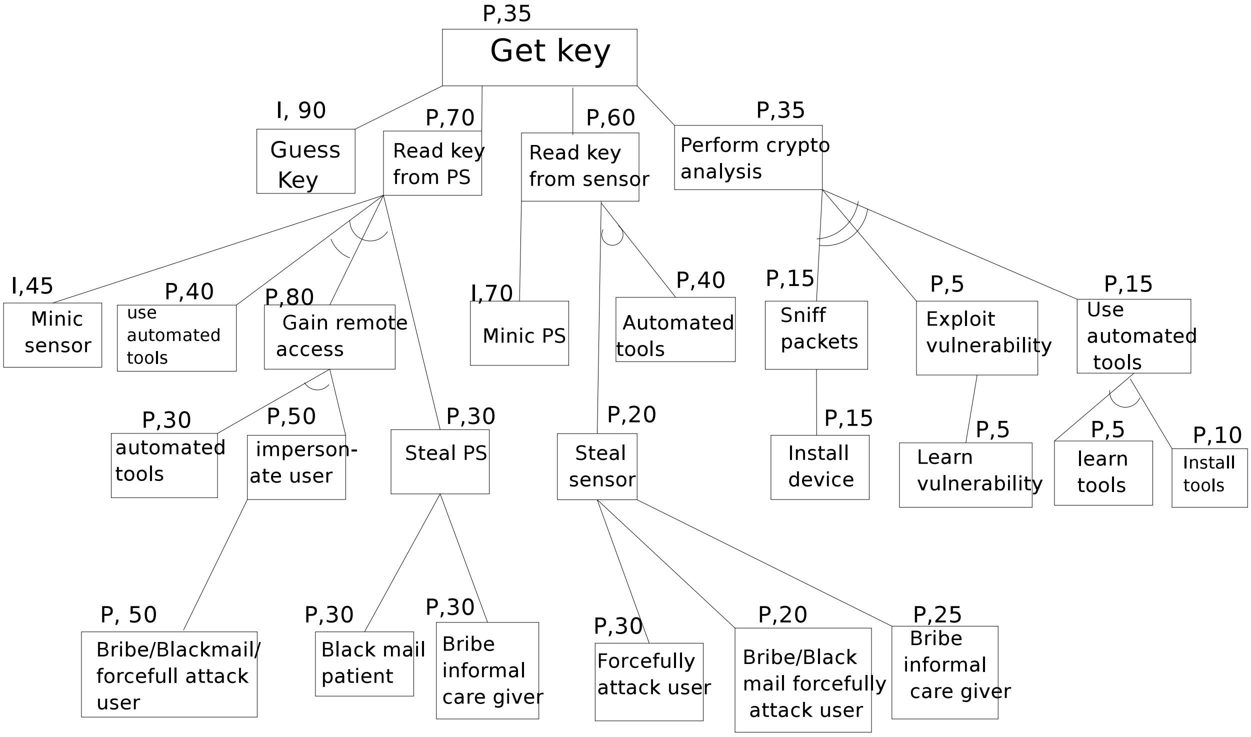

Figure 4.2: TEW-WSN KMS attack tree

imperative to take into account that, he will find motivation to mount this attack.

Alternatively, the adversary can exploit user vulnerabilities such as poor system setup and careless exposure of sensors. We present the work done by an adversary to achieve a given goal in costs and the possibility of success as P and I (with P implying that the attack is possible and I implying that the attack is impossible) (Figure 4.2). For leaf nodes, we derive their likelihood based on system deployment configuration, operational environment properties including attacker capabilities and advantages. And we estimate costs η of achieving these goals based on our intuitive judgement of the investment the adversary has to make in terms of time, knowledge, and tools to achieve the goal. For non-leaf nodes, their costs depends on the values of the children nodes and if the node is an AND or an OR node. If the node is an AND node, the cost is the sum of the costs of the children otherwise, the cost will be the minimum cost of the children (Equation 4.1). Also the likelihood entirely depends on the likelihood of the child nodes (Equations 4.2 and 4.3). Formalising the above, we have;

Notation:
Let h be a node in the tree (Figure 4.2), let $\sigma(h)$ denote the set of all children of h, and let $Cost(h)$ denote the costs for achieving the goal of node h, which is defined as

$$Cost(h) = \begin{cases} \eta_h, & \textit{if h is a leaf node} \\ \sum_{c \in \sigma(h)} Cost(c), & \textit{if h is an AND node} \\ min_{c \in \sigma(c)} Cost(c), & \textit{if h is an OR node} \end{cases} \tag{4.1}$$

Note: η is a factor representing inherent costs per node based on our own judgement. While the likelihood of *h* when *h* is an AND node is defined as,

$$Likeli(h) = \begin{cases} P, & Likeli(\sigma(h)) = P \\ I, & otherwise \end{cases} \tag{4.2}$$

And when *h* is an OR node, the likelihood is defined as

$$Likeli(h) = \begin{cases} I, & Likeli(\sigma(h)) = I \\ P, & otherwise \end{cases} \tag{4.3}$$

From our attack model (Figure 4.2), we conclude that, the most likely attack is the exploitation of system vulnerability, hence affirming our claim that more efforts are needed to design a robust KMS for TEW applications.

4.4 Proposed TEW-WSNs KMS

We begin by giving the requirements of TEW-KMS, assumptions, and justification why a polynomial based key agreement scheme is a good option for TEW-WSN. Lastly we discuss the overall KMS operation including generation of session keys and their revocation.

4.4.1 TEW-WSN KMS requirements

We categorise these requirements into: User, Functional, and Performance requirements.

User requirements: The scheme must be easy to use, easy to learn, transparent to users, and consistent with their life style. It should support plug and play operation enabling users with often little technical knowledge to assemble and disassemble the system on the fly.

Besides ease of use, the scheme must guarantee secrecy of keys since it is the basis of maintaining privacy of patients and their data as mandated by the various privacy legislation's. i.e., in the US, Health Insurance Portability and Accountability Act (HIPAA) and the European Directive 95/46 in Europe among others.

Functional and performance requirements: Under *performance requirements*, we note that, the scheme should be low resource-intensive in terms of computation power, bandwidth utilisation, and memory overheads. While under *Functional requirements*, we note the following deliverables:

- The scheme should generate strong keys, i.e., keys which cannot easily be recovered by brute-force or other means during their lifetime (*maintain secrecy of keys*).

- The scheme should be flexible and scalable allowing transparent renewal of keys and revocation of compromised ones.

- We also note that, the key management scheme should guarantee availability of service, since it is serving a mission critical application especially during emergencies.

Assumptions

- The personal server is the trusted computing base for the system.

- Every sensor is associated with a unique identity (ID), which is encoded with information about the polynomial index the sensor holds.

- The network is composed of heterogeneous sensors which include: On-body sensors that communicate with other sensors and only one personal server, and Environmental sensors that can communicate with multiple PDAs and other sensors.

- Sensors when powered on, begin transmitting their ID at low power settings and gradually increase their range until they detect another device. This is all done very fast.

- Ideally, our sensor uses three keys, the univariate polynomial for authentication, the agreed on key as master for integrity, and the session key for encryption.

- We note that although our scheme supports routing, given the communication range of most sensors and the nature of TEW systems, only a few sensors would have to relay their data via intermediaries. Otherwise, most sensors in the network are able to establish direct links with the personal server.

4.4.2 Polynomial solution justification

Symmetric polynomials have nice properties that make their application in key agreement for ad hoc sensor network a wise option which include the following;

- The symmetric property of symmetric bivariate polynomials (i.e., $f(X, Y) = f(Y, X)$) enables two arbitrary sensors to compute their common key after one round of communication. This property is optimal in communication resources and is scalable [Sánchez & Baldus, 2005].

- The degree of the polynomial (β) defines the resiliency factor $\psi = \beta + 1$ of the scheme, *(the number of sensor nodes an adversary has to compromise in-order to recover the key of non-compromised nodes)*, hence, a scheme based on bivariate polynomials achieves graceful degradiation. i.e., degradation of a system in such a manner that it continues to operate, but provides a reduced level of service rather than failing completely. Also, this property enables the estimation of security guarantee level delivered by the scheme more accurately.

- Bivariate polynomials can be optimised for different kinds of sensor platforms without lowering the resiliency factor. For example, by varying the length in bits of coefficients of a β-degree bivariate polynomial to q, $q = 2k + 1$ for k the size of CPU register in bits, the scheme can be optimised for different sensor platforms [Sánchez & Baldus, 2005].

4.4.3 Key material

Our key material *(i.e., piece of information from which keys are derived)* is based on the work of Blundo et al. [Blundo *et al.*, 1992], who proposed a bivariate polynomial scheme of establishing a shared key between two communicating entities. Before deployment, the PS generates a pool of bivariate polynomials of order β based on user authentication data, time, sensor serial numbers, and other ambiguous data over a finite field F_q with q being a prime number, which is sufficiently large for containing keys. The polynomial is of the form,

$$f(x,y) = \sum_{i,j=0}^{\beta-1} a_{i,j}x^i y^j, ([a_{i,j} = a_{j,i}][i + j \leq \beta]) \tag{4.4}$$

As always with symmetric key schemes, before deployment individual sensors are loaded with a unique key material and in our case it is a univariate polynomial of the form $f(X) = f(ID_{s_i}, X)$ where ID_{s_i} is the identity of sensor S_i.

4.4.4 Key agreement and distribution

After deployment, a sensor broadcasts its identity say ID_{s_i}, also the personal server transmits its identity which is unique (ID^i_{ps}) using the concept of selective broadcast. *Selective broadcast* refers to point-to-multiple point transmission of identical information to several selected users. The goal is to minimise total transmit power while satisfying minimum received signal-to-noise ratio (SNR) requirements. When the sensor and the personal server have received the identities of their respective communication partner, each can compute a shared master key K_{mk}, $K_{mk} = f(ID^i_{ps}, ID_{s_i})$. This amounts to evaluating the bivariate polynomial at a given point. For example, let the personal server generate a bivariate polynomial (Equation 4.5).

$$f(x,y) = x^2y^2 + 3xy + 2 \tag{4.5}$$

Then let sensor S_x be given a share

$$f(y)_{S_x} = f(S_x, y) = S_x^2 y^2 + 3S_x y + 2 \tag{4.6}$$

and sensor or personal server PS be given the share

$$f(x)_{PS} = f(x, PS) = x^2 PS^2 + 3xPS + 2 \tag{4.7}$$

If the identities of S_x and PS are integers 3 and 2 respectively, then finding K_{mk} amounts to evaluating $f(S_x, PS)$ at $S_x = 3$ and $PS = 2$. Then we can verify that, the Equation 4.8 holds.

$$f(S_x, PS) = f(PS, S_x) \tag{4.8}$$

i.e., Equation 4.6 becomes

$$f_{S_x}(3, 2) = 3^2 \times 2^2 + 3 \times 3 \times 2 + 2 = 56 \tag{4.9}$$

Also Equation 4.7 becomes

$$f_{PS}(2, 3) = 2^2 \times 3^2 + 2 \times 3 \times 2 + 2 = 56 \tag{4.10}$$

Thus, Equation 4.8 is true

From the master key we generate a chain of session keys using a one-way function. Our aim is to achieve *semantic security* by use of delayed disclosure of symmetric session keys. If K_{mk} is a master key for sensor S_x, then the first session key K_{ses} is got by the relation $K_{ses} = F(K_{mk})$ for which F is a publically known one-way hash function like MD5 [Stallings, 2003]. For simplicity, below we describe the key establishment protocol between a sensor and the PS based on concepts discussed above.

Notation:

Let S_i denote a sensor i, PS denote the personal server, K_{mk} be the shared master key, K_{ses} be the link session key, T be the current time stamp, and F denote a public known one-way function.

$PS \longrightarrow S_i : hello$
$S_i \longrightarrow PS : S_i$
$PS \longrightarrow S_i : PS_{s_i}, S_i$

During the network initialisation, the PS broadcasts a hello message to request sensors in its transmission range to transmit their IDs. When a sensor receives the hello message, it replies the message by transmitting its ID to the PS. On receiving this ID, the PS transmitts it ID to all sensors that did reply its hello message. At the end of this protocol, the PS will have the identity of sensor S_i also, S_i will have acquired the identity of PS. Hence, the two parties can compute the shared master key as follows.

At the PS we have $K_{mk} = f(PS_{s_i}, S_i)$
At S_i we have $K_{mk} = f(S_i, PS_{s_i})$

From the above master K_{mk} the sensor S_i can now compute a chain of session keys with the first one being $K_{ses_0} = F(K_{mk})$. It is clear to us that implementing security for CodeBlue based on this scheme is feasible since our protocol above forms part of the CodeBlue initialisation phase (Figure 3.4).

Adding new sensors: Ideally adding new sensors to the network amounts to running the protocol of partner discovery described in Section 4.4.4. No extra overheads are incurred since the user is given a finite set of on-body sensors which he can pre-load with the key material at once. Environmental sensors, which have to establish connections in different TEW-WSNs, have to be loaded with multiple sets of polynomials. This is done by electromagnetic induction with a short range of magnetic field in a secure environment.

4.4.5 Key revocation

In order to revoke compromised keys we need a mechanism of detecting corrupted keys, we propose a simple reputation scheme. The idea is to let sensors keep a small table on the abnormal behaviour (e.g., number of corrupt messages, long periods of inactivity, and faint signals) of their neighbours. Every sensor allocates two bytes of memory to keep reputation flags of each neighbour. The personal server also keeps a table of reputation of a sensor and its dependants using the same parameters. To get the reputation values from sensors, the personal server periodically polls a random set of sensors requesting them to send their reputation tables during their next transmission slot. Given our application scenarios (home and Mobile TEW), we anticipate the systems to encompass a few tens of sensors instead of hundred and thousands as the case with military applications. Thus, the size of a reputation table is indeed small. Below we define a simple reputation function.

Let the network consist of a set X of n sensors, $X = (S_0, S_1, ...S_{n-1})$. Let ϕ denote a reputation threshold, let C denote the number of corrupt messages received from a sensor or its dependants, let D denote the number of delayed transmissions, let f denote the frequency of corrupted messages, and let $Repu(S_i)$ denote a reputation of a sensor S_i.

Then, a sensor S_i in the network computes the reputation of its neighbour S_k as follows.

$$Repu_{S_i}(S_k) = \sum_{t=1}^{r} C_t + D_t \tag{4.11}$$

Where C_t and D_t are the number of corrupt messages and number of delayed transmissions during the transmission slot t for sensor S_k respectively. While r is number of transmission slots currently logged. The size of r is determined by the amount of memory allocated for reputation tables and in our case its two bytes.

The personal server also computes the reputation of a sensor S_k as the average reputation from $m - neighbours$ of S_k plus the independent reputation μ the PS calculates basing on the same parameters in Equation 4.11, and the factor f.

$$Repu_{PS}(S_k) = \frac{\sum_{i=1}^{m} Repu_{S_i}}{m} + \mu \tag{4.12}$$

$$Repu_{PS}(S_k) < \phi \tag{4.13}$$

If Equation 4.13 is true, a warning message is displayed on the users screen to check if the sensor is compromised and take appropriate action. Otherwise, the personal server allocates the sensor an infinite wait time until the user re-initialises the sensor.

5

Theoretical performance estimates

In this chapter we present in Section 5.1 theoretical security guarantee of our proposed KMS based on Shannon's mutual information theory [Tilborg, 2003] and the earlier work of Blundo et al. [Blundo *et al.*, 1992]. In Section 5.2 we discuss performance estimates of our scheme in terms of storage, computational, and communication resource requirements.

5.1 Theoretical resiliency estimates

Blundo el at. [Blundo *et al.*, 1992] already carried out an extensive theoretical analysis of a polynomial based KMS for dynamic conferences. Sánchez et al. [Sánchez & Baldus, 2005] extended this work to combinatorial to enable secure communication in a clustered network. The main question here is how secure are polynomial based schemes and in particular our scheme. We begin by giving a review of Blundo et al. security evaluations in Section 5.1.1, then we discuss the resiliency of and security guarantee of our scheme in Section 5.1.2.

5.1.1 Related work

By abstracting from the technical details of Blundo's et al. scheme, we note that for a group of users $(U_0, \ldots, U_{k-1})$ to compute a shared key, each user is preloaded with a secret piece of information β and a publically known derivation function f. Therefore, if user U_i wants to compute a common key for the set S, he computes $f(U_i, \beta, S)$. Based on Shannon's theory of mutual information [Tilborg, 2003], Blundo et al. proved that this scheme is secure against k colluding users, for $k < n$ in their attempt to recover keys shared between the $t = n - k$ users (n set of all users in the network) [Blundo *et al.*, 1992]. Therefore, the adversary needs to control $k = \alpha$ sensors, α being the degree of the polynomial in order to generate pairwise keys for the $n-k$ sensors.

From the concepts in Appendix A, it is easy to show that the mutual information given out by a set of colluding users about the non-compromised users is zero. i.e., let k and t be as defined above, then information leakage about the t given a set k of colluding sensors is define as

$$I(t : k) = H(t) + H(k) - H(t, k) \tag{5.1}$$

but

$$H(t, k) = H(t) + H(k) \tag{5.2}$$

since two sets of users are mutually exclusive [Tilborg, 2003]. Then, Equation 5.1 becomes.

$$I(t : k) = H(t) + H(k) - H(t) - H(k) = 0 \tag{5.3}$$

Hence, the scheme is secure against k colluding sensors in the network. i.e., an adversary cannot retrieve enough useful information from k sensors so as to derive shared keys among the $n - k$ sensors. For details, the interested reader is referred to the paper of Blundo et al. [Blundo *et al.*, 1992].

5.1.2 TEW-WSNs KMS resiliency estimates

Since our shared master keys are generated based on Blundo's el al. theory, then, the resiliency factor of the master keys equals that of Blundo et al. (i.e., colluding k-sensors in the network of n-sensors can not retrieve the pairwise master keys shared among the t-non-colluding sensors (for $t = n - k$)). Besides protection against colluding neighbours, our scheme achieves greater resilience against crypto-analysis by using three keys for different security services instead of one, i.e., the bootstrapped polynomial share for authentication, shared master key for integrity and derived session keys for encryption. Thus, learning the session key through crypto-analysis does not enable the adversary to construct valid messages, though he can generate forward session keys and read future transmissions. But, the number of future transmissions the adversary can eavesdrop is limited by the exposure he can gain from the system given the deployment architecture and transmission ranges. Hence, our scheme achieves graceful degradation, and offers improved security against crypto-analysis.

However, our scheme is not secure against physical attacks like magnetic induction since sensors are not tamper resistant. But, we make a bold assumption, that such attacks has a low probability of success since sensors are deployed in a relatively secure environment and any non-compliance to specification can easily be detected by the user. For example, a sensor which goes off-line abruptly and frequently triggers a warning message on the PS for the user to take action.

5.2 Resource requirement estimates

In this section we give theoretical estimates of memory requirements, computational, and communication costs of our scheme. Costs in our case refer to the energy in joules. We use the specifications of a generic sensor platform of 4kB of RAM, 128kB of program memory, 4kB of flash memory, 20kbps bandwith, and maximum packet size of 44 bytes i.e., the European Zigbee compliant wireless sensor.[1]

5.2.1 Memory requirement estimates

The sensor maintains a polynomial share, a master key, a session key, a routing table, and a reputation table. We allocate the reputation table for each neighbour r bytes (for $r = 3$ in our case), two bytes for the identity of the sensor, and one byte for the reputation value. If we consider the number of corrupt packets for a European standard Zigbee wireless sensor only (i.e. of bandwidth of 20kbps), then, the question is how many corrupt packets need to be counted to fill the one byte memory? We know that $20kbps = 20.000bps$ which is 2.500 bytes per second. But each packet is of size 44 bytes (Figure 5.1), hence, in one second the sensor can receive up to 56 packets of data. If we use a 1 second superframe with 20 time slots of 50ms each [Otto *et al.*, 2006], then during a given 50ms transmission slot a sensor can count a maximum of 3 packets as corrupt. Therefore, a sensor has to transmit at least 85 times before it can use up the available memory for the reputation table. For a small network like our TEW-WSN, this is sufficient for the PS to have downloaded the reputation values. Additionally, each sensor has to maintain a small routing table of three columns in which each row occupies $k$bytes ($k = 6$). Storage of a single univariate polynomial share of degree β,

$$f(x) = p(x, a_0, a_1, \ldots, a_{n-1}) = \sum_{i=1}^{\beta} a_i x^i \tag{5.4}$$

amounts to storing n coefficients of b bits and in our case $b = 64$bits, i.e., the size of the identical key. But n is dependant on β, i.e., $n = \beta + 1$ (in our case $\beta = 3$) and a variable x of size l. But the size of l is the size of the identity of the sensor in bytes, which in our case is 2bytes. The sensor generates session keys and a master key as well of size $64bits$. Let a sensor have t neighbours, then, the total memory requirement $S_i(m)$ for sensor S_i is estimated to be

$$S_i(m) = t \times (r + k + 16) + l + \frac{n \times b}{8} bytes \tag{5.5}$$

But as noted earlier t is small at any one time, since the WSN consists of a small number of sensors and besides, most sensors in the network establish direct links with the PS, hence, $S_i(m)$ takes a small fraction of the memory available on the sensor.

1 byte	1 byte	1 byte	2 bytes	2 bytes	0...31 bytes	4 bytes
Preamble	Delimiter	Time stamp	Destination address	Source address	Data	MAC

Figure 5.1: Zigbee compliant packet structure

[1] http://www.techonline.com/community/ed-resource/feature-article/36561

5.2.2 Computational estimates

Each sensor has to perform a number of security related operations which include:

1. Master key agreement and session key generation
2. Message Authentication Code (MAC) computation
3. Data encryption
4. Neighbour reputation computation

Master and session key agreement computational estimates: As noted earlier, agreeing a master key between two communicating parties amounts to evaluating the β degree bivariate polynomial at the two points represented by the identities of the parties, refer to Section 4.4.4. This costs β multiplications and β modular additions. Let these operations consume η joules.

Session key generation: The cost θ of generating a session key depends on the size of the input buffer and the number and type of operations in the one-way function. In our case the input is an integer n of b bits (where n is the master key and $b = 64$).

Data encryption and MAC cost estimates: Let κ be the costs of calculating the MAC and γ for encryption, by using the standard consumption rates 15μJ [Xbow, 2006, Oliveira *et al.*, 2005] for Mica2 for encrypting or decrypting 8 bytes of data using RC5. We note that, encryption of 32 bytes in our packet costs 60μJ ($\gamma = 60$).

Neighbour reputation costs: The cost of computing the neighbour reputation (denoted as ω) is equal to the cost of computing MAC for each packet plus the additional cost of counting their number and the number of delayed transmissions. Therefore the total computational costs $Comp_{S_i}(Costs)$ for sensor S_i are given by,

$$Comp_{S_i}(Costs) = (\eta + \theta + \kappa + \gamma + \omega) joules \tag{5.6}$$

5.2.3 Communication estimates

A Mica2 sensor, consumes 16.25μJ/byte and 12.25 μJ/byte for each transmission and reception respectively [Xbow, 2006, Oliveira *et al.*, 2005]. But additional communication costs because of security in our scheme are negligible since the signed and encrypted packet has the same size as the standard plaintext Zigbee compliant packet (i.e., 44 bytes). This is achieved by reducing the number of bytes in the data field and allocating them to the added security fields [ChipCon, 2006]. Hence, establishing the master key costs a sensor S_i.

$$Comm_{S_i}(costs) = 44 \times (16.25 + 12.25) \mu Joules \tag{5.7}$$

Which is the transmission and reception of a single packet. If a sensor has to communicate with n entities, then the total energy requirement for establishing master keys is given by Equation 5.8

$$Comm_{S_i}(TCost) = n \times 44 \times (16.25 + 12.25)\mu Joules \tag{5.8}$$

Also transmitting a reputation table of size r for a single neighbour costs the sensor S_i.

$$Comm_{S_i}(Repu_{cost}) = r \times 16.25\mu Joules \tag{5.9}$$

Therefore, for n neighbours, it will cost S_i

$$Comm_{S_i}(Repu_{cost_n}) = n \times r \times 16.25\mu Joules \tag{5.10}$$

But r and n are small in our case, yielding a maximum of 32 bytes of reputation value which is the size of a data field in the standard Zigbee compliant packet (Figure 5.1). Hence, the transmission of reputation values amounts to the transmission of a single packet. Thus, optimasing the communication costs.

We observe that implementing robust security primitives on a sensor comes with a price on performance, since a sensor has to perform the expensive bit operations in the process of delivering the various security services (i.e., authentication, encryption, and integrity). There is obviously a time delay in transmission because of these operations and for a large network it my result in a noticeable degradation in performance. Not only do these operations result in to delays in transmission but also in increased energy consumption, which causes the user to frequently replace batteries which rises questions about reliability, cost effectiveness, and user friendliness. Therefore, there is need to balance, the degree of security guarantee with cost effectiveness and performance by selecting just optimal security parameters. For example, we can let a sensor transmit raw waveforms encrypted with a 32 bit or 16 bit key instead of a 64 bit key. This reduces the number of modular bit operations at a reduced but sufficient security guarantee.

If we compare a sensor with no security implementations, the number and type of operation it performs are limited (i.e., it performs signal sampling, data formating, transmission, receiption, and routing). But a sensor with security enabled properties, in addition to the basic computations, it computes the MAC for each packet received, performs encryption, key agreement, reputation value estimates, and decryption. These operations may draw about five times more energy then a basic sensor operations.

6
Reflections and conclusions

In this chapter we give reflections on application of TEW services in developing countries particularly in Africa in Section 6.1. We present the opportunities, challenges, viable systems, and adaptions needed. We end the Chapter with conclusions of this work and thoughts on the future of TEW systems by highlighting areas that need further exploration.

6.1 Reflections

The potential of TEW services is particularly high in countries where specialists are few, and where distances and the quality of the infrastructure hinder the movement of physicians or patients. In most developing countries, particularly in Africa, populations are sparse, energy is in short supply, Internet connectivity and bandwidth are low though expanding fast[1], and the populations are averagely poor [2], hence making the implementation and sustainability of resource intensive, but critically needed TEW services (i.e., PHSs) a dream in many parts of the continent.

Therefore, in the light of the above, we note that for a foreseeable future PRSs are the most viable systems for delivering TEW services (Chapter 2). Indeed, the success of Ipath in the Solomon Islands and TeleCardio-FBC in the poor communities of northern Brazil confirms our claim. Since most of the data is in text format, the GSM network, which is well developed compared to the data network in most of these countries, can be relied on to provide connectivity among subscribers. However, PHSs can be modified to deliver primary health care services to terminally ill patients especially HIV/AIDS over the GSM network. Also, regional referral hospitals or local clinics could be linked to national referral hospitals to offer telemonitored surgery

[1] http://www3.sn.apc.org/

[2] http://www.povertymap.net/

and video conferencing. Below we present a hypothetical PHS application scenario in developing country.

Hypothetical case 2 *Imagine a village clinic/regional hospital with semi-trained medical personnel, a PC with an Internet connection, and a set of diagnostic tools (sensors) connected to the PC. When a patient arrives at the clinic or local hospital so to say, the local health care provider connects the patient to a remote specialist via a video/audio conferencing facility. The doctor then activates the remote diagnostic equipment at the local hospital/clinic. From his PC, he makes the diagnosis and types out a prescription, which is automatically displayed on the PC at the local clinic/hospital and the local practitioner can administer the medication. The entire process takes averagely the same time as personally seeing the specialist, but at a fraction of the cost. Thus, enabling specialists deliver the much needed specialised healthcare to a large community of remote patients.*

Apollo telemedicine foundation in India [Apollohospitals, 2006] is a good case study, although India has a well developed data network over the satellite (VSAT). For developed countries, PHSs hold the real promise of smart homes of the future. The infrastructure is well developed, component technologies have been tested, all that remains is optimal integration of these technologies and acceptability of TEW services in society.

The trend: Questions about the trend of TEW technologies still linger, like how many sensors will a user be wearing 10 to 20 years from now? what could be the new applications and technologies? And what will be the new security threats? Well, we state with conviction, based on the current trends in semiconductor and circuit integration advances [Philips, 2006], TEW research initiatives [Apollohospitals, 2006, Philips, 2006], and global health policies [UN, 2006] that the number of sensors per patient will not go beyond a few tens (less than 20). We envision multiple sensors being integrated into smaller devices with great processing capabilities as was the case in the evolution of PCs about 30 years ago. New applications could also be on the horizon, patients could be trained to carry out simple self tests using embedded electronic devices and home diagnostic tools. Some companies like Philips are exploring this area [Philips, 2006].

The success of PHSs, particularly in developed countries, will mainly depend on how medical practitioners perceive the usefullness of the systems as tools to enable them offer better services and improve their productivity. If they perceive them as threats to the values they believe in, then PHSs will have low acceptability. For example, losing control over patients as was the case with the national electronic prescription system in the Netherlands, which practitioners saw as a threat to their way of work [Boonstra1 *et al.*, 2004]. Also patients have moral and ethical concerns as well. For example, if the system relays incorrect information due to sabotage or malfunction and results in a loss of life, the question rises of who is to blame. However, the potential of general acceptability of PHSs is there given the fact that our world is becoming more competitive to the extent that any minor loss in productivity has a great impact on the over all progress of an individual or an organisation.

6.2 Conclusions

In this thesis, we have investigated the current trend in TEW research and development, we have highlighted the technologies, standards, services, and security implementations of a number of representative systems. From the study of these systems, we developed a framework which sufficiently describes any TEW system in Section 2.1. We categorised TEW systems into two: PHSs and PRSs. Based on the current trend in TEW research [Apollohospitals, 2006, Shnayder *et al.*, 2005, Otto *et al.*, 2006, Philips, 2006] and global health-care policies [UN, 2006] we assert that for a foreseeable future, PHSs will remain the most attractive systems for developed countries because of global productivity competitiveness and the availability of research while, PRSs will gain more in-roads in developing countries [Brauchli *et al.*, 2005, Apollohospitals, 2006].

From the general framework, we focus on the security properties of PHSs in general context and in the context of PHSs tier one (WSNs). We begin by investigating the different approaches to securing WSNs in general and TEW-WSNs in particular. We present the physical limitations of WSNs and the challenges of securing them. From these limitations and user requirements of TEW-WSNs, we present a number of security problems that need further investigation from which we select two areas of interest: threat modelling and KMS. We state that designing robust security does not entirely depend on robust cryptographic primitives but also, on optimal modeling of threats. We note that most of the current proposals rely on a generic threat models which do not take into account the unique requirements of TEW-WSNs. Thus, based on user and security requirements of TEW-WSNs, we develop a threat model (Section 4.3) for TEW-WSN home and mobile monitoring application and from this threat model, we propose a polynomial based KMS in Section 4.4.

We give theoretical security and performance estimates of our scheme. We note that our proposed KMS, which is optimal in communication costs, delivers strong resilient against inside attacks and crypto-analysis. Also, it offers a mechanism of detecting compromised keys. However, these security services are delivered at an increased computational and storage costs. We note that although the current technologies and cryptographic primitives are sound, securing WSNs is a problem due to resource constraints on sensors, but with advances in semiconductor and integrated circuits, we believe 10 to 20 years down the road, that small sensors of the size of a hand watch will have enough processing power to support robust cryptographic primitives currently implemented on PDAs.

There is need to implement a proof of concept for this work and investigate whether the theoretical perform estimates can be achieved in the real world application. Also a number of areas need further exploration and central to the challenge of securing WSNs is the need to design optimal, secure, and scalable KMSs. These scheme should cover key generation, distribution, update, detection of compromised keys, and their eventual revocation. Also, there is need to define efficient secure routing protocols that can mitigate traffic analysis and minimise the risk of denial of service attacks. Besides, there is a need to investigate which cryptographic primitive can offer greater resiliency at constrained resources, and which primitives are suitable for which application scenarios? For example, is RC5 a better solution in military application than elliptic curve cryptography. In addition to technical issues, their are organisational and social issues as well that have to be looked at for PHSs to gain acceptance in society.

References

[Anderson *et al.*, 2004] R. Anderson, H. Chan, and A. Perrig. Key infection: Smart trust for smart dust. In *Proceedings of the Network Protocols, 12th IEEE International Conference on (ICNP'04)*, pages 206–215. IEEE Computer Society, Octomber 2004.

[Apollohospitals, 2006] Apollohospitals. http://www.apollohospitals.com, March 2 2006.

[Bludau & Koop, 2002] H. Bludau and A. Koop, editors. *Mobile Computing in Medicine, Second Conference on Mobile Computing in Medicine, Workshop of the Project Group MoCoMed, GMDS-Fachbereich Medizinische Informatik & GI-Fachausschuss 4.7, 11.4.2002, Heidelberg*, volume 15 of *LNI*. GI, April 2002.

[Blundo *et al.*, 1992] C. Blundo, A. De-santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, London, UK, 1992. Springer-Verlag.

[Boonstra1 *et al.*, 2004] A. Boonstra1, D. Boddy, and M. Fischbacher. The limited acceptance of an electronic prescription system by general practitioners: reasons and practical implications. *New Technology, Work and Employment*, 19(2):128–144, 2004.

[Brauchli *et al.*, 2004] K. Brauchli, H. Oberli, N. Hurwitz, K. Kunze, G. Haroske, G. Jundt, G. Stauch, L. Banach, M. Wirdnam, M. Mihatsch, and M. Oberholzer. Diagnostic telepathology: long term experience of a single institution. *Springer-Verlag*, 444(5):403–409, May 2004.

[Brauchli *et al.*, 2005] K. Brauchli, D. O'Mahony, L. Banach, and M. Oberholzer. ipath a telemedicine platform to support health providers in low resource settings. *The Journal on Information technology in healthcare*, 3(4):127–235, 2005.

[Chan *et al.*, 2003] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, page 197, Washington, DC, USA, 2003. IEEE Computer Society.

[ChipCon, 2006] ChipCon. http://focus.ti.com/docs/prod/folders/print/cc2420.html, April 15 2006.

[Eschenauer & Gligor, 2002] L. Eschenauer and V.D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47, Washington DC, USA, November 2002. ACM press.

[Forslund, 2006] D. Forslund. http://openemed.net/background/telemed/, March, 10 2006.

[ipath, 2006] ipath. http://telemed.ipath.ch/ipath/, March 1 2006.

[Jovanov *et al.*, 2005] E. Jovanov, A. Milenkovic, C. Otto, and P.C. Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and Rehabilitation*, 2(6):10.1186/1743–0003–2–6, 2005.

[Karlof *et al.*, 2004] C. Karlof, N. Sastry, and D. Wagner. Tinysec: A link layer security architecture for wireless sensor networks. In *In Proc. Second ACM Conference on Embedded Networked Sensor Systems*, pages 162 – 175. ACM, November 3-5 2004.

[Lorincz *et al.*, 2004] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, M. Mainland, G .and Welsh, and S. Moulton. Sensor network for emergency response: Challenges and opportunities. *Pervansive computing, IEEE CS*, 3(4):16–23, October 2004.

[Maroti *et al.*, 2004] M. Maroti, B. Kusy, G. Simon, and A. Ledecze. The flooding time synchronization protocol. In *In proceedings of 2nd international conference on embedded networked sensor systems*, pages 39–49, Baltimore, USA, 2004. ACM.

[Moteiv, 2006] Moteiv. www.moteiv.com, March 20 2006.

[Oliveira *et al.*, 2005] L.B. Oliveira, H.C. Wong, and A.A. Loureiro. Lha-sp: Secure protocols for hierarchical wireless sensor networks. In *Integrated Network Management, 2005. IM 2005. 2005 9th IFIP/IEEE International Symposium*. IEEE, May 2005.

[Otto *et al.*, 2006] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4):307–326, 2006.

[Perrig *et al.*, 2002] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar. Spins: Security protocols for sensor networks. *Wireless Networks Journal (WINET)*, 8(5):521–534, September 2002.

[Pfleeger & Pfleeger, 2003] C.P. Pfleeger and S.L. Pfleeger. *Security in Computing*. 0-13-035548-8. Prentice Hall, third edition, 2003.

[Philips, 2006] Philips. http://www.research.philips.com/, June 2006.

[Pietro *et al.*, 2003] R. Pietro, L.V. Mancini, and A. Mei. Random key-assignment for secure wireless sensor networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 62–71, Fairfax, Virginia, 2003.

[Sánchez & Baldus, 2005] D. Sánchez and H. Baldus. A deterministic pairwise key pre-distribution scheme for mobile sensor networks. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 277–288, 2005.

[Shnayder *et al.*, 2005] V. Shnayder, B. Chen, K. Lorincz, T.R.F. FulfordJones, and M. Welsh. Sensor networks for medical care. Technical Report TR-08-05, Harvard University, Division of Engineering and Applied Sciences, 2005.

[Stallings, 2003] W. Stallings. *Network Security Essentials, Applications and Standards*. 0131202715. Pearson Hall, second edition, 2003.

[Tilborg, 2003] H.C.A. Tilborg. *Fundamentals of cryptology, A Professional reference and interactive tutorial*. 0-7923-8675-2. Kluwer academic publishers, third edition, 2003.

[TinyOS, 2006] TinyOS. http://www.tinyos.net/, March 1 2006.

[UN, 2006] UN. http://www.un.org/millenniumgoals, June 2006.

[Warren *et al.*, 2005] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov. Interoperability and security in wireless body area network infrastructures. In *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China,, September 1-4 2005. IEEE Xplore.

[Xbow, 2006] Xbow. http://www.xbow.com/products/productsdetails.aspx?sid=72, March 5 2006.

[Yang *et al.*, 2005] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh. Toward resilient security in wireless sensor networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 34–45, Urbana-Champaign, IL, USA, May 2005. ACM Press.

[Zia & Zomaya, 2006] T. Zia and A. Zomaya. A security framework for wireless sensor networks. In *SAS 2006 - IEEE Sensors Applications Symposium*, Houston, Texas USA, February 7-9 2006. IEEE.

[Zigbee-Alliance, 2006] Zigbee-Alliance. http://www.zigbee.org, April 11 2006.

List of Acronyms

ASP Active Server Pages.

CDMA Code Division Multiple Access. A technology for digital transmission of radio signals between, for example, a mobile telephone and a radio base station.

COAS Clinical Object Access Service. Its a scheme of authorising object access in OpenEMed system.

CORBA Common Object Resource Request Broker Architecture.

GPRS General Packet Radio Service. An enhancement to the GSM mobile communications system that supports data packets. GPRS enables continuous flows of IP data packets over the system for such applications as Web browsing and file transfer.

GSM Global System for Mobile communication. A European digital standard for mobile or cellular telephony.

HIPAA Health Insurance Portability and Accountability Act. The Act mandate standardised formats for all patient health, administrative, and financial data; unique identifiers (ID numbers) for each healthcare entity, including individuals, employers, health plans and health care providers; and security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual.

HL7 Health Level seven. It is a standard for healthcare and is the interface standard for communication between various systems employed in the medical community.

HTML Hyper Text Markup Language.

HTTP Hyper Text Transfer Protocol.

IEEE Institute of Electrical and Electronics Engineers.

ICT Information Communication Technologies.

ISDN Integrated Services Digital Network. An international standard for end-to-end digital transmission of voice, data, signalling.

ISO International Standards Organisation.

KMS Key Management Scheme.

NL The Netherlands.

PC Personal Computer.

PDA Personal Digital Assistant. A handheld computer for managing contacts, appointments and other simpler tasks.

PHS Patient Health remote monitoring System. Type of TEW system that facilitates real time remote monitoring and delivery of health care services.

PIDS Personal Identification Service. Its identity management service for OpenEMed system.

PIN Personal Identification Number.

PKI Public Key Infrastructure.

POTS Plain Old Telephone Service. The standard analog telephone service.

PRS Patient Record management System. These are TEW systems that focus on patient record management and facilitate the sharing of patient data among medical experts.

PS Personal Server. A devices that manages the TEW-WSN.

RADS Resource Access Decision Service. Difines the need to know constraints in OpenEMed system.

SNEP Secure Network Encryption Protocol.

SPINS Security Protocol for Sensor Networks.

SQL Structured Query Language.

SSL Secure Socket Layer.

VSAT Very Small Aperture satellite Terminal. A small earth station for satellite transmission that handles up to 56 kbps.

WAN Wide Area Network.

WBASN Wireless Body Area Sensor Network. Its a type of sensor network formed by sensors worn by an individual.

WAP Wireless Application Protocol. A specification that enables users to access information via handheld devices like pagers, smart phones, among others.

WLAN Wireless Local Area Network.

WSN Wireless Sensor Network.

TEW Telemedicine, E-health and Wellness. Means of providing medical and wellness services using information communication technologies.

TESLA Time Efficient, Streaming, loss-tolerant Authentication Protocol.

TEW-WSN Telemedicine E-health and Wellness Wireless Sensor Network. This is a sensor network the encampasses WSN and environmental sensors

2G Second Generation wireless. Is technology of encoding digital wireless phones on circuit switched networks. Most of the systems in the United States and Europe are using this technology.

Appendix
Shannon information theory

Below we review Shannon's information theory main concepts

Entropy:

Let X be a finite set of elements and $p(x)_{x \in X}$ be the probability distribution on X, then, the entropy of $X, H(X)$ is

$$H(X) = -\sum_{x \in X} p(x) log(p(x)) \tag{1}$$

The entropy has the property

$$0 \leq H(X) \leq log(|X|) \tag{2}$$

$H(X) = 0$ iff $\exists x_0 \in X$ s.t. $p(x_0) = 1$ and $H(X) = log(|X|)$,

iff $p(x) = \frac{1}{|X|} \forall x \in X$.
For two random variables X and Y defined on X and Y with joint probability distribution P(X=x, Y=y) i.e., $p_{x,y}(x, y) = p_{x|y}(x|y) \cdot p_y(y)$.
Then, the entropy of X give Y is defined as

$$H(X|Y) = -\sum_{i=1}^{n} p_{x|y}(x|y) log p_{x|y}(x|y) \tag{3}$$

In general conditional entropy is given by [Tilborg, 2003]

$$H(X|Y) = H(X) + H(Y) \tag{4}$$

However, if X and Y are independent variables, then the conditional entropy is defined as

$$H(X|Y) = H(X) \tag{5}$$

Also

$$H(Y|X) = H(Y) \tag{6}$$

Mutual information:

According to Tilborg [Tilborg, 2003] mutual information between the two variables is given by

$$I(X : Y) = H(X) + H(Y) - H(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \tag{7}$$