August 2012

Security on Medical Wireless Sensor Networks

Eric D. Southern

Supervisor
Dr. Abdelkader Ouda
The University of Western Ontario Joint Supervisor
Dr. Abdallah Shami
The University of Western Ontario

Graduate Program in Electrical and Computer Engineering
A thesis submitted in partial fulfillment of the requirements for the degree in Master of Engineering Science

SECURITY ON MEDICAL WIRELESS SENSOR NETWORKS: AUTHENTICATION, INTEGRITY, AND PROTECTION

(Spine title: Security on Medical Wireless Sensor Networks)
(Thesis format: Monograph)

by
Eric Duncan Southern

Graduate Program in Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Masters of Engineering Science

The School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

THE UNIVERSITY OF WESTERN ONTARIO
THE SCHOOL OF GRADUATE AND POSTDOCTORAL STUDIES

CERTIFICATE OF EXAMINATION

Supervisors	Examination Board
Dr. Abdelkader Ouda	Dr. Sylvia Osborn
Dr. Abdallah Shami	Dr. Luiz Fernando Capretz
	Dr. Raveendra K. Rao

The thesis by

Eric Duncan Southern

entitled

Security on Medical Wireless Sensor Networks: Authentication, Integrity and Protection

is accepted in partial fulfillment of the
requirements for the degree of
Masters of Engineering Science

Date	Chair of the Thesis Examining Board

Abstract

Wireless technology is fast becoming a very important tool for all aspects of communication. An area that lacks a strong implementation for wireless communication is the medical field. Wireless systems could be used by clinicians to be better able to diagnose and monitor patients. The reason behind the lack of adoption in healthcare is due to the need to meet the legislated and perceived requirements of security and privacy when dealing with clinical information. The current methods of wireless authentication are investigated and an existing issue in mobile networks is described and solved with two novel solutions; one solution within GSM and the other within UMTS. Strong authentication protocols are developed based on the existing wireless protocols, while using minimal messages and symmetric operations to limit resource utilization to meet the needs of the healthcare environment. To ensure the quality of the protocol a BAN (Burrows-Abadi-Needham logic) analysis is performed which verifies that the desired goals of the protocols are appropriately met within the results analysis. The developed security protocol is shown to be secure, uses minimal messages to maintain efficiency and meets the legal requirements to be used in medical wireless sensor networks.

Keywords: Medical Wireless Sensor Networks, Authentication, Integrity, Key Agreement, BAN Analysis, Mobile, Security, Privacy, HIPAA, and PIPEDA.

Dedication

This thesis is dedicated to my father who encouraged an understanding and passion for computers early in my life. I also dedicate this thesis to my mother who has given me support throughout every step of my educational career. Finally I dedicate this thesis to my son, Isaac, who with his every breath makes me achieve more and be more so that I can ensure the best possible future for him.

Acknowledgments

This thesis has been made possible with the guidance and help of several important individuals who in one way or another contributed and extended their valuable insight and assistance in the completion of this work.

Foremost of those contributors is Prof. Ouda who has helped me through every step of my career as a student here at UWO. He has given me invaluable insight into many areas of study relating to software engineering and has greatly enriched both my Bachelors and my Masters.

I would like to thank Prof. Shami for his assistance and guidance in helping to finalize my work and for his clarity in analyzing my submissions to greatly increase the quality of my output.

Many thanks go out to all of the educators in my life that have had a significant impact on my desire to extend my knowledge and continue learning throughout my life, including but not limited to, Madam Heidi, Mrs. Armstrong, Mr. Hamilton, Mr. Morrison, Mr. Goldberg, Mr. Lafontaine, Mrs. Stillman, Prof. Frost, Prof. M. Capretz and Prof. L. Capretz.

Glossary

3G - 3rd Generation of Mobile Telecommunications

3GPP - 3rd Generation Partnership Project

4G - 4th Generation of Mobile Telecommunications

AES - Advanced Encryption Standard

AK – Anonymity Key

AKA - Authentication and Key Agreement

AMF – Authentication Management Field

AMPS - Advanced Mobile Phone System

AP - Access Point

AS – Access Stratum

ASME - Access Security Management Entity

AUC – Authentication Center

AUTN – Authentication Token

AV - Authentication Vector

BS - Base Station

CBC - Cipher Block Chaining

CFB - Cipher Feedback

CK - Ciphering Key

CRC - Cyclic Redundancy Check

CTR - Counter

EAP - Extensible Authentication Protocol

ECC - Elliptic Curve Cryptography

EKE – Encrypted Key Exchange

EPS – Evolved Packet System

FIPPA - Freedom of Information and Protection of Privacy Act

GSM - Global System for Mobile Communications

GTK - Group Temporal Key

HAAA - Home Authentication, Authorization and Accounting Server

HIPAA - Health Insurance Portability and Accountability Act

HMAC - Hash-based Message Authentication Code

IK - Integrity Key

IMSI - International Mobile Subscriber Identity

ISP - Internet Service Provider

ITU - International Telecommunication Union

IV - Initialization vector

KDC – Key Distribution Center

KDF - Key Derivation Function

KEK - Key Encryption Key

LTE - Long Term Evolution

MIC - Message Integrity Check

MME – Mobile Management Entity

MSN - Medical Sensor Network

MWSN - Medical Wireless Sensor Network

NAS – Non-Access Stratum

OFB - Output Feedback

PDA - Personal Digital Assistant

PHI - Protected Health Information

PHIPA - Personal Health Information Protection Act

PIPEDA - Personal Information Protection and Electronic Documents Act

PKC - Public-key Cryptography

POTS - Plain Old Telephone Service

PTK - Pairwise Transient Key

RAND - Random Challenge

RRC – Radio Resource Control

SHA - Secure Hash Algorithm

SIM - Subscriber Identity Module

TKIP - Temporal Key Integrity Protocol

UE - User Equipment

UMTS - Universal Mobile Telecommunications System

USIM - Universal Subscriber Identity Module

WEP - Wired Equivalent Privacy

WPA - Wi-Fi Protected Access

WPA2 - Wi-Fi Protected Access 2

WSN - Wireless Sensor Network

WiMAX - Worldwide Interoperability for Microwave Access

Table of Contents

List of Figures

List of tables

Chapter 1

Introduction

Technological innovations for communication and computing have been advancing at an accelerated pace. The ability to co-ordinate and communicate between many devices by using wireless communication has had a major impact in many areas of life. One area that has seen slow advancement is medical care. There are many concerns about the security and integrity of the information created and stored in the systems that are being developed to help meet the needs of clinicians and patients. Patient privacy and safety are of major concern when applying many of the new innovations in wireless communication to the problems faced by the medical community. The general public is concerned about how their medical information is stored, transmitted and cared for. Clinicians are concerned about the quality and integrity of the medical data they receive. To help alleviate the

perceived issues of applying wireless technology to monitor patients, it is worthwhile to investigate existing security issues in wireless networks as well as how those issues have been resolved. By applying the experience gained from wireless deployments it will be possible to address the concerns and requirements of clinical systems, to ensure the safety of patients and staff.

Before wireless technology can be applied to the clinical environment, which will bring many benefits and advantages to clinical care, the security issues need to be addressed. The ability to remotely track patient information will allow clinicians a more robust picture of patient health. The extended time that patient information can be gathered will increase the understanding of the results of medical treatments and allow for stronger refinement of those treatments to create better results overall or tailored treatments for each patient. The technology will afford clinicians the ability to understand if a patient is in stable or in declining health over a long period of time.

1.1 Hypothesis

This thesis will investigate the needs of wireless communication in a healthcare setting and attempt to develop a protocol that will meet the needs of the legislation. The protocol will also need to use a minimum number of messages to achieve its desired goals of mutual authentication and key agreement. The protocol will avoid public key authentication to limit resource utilization and therefore it will require the use of symmetric operations or hashing. The protocol will need to be shown to be secure while achieving the desired mutual authentication and key agreement.

1.2 Methodology

To achieve the desired authentication protocol, different steps will be taken. First an investigation of current protocols will be completed focusing on protocols that are already in use in real world wireless communications. The protocols will be analyzed for their strengths and weaknesses as well as addressing those weaknesses. A protocol will then be developed that will meet the needs of the healthcare environment. The developed protocol will then be analyzed with existing theoretical analysis tools. Once the protocol has been successfully analyzed and shown that it meets the desired goals, we can be certain that it has met the stated hypothesis.

1.3 Contribution

This thesis proposes two different solutions to the issues brought about by the integration of the UMTS and GSM protocols. One solution focuses on minimal changes to the GSM protocol by modifying the key used for encryption with the use of a cryptographic hashing algorithm. The second solution to the problems brought about by the integration is a modification of the UMTS protocol and the integration equations to protect the communications. This thesis also proposes a new secure authentication protocol to be used in medical wireless sensor networks. The protocol has a minimum number of messages to ensure efficiency and to limit the resources needed for communication. The protocol avoids public key cryptography to reduce the resources required for authentication by using hashing similar to the mechanisms used in the existing UMTS-AKA protocol. The

protocol is also found to be secure using BAN analysis to be certain it meets the desired authentication goals.

1.4 Thesis Outline

The remainder of this thesis is organized as follows. Chapter 2 provides a broad background on many of the requirements, implications, and needs of medical wireless sensor networks (M-WSN) as well as information pertaining to security of wireless communication. In Chapter 3 we discuss authentication in existing 802.11 and mobile networks and the issues faced by those networks as they have adapted to new security challenges. A scenario on how an M-WSN would be used is discussed as well as how the authentication of the system is achieved and a formal verification that the authentication achieves the desired results are in Chapter 4. Chapter 5 discusses other privacy concerns and how they may be addressed. Chapter 6 concludes this thesis and offers future research directions and suggestions.

Chapter 2

Background

Technology has become a required tool for informed medical care. To address the concerns of how to properly apply our technological toolset to the medical problem space we need to properly meet the legislated needs of the countries in which the system would be deployed and address the privacy concerns of the patients and clinicians that will be gathering and using the information. This will help to develop acceptable systems that will meet the legislated needs of the organizations wishing to pursue the application of this technology with respect to medical care. It will also help to address the concerns of patients regarding the handling and control of their confidential information. With both the legislated requirements and the patient concerns addressed, it will lead to adoption of the technology to help increase the positive outcomes in patient care.

We will also be investigating the existing frameworks of sensor networks to understand how they handle the security concerns of each type of sensor deployment while working within the limited resources available on sensor nodes.

2.1 Legislated Requirements

Privacy of medical information is a very important requirement as the information has a large potential for abuse. To address the issue of privacy and security the United States, Canada and many other countries have developed legislative requirements on how the data can be handled by the organizations that need access to the information. Many different organizations need information related to MSNs that are deployed with patients. The clinicians, pharmacies and health care providers each need some, if not all, of the telemetry that is received from the sensors. Insurance providers need to know which MSN has been deployed with what sensor types and what billable actions have been taken with the system. Researchers need a variety of information collected to be able to conduct research and increase knowledge and positive outcomes of clinical care. Public health organizations may need information collected to understand if there is a public health issue in an area. The part of the requirements this thesis is concerned with are the regulations that most countries have in their legislation relating to how the information can be transmitted to ensure that there is limited opportunity for eavesdropping or modification of the information.

2.1.1 Health Insurance Portability and Accountability Act (HIPAA)

The United States passed legislation dealing with patient information that requires the establishment of national standards for electronic health care transactions and national

identifiers for providers, health insurance plans, and employers. HIPAA [1] required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. There are two rules that are the foundation of the legislation, the Privacy Rule and the Security Rule. The Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information while still permitting the disclosure of personal health information needed for patient care and other important purposes.

The patient has rights related to the health information collected and can request to see a copy of the health records. Patients can have corrections added to their health information, receive a notice that tells them how their information is used and shared, decide whether to give permission before information can be used or shared for certain purposes and get a report on when and why the health information was shared. The entities covered under the law must teach the people who work for them how patient information may or may not be used and shared and they must take appropriate and reasonable steps to keep your health information secure.

The Security Rule establishes national standards for protecting the integrity, confidentiality and availability of electronic protected health information (e-PHI). The requirements state that entities must ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain, or transmit. They must identify and protect against reasonably anticipated threats to the security or integrity of the information. They must protect against reasonably anticipated, impermissible uses or disclosures. They must also

ensure compliance by their workforce. The technical safeguards that are required are Access Control, Audit Controls, Integrity Controls and Transmission Security.

2.1.2 Personal Information Protection and Electronic Documents Act (PIPEDA) and Other Relevant Laws

Canada passed legislation that governs how organizations collect, use and disclose personal information in the course of business. Unlike the American legislation, PIPEDA [2] applies to all organizations that have access to personal information for commercial purposes. This requirement makes hospitals exempt from many of the regulations but physicians' commercial activities and private practice is covered under the law. Private group homes are also covered under PIPEDA and need to meet the requirements. There are laws that apply to hospitals and other primary care facilities on a provincial basis such as the Personal Health Information Protection Act (PHIPA) [3] and the Freedom of Information and Protection of Privacy Act (FIPPA) [4] in Ontario. PIPEDA requires that all organizations receive consent for collection of information, except in a few specific limited circumstances. The information can only be used or disclosed for the purposes for which consent has been given. Even with consent, the collection, use and disclosure must be limited to purposes that a reasonable person would consider appropriate under the circumstances. The law also requires that individuals have a right to see the personal information and the ability to correct any inaccuracies. The acts that relate to hospitals in the different provinces have many of the same requirements as stated in PIPEDA.

PIPEDA and the other laws generally require that safeguards be put in place to protect personal information against loss, or theft. The information must be protected from

any unauthorized access, disclosure, copying, use or modification. The information must be protected regardless of the format in which it is held.

2.2 Medical Wireless Sensor Networks (MWSN)

Wireless Sensor Networks will have a very large impact on many aspects of society from military applications to common household appliances. The application of WSN to the field of medicine will have widespread consequences in the gathering of medical information and giving a more robust picture of patient health. Sensor networks can give real-time information and telemetry to the clinicians that require the information to properly respond to medical situations and emergencies. A MWSN can track many different aspects of the patient including movement inside their home, their temperature and other bio-medical information such as oxygen saturation. The telemetry will help reduce costs for healthcare facilities by allowing patients to be remotely monitored instead of being in a facility for observation. There are a few different frameworks based on the Telos Mote[5] and Mica[6] Sensors. These frameworks generally use TinyOS [7] to efficiently manage and utilize their resources with many different deployment strategies to meet the differing needs of modern healthcare. Along with sensor information, there is a very real possibility of medication being delivered in minute doses to patients based on information gathered from medical sensor networks. The delivery of the medication would be controlled by wireless communication. When the information gathered from an MWSN reaches this level of integration with the medical care of patients, it is imperative that all communication be very secure with high integrity and availability so that no mistakes can occur and to be certain that the medication needed is the medication delivered to the patient

when needed. The types of sensor networks gathering the medical telemetry that can be used in the healthcare problem space are body sensor networks that are affixed to the patient or implanted inside the body and environmental sensor networks that gather information from the environment and are not physically connected to the patient and are usually stationary. We describe both types of sensor networks in the next two sections.

2.2.1 Body Sensor Networks

The sensors are applied directly to the body and monitor patient vital signs. The sensors will gather the information from the body and send it to clinicians for understanding and monitoring. The CodeBlue framework presented by V. Shnayder, et al. [8] shows a decentralized integrated MWSN for use in a clinical setting that will allow clinicians to query patient sensors to send vital information. The telemetry devices they use to collect data include a pulse oximeter, two-lead electrocardiogram, and a specialized motion-analysis sensor. They have built routing protocols to allow a clinician device to be able to query and receive data from these sensors while at a remote location in the medical facility. The CodeBlue framework lacks security and data protection. B.Sarikaya, et al. [9] integrate electroencephalography (EEG) sensors into the CodeBlue framework.

There are other frameworks that have encryption and integrity but lack authentication or key agreement such as Kumar, et al. [10] who have built a sensor system for monitoring patients; their example monitors Electrocardiograph (ECG) information. To ensure confidentiality of the data, they have used the Ping-Pong [11] encryption algorithm with the Ping-Pong MAC to ensure integrity. They proceed to develop a framework in [12] based on the original paper where they describe an application that allows the sensor

information to be presented to clinicians in a human usable format. Waluyo, et al. [13] have developed a centralized framework that has a personal digital assistant (PDA) or other powerful computing device as a sensor gateway. They have built the functionality for data collection as well as command and control within their network which is built on TinyOS on the sensors with a Java framework on the PDA. They have applied the SkipJack [14] encryption algorithm to their communication to ensure confidentiality. There is no method of Authentication and Key Agreement (AKA) as they have a single pre-distributed key for all devices.

A home network for health monitoring is proposed by Singh, et al. [15] which relies on stationary cameras, a PDA, body sensors, and home health controller system. This will then send the clinical information over the internet to a medical center. They use an Encrypted Key Exchange (EKE) [16] protocol for key distribution as well as a Key Distribution Center (KDC) to limit the impact of losing the PDA as a core device in the network. When establishing keys between body sensors the EKE uses user secure environmental values (SEV) such as Inter-Pulse-Interval (IPI) or Heart Rate Variance (HRV). Diffie-Hellman based EKE (DH-EKE) described in their work is used to establish a session key, SEV is used as the Encryption in EKE. They show how this uses fewer resources than Elliptic Curve Cryptography (ECC). PDA authentication uses KDC with a multiple server protocol (each of the cameras). The user enters a password into the PDA. This password is used as the encryption in the DH-EKE to authenticate the PDA against the cameras. All of the cameras then authenticate against the PDA sending secure information

allowing the PDA to authenticate the body sensor. As long as a minimum number of cameras return the proper values then the PDA is authenticated against the body sensor.

2.2.2 Environmental Sensor Networks

Environmental sensors are placed within an environment to track information on the patient and the environment which gives a holistic view of all conditions that the patient may experience. An example is the stationary cameras previously mentioned in a home network for health monitoring proposed by Singh, et al. [15]. Some sensors already exist in the home such as carbon dioxide and carbon monoxide sensors. Sensors can be added to the bed to monitor movement of bedridden patients to give information that would help clinicians reduce the occurrence of bedsores. Infrared and other types of sensors can be used in the environment to monitor patient bio-metric data without needing physical contact with the patient.

2.3 Authentication in Sensor Networks

Authentication schemes in sensor networks always need to consider the limited resources of the nodes that will need to authenticate themselves against the system. Sensor nodes have limited power, limited processing, and limited memory. When considering any protocols within this framework it is essential to reduce the overhead and processing to increase the life of the sensor while ensuring security. There are many different methods used to achieve secure authentication and key agreement. Symmetric key cryptography or the more resource intensive asymmetric-key cryptography such as ECC, and RSA can all be used to authenticate to a network. Authentication is an important aspect of MWSNs due to the need for a patient to get their data to the clinicians handling their care. Mutual

Authentication allows the patient to be certain that the network they connect to is the appropriate network and it allows the clinical systems/clinician to be certain of which patient is connecting to their system. Mutual authentication is also a very important factor in billing for medical services rendered by the sensor network (eg. monitoring, medications).

Collaborative Bloom Filters are used by B. Tong, et al. [17] to achieve authentication for devices that wish to connect to the sensor network in conjunction with a Merkle hash tree and ECC. When a node is added to the network it presents and authenticates itself to the other 1-hop nodes in the sensor network giving each of those nodes a share of its private key. If the node misbehaves then the 1-hop nodes can collaboratively use the information to discern the private key of the misbehaving node to add to the revocation list. M. Kim, et al. [18] present an adaptive mechanism that first relies on symmetric key authentication that as the node behaves properly it will eventually gain enough information to use a public key for authentication. This method relies on a shared common symmetric key for all nodes and it may be possible to discern the private key of the node if other nodes are compromised.

ECC is used as one of the two factors of authentication in Malasri, et al. [19]. The second tier of authentication is by using biometric data such as a fingerprint reader or a finger vein reader. The two factors allow for a more secure system compared to a single factor of authentication. They also propose that the data collected by the sensor be checked against the previous data as a method of ensuring the patient is the appropriate patient. If the data collected does not correspond to the patient then an alert will be raised. The issue

with this method of biometric authentication is that some patients will not present themselves at the healthcare facility in a desired biometric state required for the initialization of the biometric data. This will result in either alerts happening when the patient is no longer experiencing the undesired biometric state or with no alert going off when they are experiencing an undesired state.

Ren, et al. [20] use Public Key Cryptography (PKC) as they state that it is no longer impractical for WSNs. Broadcast authentication is used in their WSNs under the multiuser scenario by designing PKC based solutions with minimized computational and communication costs. Their approach allows for the following security actions - user authentication (illegitimate users will be excluded from injecting bogus messages), user revocation (sensor nodes can deal with user revocations), and authenticity of any message broadcast by a user should be able to be verified by every receiving node.

2.3.1 Authentication of Sensor Nodes

The sensor nodes will authenticate against each other or to a sink node. Sensor nodes generally have the least resources of any device in the network. In many different sensor networks the nodes will perform authentication against each other and to the network. The nodes will also try to detect attacks on the system when routing information through other nodes to a sink node for collection and possible transmission to the desired recipients. Most sensor networks have many nodes all of the same type to achieve the desired task such as intrusion detection into an area for military purposes. In a MWSN most of the sensors are specialized to be able to collect the appropriate information from the patient.

2.3.2 Authentication of Sink Nodes

These types of nodes are generally more powerful, can be a laptop or PDA, with greater resources and communicate the sensor information back to a more central system. The authentication of sensor nodes to the sink node will usually be less powerful than the authentication of the sink to the central system.

2.4 Key Agreement in Sensor Networks

Key agreement is required in a secure network to allow devices to begin to communicate securely and with integrity. Du, et al. [21] describe a methodology for an asymmetric pre-distribution key management scheme in a Heterogeneous sensor network. Their design has pre-distributed key pools to the sensors that allows for high probability of key agreement between sensor nodes. The nodes can therefore authenticate against each other by use of the pre-distributed keys. Camtepe, et al. [22] also propose a probabilistic key distribution methodology to increase the likely-hood that two sensors will be able to authenticate each other and proceed to communicate securely.

The proposed security framework for wireless medical sensor networks in Morchon, et al. [23] relies on cryptographic keying material, a lightweight digital certificate linked to the keying material and a security policy. This system is used to enable distributed key agreement by means of the multidimensional secure key establishment scheme and cryptographically enforced access control. Each node has keying material related to the main security domain as well as other keying material related to each of the sub-domains to which it has access. The design allows for quick and easy agreement between the medical devices such as a PDA and the sensors on the type of access allowed by matching the keying material.

2.5 Encryption and Integrity in Sensor Networks

The limited resources in sensor networks require the design of the security to be limited. To achieve confidentiality, Malasri, et al. [19] use the RC5 [24] encryption algorithm and to achieve integrity in their communication they use the SHA-1 [25] algorithm. Waluyo, et al. [13] use the SkipJack encryption algorithm to secure the information sent in their framework from passive eavesdropping. They do not have any integrity algorithms to ensure the quality of the communication and they do not have any protections against active attacks. The single key used on all devices will allow one compromised device to have full access to all information on their MWSN. The Ping-Pong and Ping-Pong-MAC algorithms used by Kumar, et al. [10] meet both of these requirements of confidentiality and integrity allowing the sensor to use similar algorithms to reduce the overhead in both of these operations. There are many tools used in security to achieve these goals such as stream ciphers, block ciphers and cryptographic hash functions.

Due to the limited resources available to sensor nodes it may be appropriate to use stream ciphers to secure the communication between nodes since they generally use less overhead and can easily be implemented in hardware. Ping-Pong, RC4, A5/1 and A5/2 are stream ciphers that are used to protect communication. RC4 is the algorithm used in WEP and it is also in active use by many websites such as Gmail, Amazon, and RBC. A5/1 and A5/2 are encryption algorithms used in GSM communication but these algorithms have serious flaws.

Block Ciphers generally require more resources than stream ciphers but there are many advantages of using block ciphers. Block ciphers are the most active area of

symmetric encryption research and they provide many different modes of securing the information that have been accepted by the National Institute of Standards and Technology [26]. One mode of operation is Cipher Block Chaining (CBC) which reduces the chance of using a dictionary attack on the cipher text as each input block is XORed against the previous block of cipher text. Other modes of operation that are very useful and allow the block cipher to act as a stream cipher are Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR). Counter mode has the added advantage of being able to be decrypted in parallel. Due to the increased complexity of block ciphers most cannot be easily implemented in hardware but the AES block cipher is able to be implemented in hardware.

Hash functions have many applications in security and allow for simple methods of ensuring integrity. Cryptographic hash functions take an input message and create a pseudorandom output message digest that is easy to compute given the message but it is infeasible to generate a message given the hash digest. It is also infeasible to modify a message without changing the hash or to find two different messages with the same hash. These properties make hashing a useful tool for integrity and for deriving pseudorandom keys.

Chapter 3

Wireless Authentication and Key Agreement

Wireless communications have revolutionized the way the world communicates. An important process used to secure that communication is authentication. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. The traditional method of authentication in computing is the challenge-response mechanism. There is a shared secret between the two parties that is used in an algorithm so that one party asks a question as a challenge and the other party must reply with a correct answer as a response. For any wireless communication to be secure there needs to be some type of authentication and key exchange to create that security. As flaws in the security of a wireless network are discovered new protocols and algorithms are

required to meet those security issues. When creating new algorithms and systems it is possible that the existing equipment may not be able to implement the new protocols, which means that integration may be required to transition from the old security protocols to the new more secure protocols.

Using a wireless medium for communication means that any attacker has full access to everything sent over the air and can use that information to attack, modify, and eavesdrop or any other activity if the information is not properly secured. Stationary wireless networks were created without a strong need to integrate protocols and have simply developed slightly more secure protocols to protect old equipment. New protocols in stationary wireless networks are implemented without integration as a requirement.

Mobile network security is constantly evolving and adapting to meet the needs of users and network operators. Mobile wireless networks have the requirement of allowing old equipment to use the entire network, as it is advantageous to allow new mobile equipment to connect to old networking equipment to increase coverage areas and for old equipment to be able to connect to new towers for roaming and billing. This requirement for mobile networks means that integration is required. Mobile networks originally had no security which proved to be a deployment nightmare that was attacked constantly and the providers were defrauded of millions of dollars. To address the security issues in mobile networks, the subscriber identity module (SIM) authentication protocols [27] were developed to secure the resources of the network providers. The original SIM security framework developed in Global System for Mobile Communications (GSM) networks had weaknesses brought about by the one way authentication protocol as well as weaknesses in

the algorithms used to secure the communication. The evolution of authentication in mobile networks to address the problems in the SIM framework brought about the creation of the universal subscriber identity module (USIM) protocols which are used in Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX) to secure the network from the SIM framework security issues. The integration of those two SIM and USIM frameworks brought forward the major weaknesses first found in the SIM framework.

This chapter discusses authentication in mobile wireless networks as well as the needs of those networks to interoperate and the security issues brought about by that integration. This will include a description of the authentication and key agreement (AKA) protocols of the legacy SIM based 2G GSM networks, and the modern USIM based 3G UMTS networks, 4G LTE networks and WiMAX networks. The authentication protocols in the new generations of mobile wireless networks are designed to interoperate (not replace) the existing protocols as the infrastructure for the existing system is deployed nationally and is very expensive to replace requiring time, effort and expense. Therefore the integration of the different protocols to allow this interoperation gives the mobile operators the ability to upgrade their networks while still maintaining coverage for their customers. The protocols and methods used for the integration of the legacy systems into the modern AKA systems will be discussed. We explore simple and effective solutions to reduce the possible attacks on the USIM protocols due to the above integration. First we propose a subtle modification to the SIM based GSM security protocols as a stand-alone solution, and then a modification to the USIM based UMTS security protocols is proposed

as a second solution. When considering authentication in an M-WSN we need to investigate the common methods of wireless authentication that have already been deployed and therefore have undergone a large amount of scrutiny and have been able to withstand many different vectors of attack.

It is worth mentioning that the integration of the old (flawed) security protocols is not always the right option. For instance, the new authentication protocol described by IEEE 802.11i to protect stationary wireless networks replaced (did not interoperate with) the legacy Wired Equivalent Privacy (WEP) due to the problems found in the earlier algorithms and protocols. Southern, et al. [28] compared the differences between the interoperation solution in mobile networks and the replacement solution employed in stationary wireless networks.

3.1 Evolution in Wireless Communications

Wireless communication allows for easy connectivity of devices without the expensive requirements of laying a physical network. One of the main difficulties in deploying wireless networks is the ability to secure information and resources on a medium that by its very nature broadcasts all information. A key aspect of securing wireless communication is the authentication protocol used to allow access to the network. The two major types of wireless networks are the stationary networks generally defined by the IEEE 802.11 standards and the mobile networks defined as 2G, 3G and 4G networks. As security requirements have changed, the protocols for authentication have adapted with those changes. Both of these network types have faced significant security problems that have needed to be addressed with stronger protocols and more secure cryptographic

algorithms. When creating the new more powerful algorithms and protocols the older hardware cannot implement them due to the more strenuous requirements.

The demands on mobile communication and networks have been constantly increasing. Originally the need was simply to have a phone system that could meet most of the requirements of the standard plain old telephone service (POTS) in most homes. The original first generation (1G) systems, such as the advanced mobile phone system (AMPS), were analog cellular networks which met this need without considering the inherent issues that arise due to using a wireless medium as opposed to a wired one. Security was a major issue that was not properly addressed when developing the 1G systems and therefore the phones were susceptible to cloning. This was due to the phones broadcasting their identities without encryption or integrity when phone calls are placed. Attackers could then take this information and apply it to their own phone to then use it to connect to the provider network allowing them to call anywhere without having a legitimate account with the provider. The cloning defrauded many providers of large amounts of money while inappropriately making unauthorized use of their resources. Securing resources against inappropriate use is one of the many benefits and requirements of security in mobile wireless communication.

The second generation of mobile communications (2G) strove to solve the phone cloning issue and while meeting the expanding requirements of consumers with GSM/2G networks. GSM networks also addressed some of the issues with using a wireless medium when sending information. The new network authenticates the user against the network in a cryptographically secure method to limit the potential of phone cloning security issues as

well as ensuring that the network resources are not accessed inappropriately. This made phone cloning a much more difficult proposition for attackers to inappropriately make use of provider networks, while allowing providers to be much more certain that their resources were not being fraudulently used by unauthorized devices. The problem with GSM networks was that they did not appropriately protect the user from many other types of attacks, such as the false base station attack that would allow an attacker to listen in or modify the communication from the GSM user. The false base station attack and other security issues in GSM networks were attempted to be resolved by providers with the third generation of mobile communication (3G).

3G mobile communications allowed for much better use of the spectrum available allowing much "smarter" devices to be on the network. Even though the cloning issue was mostly resolved with the GSM networks there were other security issues that needed to be addressed in universal mobile telecommunications systems (UMTS) networks. To address these new issues the 3rd generation used mutual-authentication between the mobile device and the provider network. The UMTS networks also have much higher speeds for IP communication to allow for users to make extensive use of the network resources.

The next generation of mobile communication will make even further use of the available spectrum and increase the ability of smart devices to do much more robust communication with media and other applications. The authentication in the fourth generation (4G) is still going to be the same authentication protocols as the USIM 3G to make certain that resources are not misappropriated. 4G long term evolution (LTE)

networks will allow wider bandwidths, higher efficiency and a fully IP network for all communication.

GSM networks had by far the largest installed base of users with over 3 billion GSM devices in use around the world [29]. This large market of devices has made it a business requirement of all providers to allow for the legacy GSM system to be integrated into new systems to ensure that these users can use the network resources and be billed appropriately for that usage. The interoperation of legacy systems needs to be executed with the utmost care to ensure that issues in the legacy system do not manifest themselves in the new integrated system. There are many security concerns when integrating legacy systems and the evolution of those systems to handle new requirements. The authentication done in the GSM network was maintained in the new UMTS networks to allow these devices to connect. This integration allows some of the security issues in GSM networks to be exploited in the new network.

3.2 Authentication in Mobile Wireless Networks

When authenticating against a mobile wireless network the mobile equipment needs to be able to send from one base station to another without a loss of communication or interruption to an active connection. The requirement to roam without interruption forced the development of a network that would allow a user to be able to authenticate to and use all parts of the network seamlessly. A major difficulty faced by mobile networks is the ability for a user to roam from one network operator to another network operator which allows mobile network providers to bill foreign users and systems. This support limits the control a network provider has over the hardware connecting to their network. These

networks also tend to be built out nationally, a very large investment, which needs to be leveraged as long as possible to have connectivity for all users. Some users are also likely to keep a functioning phone for a much longer time than a functioning laptop. GSM phones will operate as a worthwhile and functioning phone for more than a decade which to many users that means there is no reason to upgrade their device.

3.2.1 SIM-based Authentication Mechanism

Mobile service providers needed to secure their networks from attack and misappropriation of networking resources. In the attempt to achieve the goals set out in GSM of protecting access to mobile services and to protect any relevant item from being disclosed on the radio path [30], the GSM security protocols were developed. There are many technical constraints that needed to be addressed when adding security to mobile communication. When authenticating against a mobile wireless network the mobile equipment needs to be able to send from one base station to another without a loss of communication or interruption to an active connection. The requirement to roam without interruption was a major factor in development of mobile networks that would allow a user to be able to authenticate to and use all parts of the network seamlessly. The authentication protocol deployed to address these problem was the SIM based GSM protocol.

The authentication in GSM is a one-way authentication algorithm to authenticate the mobile device to the service provider network. As shown in Figure 3.1 the algorithm uses a secret key K that is shared between the GSM home network and the mobile device. The mobile device identifies itself to the network by sending its international mobile subscriber identity (IMSI) to the base station (BS). The BS forwards the IMSI to the home network of

the device. Based on the IMSI the home network recognizes the corresponding key *K* that is used along with a random challenge (RAND) to generate a session key K_c =A8(RAND, *K*) and the expected response to the challenge SRES=A3(RAND, *K*), where A8 and A3 are two hashing functions. The home network sends the authentication vector (RAND, SRES, K_c) to the BS who will retain SRES and K_c and sends the RAND to the mobile device as a challenge. Using the shared secret key *K* along with the received RAND the mobile generates the response SRES' and generates the same session key K_c. The mobile device responds to the BS with the SRES which the BS then matches against the SRES to verify the identity of the mobile device. This authentication in GSM gave the service providers the ability to address the issue of cell phone cloning by issuing a challenge to the device that would appropriately be responded to with the SRES'. GSM also added encryption using the key K_c to the channel to allow the confidentiality on the information transmitted across the air interface.

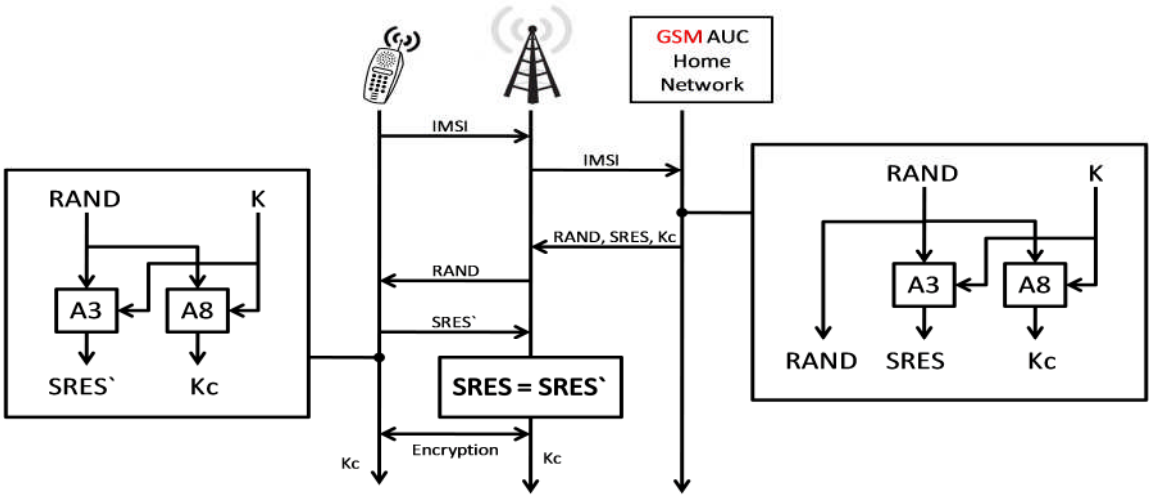


Figure 3.1: GSM Authentication Protocol.

Even with all of these new security enhancements to wireless communication, there are many problems with the authentication and security in GSM. The encryption and hashing algorithms were developed in secret design, in violation of Kerckhoff's principle [31]. It says a cryptosystem should be secure even if everything about the system, except the key, is public knowledge, which led to the system being less secure than if they had used known algorithms that had been vetted by cryptographers not involved in the design. In addition, the stream cipher A5 is used for encrypting the communication channels. The adopted A5/1 encryption algorithm in GSM can be broken in real time [32] and the A5/2 algorithm is easily broken in seconds [33] meaning that the intent to keep communication of the customer on the network private is no longer truly provided by the protocol. The GSM framework does allow providers to choose different algorithms for both the hashing and encryption but due to the established base and weaknesses in the protocol this is not entirely feasible for the encryption protocol (hashing protocols can be set specifically for each device at the discretion of the provider). The XRES and other values are also limited by their length as required in the GSM protocol.

The authentication protocol has many flaws that allow for denial of service, and false base station attacks since the subscriber does not authenticate the network. Note that, GSM uses one-way authentication. A false base station attack is visible due to the mobile device not authenticating the network. The false base station attack is a classic man-in-the-middle attack that generally passes most of the communication from the handset to the tower but will modify some of the transactions to attack the network. These attacks have a method that can retrieve the IMSI of the device and they can have the false tower also force the

device to not use encryption for communication which allows the attacker to listen to the conversation and possibly inject information into the channel. Again, the fact that GSM protocol authenticates only the phone and leaves the network unauthenticated allows for these base station attacks to neutralize any increase in the quality of the encryption algorithms since the devices will support the older implemented algorithms and no encryption. The insecurity brought about by the protocol allows these attacks to compromise the confidentiality and integrity of the user communication with the network.

3.2.2 USIM-based Authentication Mechanism

3.2.2.1 UMTS-AKA Authentication Protocol

UMTS networks have mutual authentication in which the mobile device is authenticated to the network as well as the network authenticating the phone as shown in Figure 3.2. This mutual authentication allows the device to discern whether or not the network they are connecting to is a legitimate network. The authentication protocol also makes use of integrity to ensure that the communication is not modified when selecting algorithms for encryption and integrity. The authentication protocol follows many of the same network steps in the GSM protocol with some important changes. The authentication token AUTN as well as the integrity key (*IK*) are sent from the home network. The AUTN token along with the RAND are then sent to the mobile device which processes the RAND with the key to verify the AUTN token by validating the MAC section of the token sent from the network against the XMAC created by using the key, sequence, authentication management field (AMF), and RAND. Note that, AMF is a section of the AUTN token.

The mobile equipment also does a validation of the sequence to ensure that it is within the desired range. This verification allows the mobile device to trust the connection to the network.

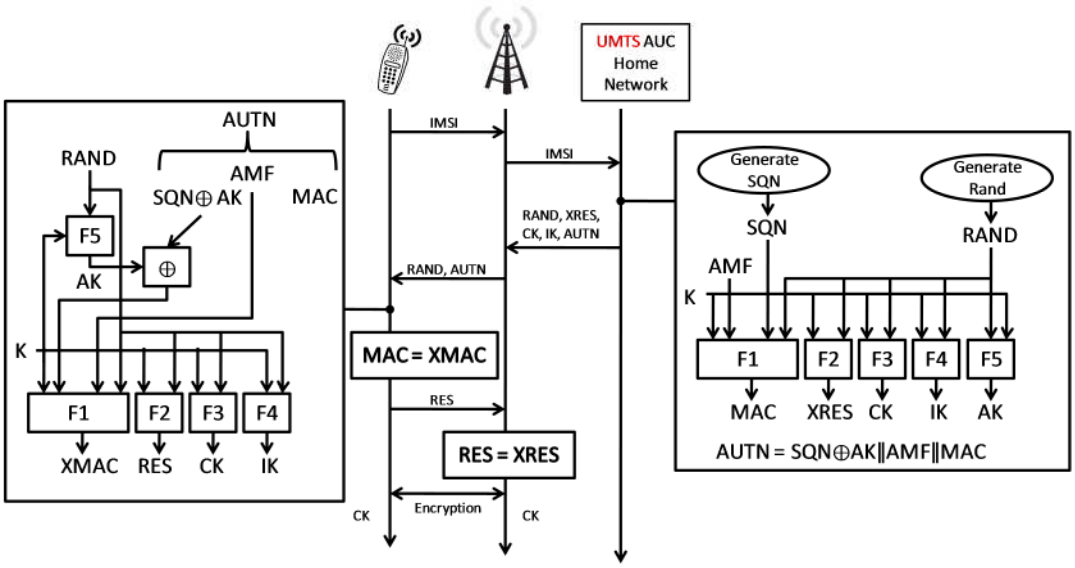


Figure 3.2: UMTS Authentication Protocol.

The algorithms are at the discretion of the providers but generally the Kasumi [34] algorithm is used for both integrity and encryption with an option of no encryption. The UMTS protocol does not allow the system to operate without integrity, which in conjunction with the authentication allows the mobile device and network to have a reasonable expectation that there has been no modification of the communication. This method of authentication with integrity limits many attacks in a purely UMTS network. The Kasumi algorithm is a modified MISTY1 algorithm that was chosen for its suitability for implementation in hardware. The algorithm has some weaknesses but is not susceptible to real-time attacks [35]. Currently the ITU (International Telecommunication Union) is

still developing the standards for 4G mobile communications but the authentication protocols are the same as those of the UMTS network [36].

3.2.2.2 EPS AKA, LTE Authentication Protocol

LTE networks were developed to meet the growing mobile data usage of users. The new network moved voice off of a circuit switched network to a packet switched IP based VoIP protocol. There is better utilization of the bandwidth and increased speed and capacity available for providers to meet the constantly growing needs of their users.

LTE networks have expanded the authentication key agreement used in UMTS. The beginning of the protocol is identical with the IMSI request being forwarded by the base station to the authentication center (AuC) as can be seen in Figure 3.3. The changes begin with the evolved packet system (EPS) authentication vector (AV) which has RAND, AUTN, XRES, and K_{ASME} which is the access security management entity (ASME) instead of *CK* and *IK*. The *CK* and *IK* values in the USIM along with the serving network's identity are the input into a key derivation function (KDF) to generate K_{ASME}. Then the similarities to the UMTS protocol continue with the user equipment (UE) validating the MAC and then responding with the RES for the network to complete the authentication procedure by comparing it with XRES. The major change in EPS is that the K_{ASME} is used to generate keys in a key hierarchy. Keys are generated for three different traffic types: the non-access stratum (NAS), access stratum (AS) and radio resource control (RRC).

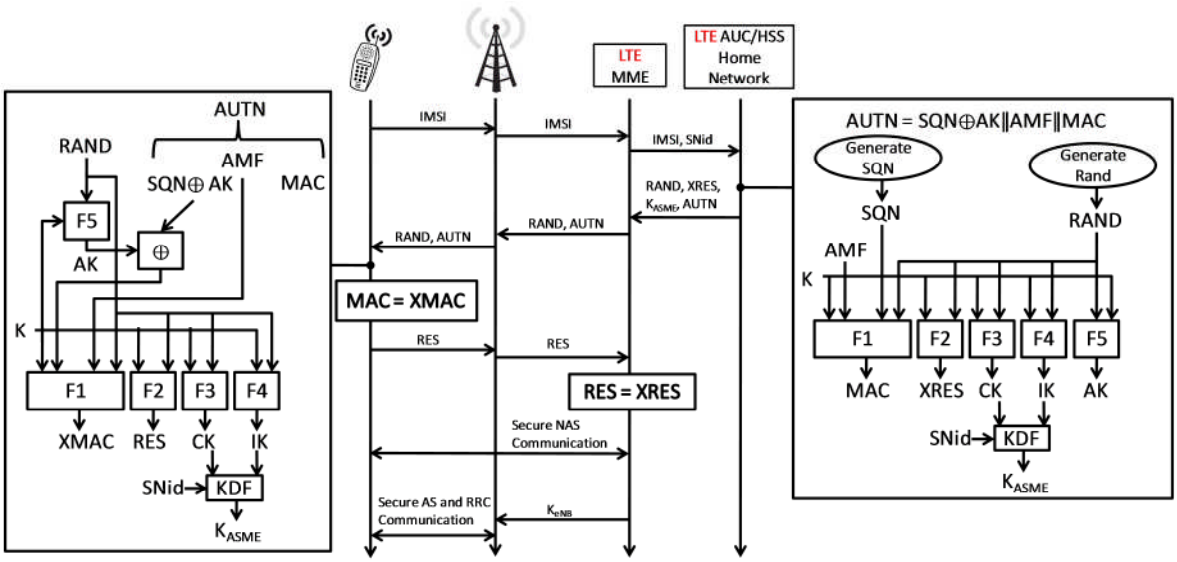


Figure 3.3: EPS-AKA Authentication.

The Key Agreement within the EPS-AKA protocol allows for 6 different keys to be generated as shown in Figure 3.4 which shows the different equipment that will be used to derive each key, as follows.

- *K* is a 128-bit secret key stored permanently in USIM and AuC.
- *CK* and *IK* are a pair of 128-bit keys derived in AuC and USIM during the AKA process.
- K_{ASME} is a 256-bit intermediate key derived in the home subscriber server (HSS) and UE from *CK* and *IK*, during the AKA process. K_{ASME} is then forwarded to MME as a part in the EPS AV along with RAND, XRES and AUTN.
- K_{eNB}, K_{NASint}, K_{NASenc}, are 256-bit Intermediate Keys derived in MME and UE as well from K_{ASME} when UE transits to EPS Connection Management ECM state or by UE and target base station eNodeB (eNB) using the previous K_{eNB}

during eNB handover. K_{eNB} is then forwarded to the eNB. K_{NASint} is an integrity key for protection of NAS data derived in MME and UE. K_{NASenc} is an encryption key for protection of NAS data derived in MME and UE.

- K_{UPenc}, K_{RRCint} and K_{RRCenc} are 256-bit keys derived from K_{eNB} in eNB and UE. K_{UPenc} is an encryption key for protection of user data derived in eNB and UE. K_{RRCint} is an integrity key for protection of user data derived in eNB and UE. K_{RRCenc} is also an encryption key for protection of RRC data derived in eNB and UE.

Therefore, these keys are all based off of the pre-shared key *K*. They follow the same processes in UMTS as is evident in Figure 3.3 which are used to generate the different keys and values required for the key agreement and authentication. The difference arises when the keys *CK* and *IK* as well as the serving network identity (SNid) are used as input into a key derivation function KDF generating K_{ASME} which is then used to generate all the other keys.

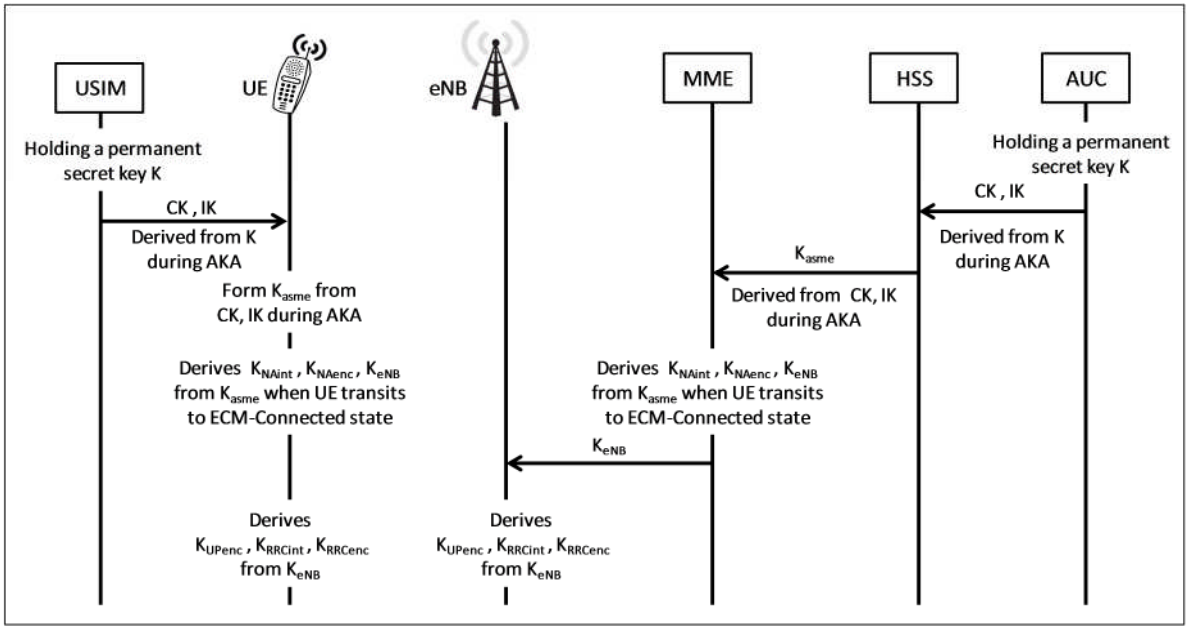


Figure 3.4: EPS-AKA Key Derivation.

The authentication and key agreement in EPS-AKA has identical steps for mutual authentication as UMTS only the key agreement and which devices perform the key generation steps differ.

3.2.2.3 EPS AKA, LTE Authentication Protocol

Worldwide Interoperability for Microwave Access (WiMAX) is an IP based, wireless broadband access technology that provides performance similar to 802.11/Wi-Fi networks with the coverage and quality of service (QOS) of cellular networks. In a fixed wireless configuration it can replace the telephone company's copper wire networks, the cable TV's coaxial cable infrastructure while offering Internet service provider (ISP) services. In its mobile variant, WiMAX has the potential to replace cellular networks. It is an IEEE standard designated 802.16-2004 (fixed wireless applications) and 802.16e-2005 (mobile wire-less).

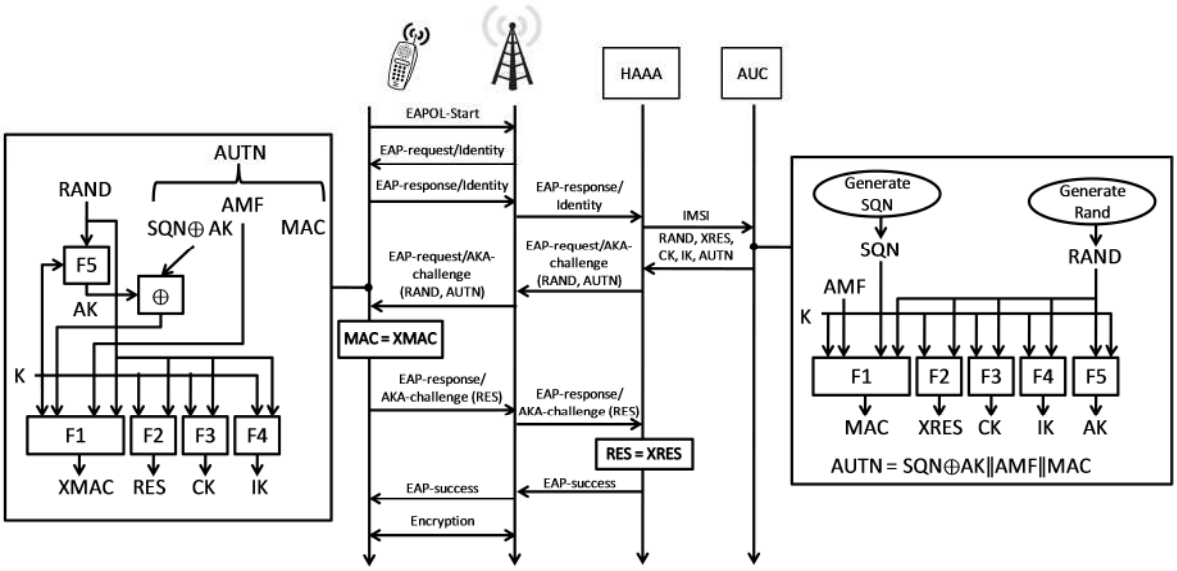


Figure 3.5: EAP-AKA Authentication.

To allow connections to WiMAX by current USIM cellular devices an extensible authentication protocol method for UMTS Authentication and Key Agreement or for short EAP-AKA was developed to integrate the UMTS-AKA algorithm into the extensible authentication protocol (EAP) framework as seen in Figure 3.5. The start of the protocol requires the UE to initiate the connection with the access point (AP) by sending an EAPOL-Start message. The AP will then respond with the EAPOL-request/identity message. The remainder of the protocol is very similar to the UMTS-AKA algorithm but with the elements wrapped in their equivalent EAP message types. Therefore the UE will respond to the EAPOL-request/identity message with an EAPOL-response/identity which contains the IMSI of the USIM. The IMSI will be sent from the AP to the home authentication, authorization and accounting server (HAAA) which will control all future communication with the UE through the AP. The HAAA will then forward the IMSI to the AuC which will then create the authentication vector, identical to the one created in UMTS.

The AuC will send the authentication vector of *CK*, *IK*, RAND, XRES, and AUTN to the HAAA. The HAAA will then send an EAP-request/AKA-challenge containing the RAND, AUTN, and MAC to the UE. The UE will verify the MAC and respond to the HAAA with the RES in an EAP-response/AKA-challenge message which is then to be validated by the HAAA. The HAAA will then respond with an EAP-success message.

The EAP framework adds some extra overhead to the UMTS-AKA protocol with the addition of the EAP standard messages that complete the requirements of the EAP framework but the overall protocol uses the same messages and mutual authentication requirements.

3.3 Authentication in Stationary Wireless Networks

To understand the security environment in mobile wireless networks it is worthwhile to review the security in stationary networks since both types of networks have undergone a phase of broken security and a migration of equipment from the less secure to more secure environments. Stationary wireless networks allow user equipment to connect to a network without the need of a physical wire. This allows for more user mobility and to create a network quickly and in environments where it is difficult or expensive to deploy physical networks. Generally, there is no need in these types of networks to manage the mobility of the user from one network access point to another as the connection does not need to be maintained if a user roams from one network area to another. The main difference for stationary networks is that the wireless users generally have modern or more powerful equipment that connects to the network and the network operator will generally have more control over all devices on the network. Stationary network providers did not

have the same need to make their network allow access to old devices. Another major consideration in the evolution of security in stationary networks is that the equipment manufacturers were in control of the development and migration of the security framework and therefore did not have a strong vested interest in maintaining older hardware and would prefer to sell the new hardware that meets the new standard.

3.3.1 Wired Equivalent Privacy

The first type of security devised for wireless communication in the 802.11 standard is WEP. The algorithm relies on a shared Key (WEP key) of 40 bits or 104 bits as well as an Initialization Vector (IV) of 24 bits. As can be seen in Figure 3.6, WEP authentication process starts when a user equipment UE requests to associate with the access point AP, where UE must authenticate itself to the AP. Based on this request, AP sends a challenge nonce R (random number) to the UE, and waits for the response. The UE then encrypts the challenge R using a stream symmetric cipher RC4 as follows.

- The challenge R is first checksummed using CRC32 that is added to R to form the data payload.
- Then the UE creates a 24-bit random initialization vector (IV).
- The IV and the WEP key are used as a seed to generate RC4 key stream K.
- The ciphertext is produced by XORing the key stream K with the data payload.

UE then transmits the ciphertext and the IV to the AP as its response. The AP uses the IV that it received and the shared WEP key to decrypt the data and verify the

checksum. If a match is found, the authentication declared successful and the association is formed.

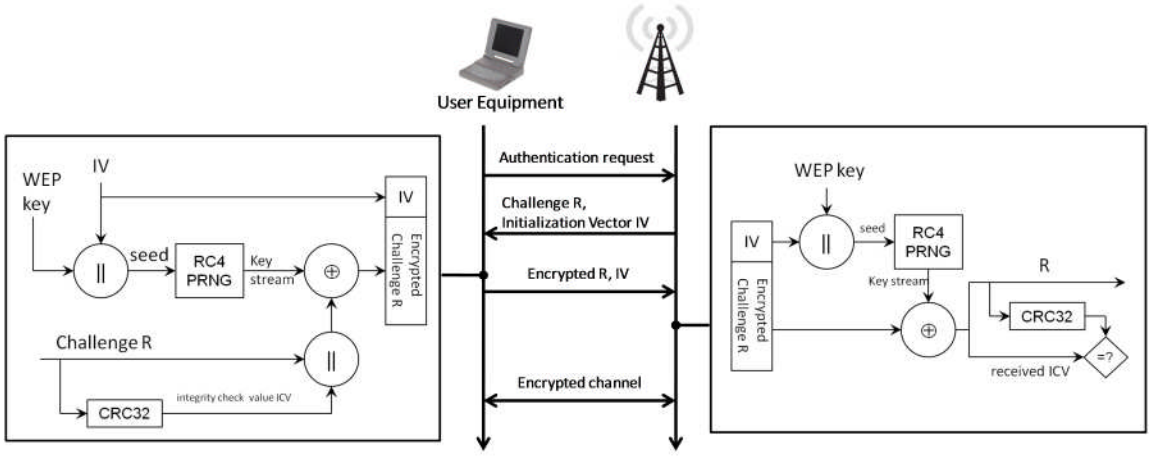


Figure 3.6: WEP Authentication Protocol.

Note that the cryptosystem used in WEP is a stream symmetric cipher RC4, and the key that encrypts the data is the same key that will be used for decryption to recover the data.

Scott Fluhrer, et al. [37] describe in their work titled "Weaknesses in the Key Scheduling Algorithm of RC4", a number of weakness in the WEP protocol. The flaws are related the way RC4 was implemented. They have mentioned that WEP can be cracked if enough traffic can be intercepted. This is because there are only 16 million possible IV's (24-bit), so after intercepting enough packets, there are sure to be repeats in the IV's. When IVs repeat, the RC4 key stream can be easily discovered and hence a known-plaintext attack can be utilized to recover the plaintext without the need for the WEP key. The end result is that WEP has suffered from key management problems, implementation errors, and overall weakness in the encryption mechanism.

3.3.2 Wi-Fi Protected Access (WPA)

The major flaws in WEP made it necessary for the Wi-Fi Alliance to create a stronger protocol to increase the security of wireless networks without replacing the legacy hardware. There was a rush to create a more secure wireless network and therefore WPA was developed as a pre-standard 802.11i protocol that would be able to be loaded as an update to most WEP firmware and would improve the security of existing wireless networks until the 802.11i protocol could be ratified. WPA has the endorsement of the Temporal Key Integrity Protocol (TKIP) and Message Integrity Check (MIC) by the Wi-Fi Alliance. Authentication under WPA is completely different than that in WEP as shown in Figure 3.7.

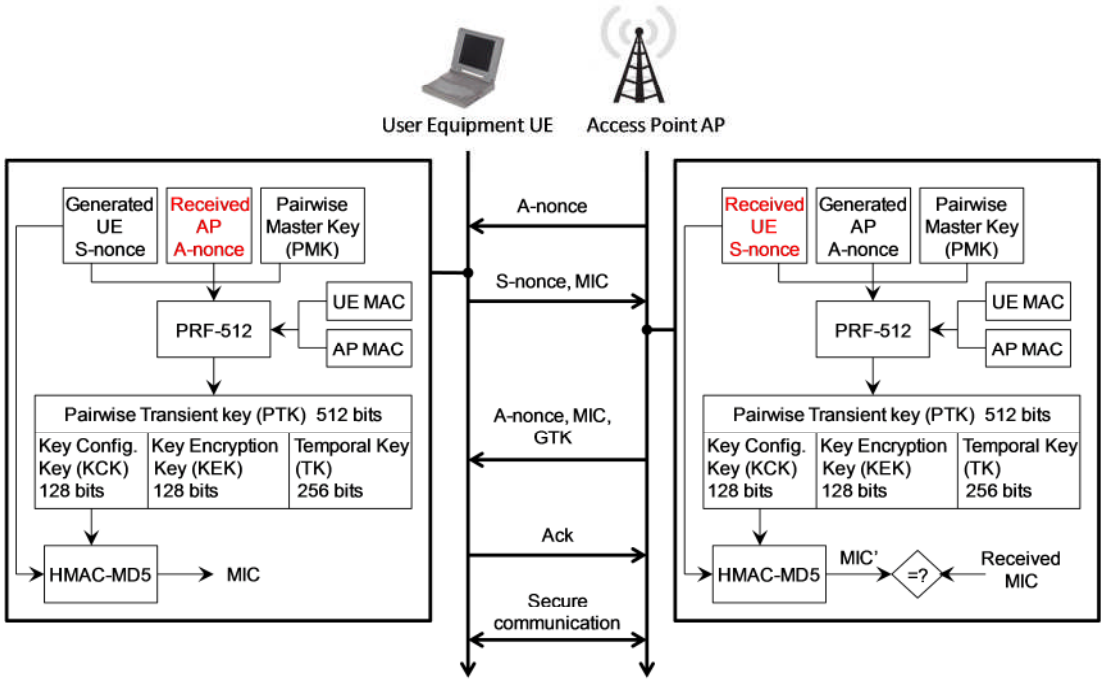


Figure 3.7: WPA authentication against the access point.

The AP sends a random A-nonce to the UE. The UE takes the Pairwise Master Key (PMK), a pre-shared key given to the UE and AP, the received A-nonce, a generated S-nonce, along with AP and UE MAC addresses to compute a Pairwise Transient Key (PTK). This is done by using the Pseudo-Random Functions PRF-512. The PTK is then used to create a Hash-based Message Authentication Code (HMAC) created by the Message-Digest Algorithm (MD5) by giving the Key confirmation key (KCK) which is the first 128 bits of the PTK and the S-nonce as the input into the HMAC-MD5 algorithm. The S-nonce and produced MIC are then sent to the AP. The AP can perform the same PRF-512 done by the user equipment to generate the PTK and then use the PTK to verify the MIC. Once verified the AP will send an encapsulated Group Temporal Key (GTK) and MIC back to the UE for verification. The UE will then respond with an Acknowledgement of successful authentication. The PTK is also used to generate the Key Encryption Key (KEK) and the Temporal Key (TK). The KEK is used to encapsulate the GTK and other handshaking encryption and the TK is used for encrypting the communication over the link. The encryption in TKIP is done using RC4 similar to the encryption in WEP. The methodology used for the encryption of packets in TKIP greatly increases the security compared to WEP as the TK is constantly updated by the larger IV.

3.3.3 Wi-Fi Protected Access 2 (WPA2)

The Wi-Fi Alliance completed 802.11i as WPA2 to secure communication on wireless networks due to the weaknesses of WEP and WPA. The protocol relies on a shared key called the same Pairwise Master Key (PMK) generated in WPA which is designed to last the entire session and is exposed as little as possible. WPA2 uses the same

four-way handshake to authenticate the user equipment (UE) to the access point (AP) and create keys for communication which can be seen in Figure 3.7. Similar to WPA using TKIP, WPA2 uses counter mode (CTR) with cipher-block chaining message authentication code (CBC-MAC) Protocol (CCMP) to perform many operations including securing the communication channel. There are some differences in the authentication between WPA and WPA2 such as the PRF used to generate the PTK in WPA2 is 384 bits. The MIC in the authentication is SHA-1. The encryption in CCMP uses the advanced encryption standard (AES). There are major differences in the way the encryption is completed in CCMP compared to TKIP but those differences are not being investigated in this paper as we are focusing on authentication. The change to using the more secure SHA-1 for the MIC instead of MD5 creates a much more secure authentication.

The migration from WEP/WPA to WPA2 could be accomplished relatively quickly due to the fact that most mobile equipment (laptops and other powerful equipment) is upgraded frequently and has very few requirements to run on minimal resources. The migration of the network from WEP/WPA to WPA2 is handled by the network provider which was only limited by each organization mandate and could be accomplished when needed. Overall the cost of the upgrade has involved a massive replacement of equipment on a very large worldwide scale. The capacity of network devices has also grown with the migration from 802.11a to b to g to n, therefore, most providers would have upgraded their networks with the new technology and most users would upgrade their devices at the same time as well to make use of new computing power. The mobile networks have very different considerations when upgrading or integrating protocols. Mobile network

operators have agreements with many other operators to allow almost any devices onto their network. To facilitate this requirement the network needs to operate in both SIM and USIM security contexts which we will show in the following section.

3.4 Legacy Integration of SIM with USIM

When the time came for industry to move to UMTS networks the market was already saturated with a large number of GSM devices and network equipment. The integration offered by the protocol allows for the providers to make use of the already embedded systems. To make the transition cost effective and to make maximum use of the existing user and network hardware, GSM backwards compatibility was built into the UMTS protocols [38]. The interoperation between the two systems allows GSM devices on the UMTS network and allows the network to be slowly upgraded to the new infrastructure. A provider can then support the large number of devices owned by customers as well as have a planned strategy for upgrading their network infrastructure.

To achieve the integration there are some equations that are used to convert the keys from UMTS *CK* and *IK* to GSM K_c and vice versa. Those equations allow the mobile device and network to continue to operate without requiring re-authentication to roam from one network configuration to another. Those equations to create K_c are:

$$K_c = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2 \tag{3.1}$$

$$where, \quad CK = CK_1 \parallel CK_2 \tag{3.2}$$

$$and \ IK = IK_1 \parallel IK_2 \tag{3.3}$$

To create *CK* and *IK* from K_c when moving from a GSM context to a UMTS context the following equations are used:

$$CK = K_c \parallel K_c \tag{3.4}$$

$$IK = K_{c1} \oplus K_{c2} \parallel K_c \parallel K_{c1} \oplus K_{c2} \tag{3.5}$$

$$where, \qquad K_c = K_{c1} \parallel K_{c2} \tag{3.6}$$

The following sub-section will be exploring 3 different authentication scenarios of GSM and UMTS equipment to show the methods of integrating these two generations of mobile communications.

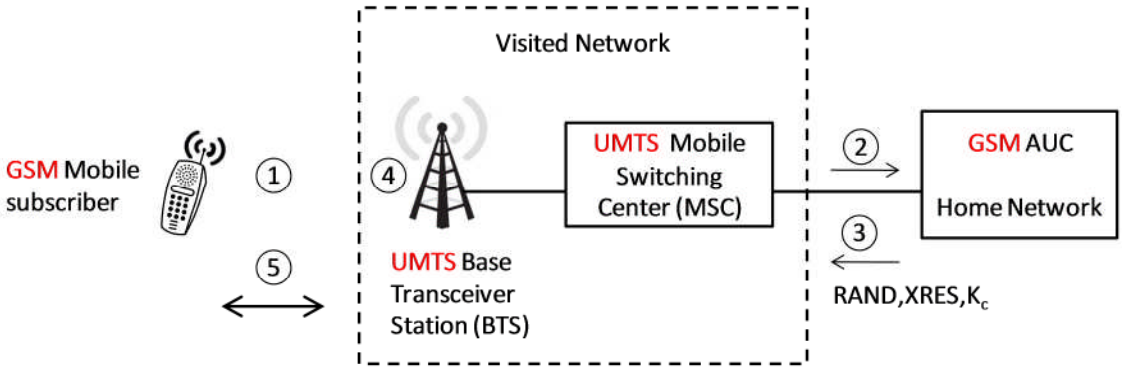
The 3GPP attempted to address these issues with the security upgrades to the USIM protocol in LTE. They do adequately address protecting the existing USIM keys when moving to the less secure GSM or UMTS network configurations but there are possible issues with security spoofing that may bring the GSM issues forward into the LTE framework. When moving to the less secure UMTS network the proposed specification [39] states that the key K_{ASME} will be used with the KDF to generate a *CK*' and *IK*' to be used in the UMTS network. This will protect the LTE framework from an attacker gaining information during the subsequent UMTS or GSM communication and trying to learn information about K_{ASME} to attack the previous LTE communication.

The LTE specification also states that when moving into LTE from UMTS that a check of *CK* should be done to see if the first 64 and last 64 bits match. If they do it can be assumed that the connection was at one time a GSM connection. These are to be dropped unless there is an ongoing emergency communication occurring. It may be possible to

spoof this status of emergency communication as an attacker due to the fact that an attacker could have full control of the communication from the UE. It also doesn't seem entirely practical to refuse the authentication transfer if an active non-emergency conversation is occurring.

3.4.1 GSM Mobile Device with UMTS Network

When a GSM Mobile device is on a UMTS network as shown in Figure 3.8, and as per the order of the circled numbers, GSM Mobile subscriber requests a secure connection to UMTS BTS. The UMTS MSC requests from the GSM home network the authentication vector (RAND,XRES, K_c). The UMTS MSC receives and then forwards the authentication vector to the UMTS BTS. The UMTS BTS then perform the GSM Authentication protocol with GSM Mobile subscriber as described in 2.3.1 and Figure 3.1 above. If the authentication process succeeded, the GSM Mobile and the UMTS BTS can communicate securely applying the UMTS encryption algorithms using the UMTS key *CK* and the integrity key *IK*.



(1) GSM Mobile subscriber requests a secure connection to UMTS BTS
(2) UMTS MSC requests from the GSM home network the authentication vector (RAND,XRES,K_c).
(3) UMTS MSC receives the GSM authentication vector and forward it to the UMTS BTS
(4) UMTS BTS perform the GSM Authentication protocol with GSM Mobile subscriber
(5) When the authentication process in (4) succeeded, the GSM Mobile and the UMTS BTS can communicate securely applying the UMTS encryption algorithms using the UMTS key CK and the integrity key IK. These keys are generated using the GSM K_c

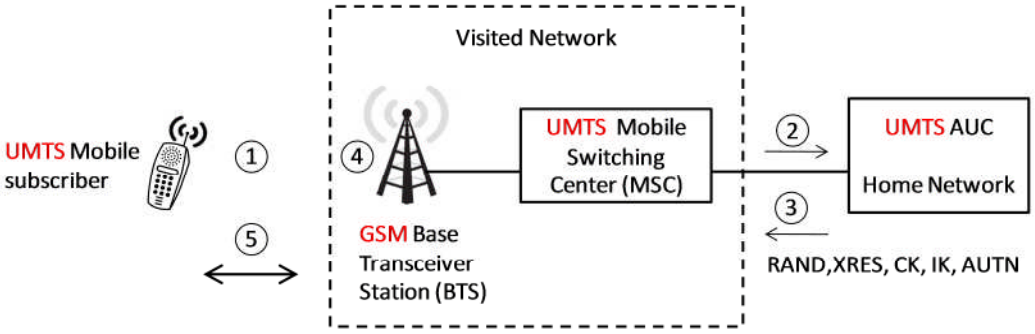
Figure 3.8: The GSM Mobile subscriber is authenticated via a UMTS BTS, which is connected to a UMTS MSC.

Note that, the system will create K_c at the home AuC of the GSM which will then be expanded with Equations (3.4) and (3.5) to create *CK* and *IK* in an enhanced GSM mode to increase the security of the communication. The issue brought about by this configuration is that when K_c has already been discovered by an attacker when the phone is operating in a fully GSM context the expanded *CK* and *IK* are easy to discern from the equations and all of UMTS communication can be discovered by an attacker.

3.4.2 UMTS Mobile Device with GSM BTS

When connecting to the network it is possible for a UMTS mobile device to connect to a GSM BTS. As shown in Figure 3.9, and as per the order of the circled numbers, the UMTS Mobile subscriber requests a secure connection to GSM BTS. Accordingly, the UMTS MSC requests from the UMTS home network the authentication vector

(RAND,XRES, *CK*, *IK*, AUTN). The UMTS MSC receives the UMTS authentication vector and proceeds to generate a GSM K_c using Equation (3.1) and then forwards it to the GSM BTS. The GSM BTS performs the GSM authentication protocol with UMTS Mobile subscriber as described in Section 3.2.1 and Figure 3.1 above. If this authentication process succeeds, the UMTS Mobile and the GSM BTS communicate using the GSM encryption algorithms using the GSM K_c.



(1) UMTS Mobile subscriber requests a secure connection to GSM BTS
(2) UMTS MSC requests from the UMTS home network the authentication vector (RAND,XRES, CK, IK, AUTN).
(3) UMTS MSC receives the UMTS authentication vector and proceeds to generate a GSM K_c and forwards K_c to the GSM BTS
(4) GSM BTS performs the GSM Authentication protocol with UMTS Mobile subscriber
(5) When the authentication process in (4) succeeds, the UMTS Mobile and the GSM BTS communicate using the GSM encryption algorithms using the GSM K_c. Which is insecure due to the attacks available against the GSM algorithms.

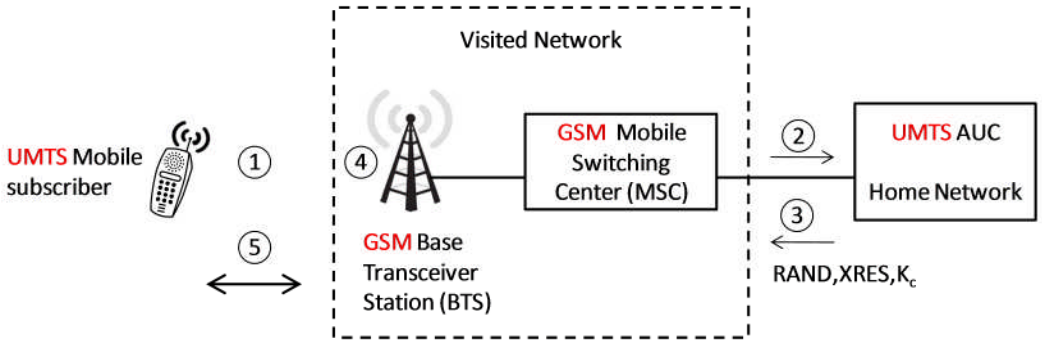
Figure 3.9: The UMTS Mobile subscriber is authenticated via a GSM BTS, which is connected to a UMTS MSC.

This type of connection is created either during authentication or during handover to this type of network. The only network device that uses the GSM protocols in this type of connection is the BTS. The MSC, Mobile and AUC are all UMTS devices. The MSC will retain the CK and IK generated by the UMTS authentication but all encryption between the Mobile and the GSM BTS is done using the K_c created using equation(3.1). K_c is created by the Mobile and by the UMTS MSC and the GSM BTS is oblivious to this operation.

The communication between the Mobile and the BTS can be considered as secure as that of normal GSM communication. When moving to other network configurations the MSC will use the *CK* and *IK* that were originally generated instead of using the K_c generated for the BTS. We know that, the K_c can be compromised during communication with the BTS and will therefore give 64 bits of information relating to the original *CK* and *IK*.

3.4.3 UMTS Mobile Device with GSM BTS and MSC

Figure 3.10 shows another scenario when a UMTS mobile device is connecting to a GSM network. Following the order of the circled number in the Figure, the UMTS Mobile subscriber requests a secure connection to GSM BTS. Accordingly, the GSM MSC requests from the UMTS home network the authentication vector (RAND, XRES, K_c) where it is generated using the UMTS authentication vector (RAND, XRES, *CK*, *IK*, AUTN). The GSM MSC receives the GSM authentication vector and forwards K_c to the GSM BTS. The GSM BTS then performs the GSM Authentication protocol with UMTS Mobile subscriber as described in Section 3.2.2 and Figure 3.2 above. If this authentication process succeeded the UMTS Mobile and the GSM BTS communicate using the GSM encryption algorithms using the GSM K_c.



(1) UMTS Mobile subscriber requests a secure connection to GSM BTS
(2) GSM MSC requests from the UMTS home network the authentication vector (RAND,XRES, K_c) which is generated by using the UMTS authentication vector (RAND,XRES, CK, IK, AUTN).
(3) GSM MSC receives the GSM authentication vector and forwards K_c to the GSM BTS
(4) GSM BTS performs the GSM Authentication protocol with UMTS Mobile subscriber
(5) When the authentication process in (4) succeeds, the UMTS Mobile and the GSM BTS communicate using the GSM encryption algorithms using the GSM K_c. Which is insecure due to the attacks available against the GSM algorithms.

Figure 3.10: The UMTS Mobile subscriber is authenticated via a GSM BTS, which is connected to a GSM MSC.

In this type of connection authentication or handover occurs when a UMTS authenticated session moves to a GSM network. The GSM MSC and GSM BTS can only handle the K_c for GSM communication. Therefore the UMTS authenticated network transfers K_c derived from equation (3.1) to the GSM MSC. The new K_c will be used to create any future *CK* and *IK* as well as for all communication between the GSM BTS and the Mobile using equations (3.4) and (3.5). This decreases the security of the system beyond the 64 bits of knowledge shown in the previous weakness to a full break of all future communication. All future communication until a new authentication request can be discovered and modified by a false base station. This is the worst case scenario for a UMTS device as it is fully compromised.

3.5 Proposed Solution to Problem of GSM Integration in UMTS

To solve the issues brought about by integrating the large install-base of the GSM platform and network equipment into the new and more secure UMTS system we have two solutions. We cannot do large modifications to the existing GSM system to protect the communication that will happen when in a GSM context and will therefore assume that when communication happens in a GSM context that K_c will be compromised and known to attackers. Our focus is on protecting the UMTS communication from attacks through the integration with GSM. First we show a modification to GSM that will allow future communication to be secure when on an UMTS network. Our second proposal is a larger modification to the UMTS protocols to harden the communication in UMTS from attacks due to the GSM integration. It is worth mentioning that, both of the proposals do nothing to increase the security in GSM. GSM is still insecure but we are protecting UMTS from the integration with GSM.

3.5.1 Proposed Modification to GSM

The change we are proposing to the GSM authentication protocol shown in Figure 3.11 is simple and yet very effective. As all GSM devices have a hashing algorithm available, such as A3 and A8, and this operation need only happen once when moving from tower to tower the overhead should be minimal. It may be simple to implement this change to existing GSM system hardware. A hashing algorithm is able to keep the source material unknown while creating the same output if given identical input.

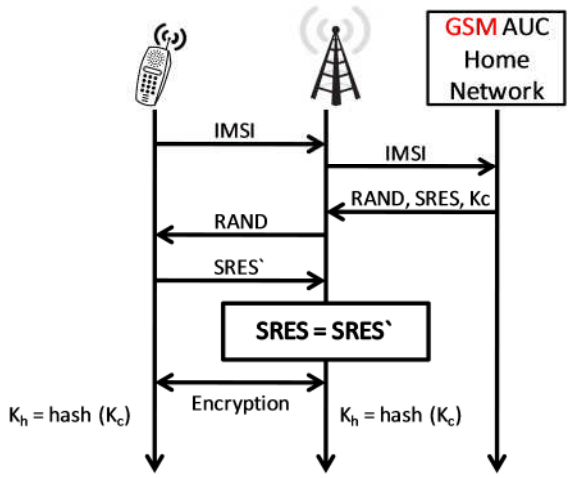


Figure 3.11: Proposed modification to GSM Protocol.

This is because it is computationally hard to discover the input if the output is known. Therefore we propose that the encryption in GSM is done with a new key K_h which is a hash of K_c instead of K_c directly, as it is shown in Equation (3.7).

$$K_h = hash(K_c) \tag{3.7}$$

This would leave the GSM communication open to all of the previous attacks but when compromised would give the attacker access to K_h instead of K_c. We will now describe how this change protects the communication in each of the previously described scenarios.

Case 1: GSM Mobile Device with UMTS Network

Figure 3.11 shows how GSM authentication takes place with the proposed modification, we see that the air-interface between the mobile subscriber and the BTS is encrypted using shared key K_h. If we assumed an attacker has successfully compromised K_h due to the insecurity of GSM, still the attacker has no access to the value of K_c. This means

the values of *CK* and *IK* that are derived from K_c (see Equations (3.4) and (3.5)) are not compromised. Therefore, in this scenario UMTS security is not be compromised and its strength depends on the security of the cryptographic hash function used in Equation (3.7).

Case 2: UMTS Mobile Device with GSM BTS

When encrypting the communication again between the mobile and the GSM BTS using the key K_h (see Figure 3.11), the value of K_c will be shielded by the cryptographic hash function. This hash would keep the attacker far from deriving 64 bits of *CK* and *IK* when the user moves to other networks as the attacker would not be able to discern anything beyond K_h when the system is communicating in this scenario. Again, knowing the value of K_h gives no significant knowledge of K_c and therefore no partial knowledge of *CK* and *IK*.

Case 3: UMTS Mobile Device with GSM BTS and MSC

Similarly in this scenario, the cryptographic hash function protects K_c from the attacker. This has a much larger implication in this scenario as the CK and IK that will be used in the future are completely derived from K_c and will be protected from attack due to the fact that the hash function is one-way function. Therefore, the compromised K_h will not give the attacker significant knowledge of K_c and through that will protect all future communication using *CK* and *IK* that are derived directly from K_c.

3.5.2 Proposed Modification to UMTS

The change to the UMTS protocol is two-fold as it needs to protect information when moving to a GSM network and protect the user when moving back to a UMTS network context. First we recommend that instead of using the equations developed for integration of the legacy GSM protocols we propose that a hash of *CK* and *IK* be used to create the key K_c to be used when communicating in the GSM network. I.e., Equation (3.1) above will be modified as follows:

$$K_c = CH_1 \oplus CH_2 \oplus IH_1 \oplus IH_2 \tag{3.8}$$

$$where, \quad hash(CK) = CH_1 \parallel CH_2 \tag{3.9}$$

$$and \ \ hash(IK) = IH_1 \parallel IH_2 \tag{3.10}$$

The advantage to using this equation as opposed to Equation (3.1) is that the attacker will be unable to find information relating to *CK* and *IK* by knowing the value of K_c. This modification would protect the information sent before moving to the GSM context by securing the values of *CK* and *IK* from creating the value of K_c.

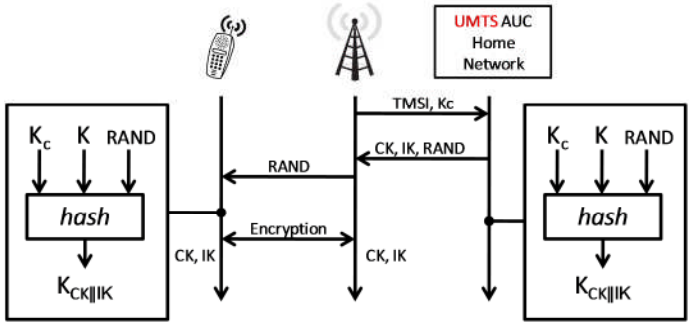


Figure 3.12: Request/Response to retrieve new *CK* and *IK*.

The second change to the protocol is to have the UMTS mobile device and the network do a simple hash of K_c, *K* and a RAND to create a new *CK* and *IK* for use after

leaving the GSM context. This would be a simple request/response from the new UMTS network to the UMTS AuC to create the new *CK* and *IK* to be used for communication similar to a location update as can be seen in Figure 3.12. The small request would require much less overhead than a full re-authentication in UMTS to limit resource utilization on the network. The message sent would be similar to the location update by sending the TMSI along with K_c to the UMTS AuC. The UMTS AuC would then perform a hashing operation as to create a new set of keys for *IK* and *CK* that we will call $K_{CK||IK}$ shown as follows:

$$K_{CK||IK} = hash(K_c \parallel K \parallel RAND) \tag{3.11}$$

$$where, \qquad K_{CK||IK} = CK \parallel IK \tag{3.12}$$

The AuC will proceed to respond with the new $K_{CK||IK}$ and a RAND to be sent to the mobile device to perform the same operation. This would by necessity have to occur before or immediately after handover to a fully UMTS context. The mobile device and the UMTS network would then be able to communicate securely without considering the fact that the Kc could have been compromised during the GSM communication context. The next sections will describe the impact of this change on the different network scenarios.

Case 1: GSM Mobile Device with UMTS Network

This context would use the new $K_{CK||IK}$ created in Equation (3.11) for the keys *CK* and *IK* to be used in the UMTS encrypted communication. This would make the communication secure from any possible attack if the value of K_c had been discovered previously during a fully GSM context. The new values of *CK* and *IK* are not derived with

Equation (3.1) and therefore do not directly come from K_c which makes future communication secure from a compromised GSM context.

Case 2: UMTS Mobile Device with GSM BTS

The communication in this context would be encrypted using a K_c derived from Equation (3.8). The communication during this GSM based context would be compromised but communication that occurred before this point would be secure due to the hash in Equation (3.8) that creates the key K_c and communication after this context would be secure due to the fact that K_c would have been created from a hash and therefore the existing *CK* and *IK* can be used with confidence for future communications as no information on the existing *CK* and *IK* has been discovered.

Case 3: UMTS Mobile Device with GSM BTS and MSC

In this context, once again the hash in Equation (3.8) protects *CK* and *IK* from the attacker and therefore all previous communication is secure and no significant knowledge of *CK* and *IK* is available to the attacker. K_c is still available to be compromised by an attacker in this configuration and therefore, when moving to another context from this context we will be creating a new *CK* and *IK* from Equation (3.11) that will make future communication secure.

3.6 Summary

Wireless network communication requires that user equipment be able to securely connect to the network and maintain integrity of that communication. In stationary

networks there is no requirement for user equipment to be able to use all access points and to communicate while roaming between access points. Mobile networks have a different requirement that requires that user equipment be able to use all base stations and communicate while roaming and therefore, legacy protocols needed to be integrated into new network systems.

To help manage the transition from the legacy GSM system, protocols were devised to integrate the billions of existing devices into the new UMTS network. The integration protocols that allow for the integration of those legacy devices also inadvertently brought the insecurity of the GSM system into the new much more secure UMTS system. The GSM key K_c can be compromised and therefore, due to the method of integrating the two systems together which uses simple Equations (3.1), (3.4) and (3.5) to create the keys *CK*, *IK* and K_c used for encryption and integrity, an attacker that has discovered K_c can discern either all or part of *CK* and *IK*. This integration has allowed previous attacks on the GSM system to be effective against attacking the UMTS network negating the positive changes brought about by the mutual authentication in UMTS.

We have proposed two different changes to the protocols in mobile networks to protect against the legacy integration of GSM. One is a very simple change to the GSM protocol to protect K_c by creating K_h a hash of K_c shown in Equation (3.7) which is to be used when encrypting. This will protect K_c from attackers and therefore, protect the UMTS communication that depends on the keys devised from Equations (3.1), (3.4) and (3.5). The other change we propose is for the UMTS protocol to be modified to remove the Equations (3.1), (3.4) and (3.5) used to generate *CK*, *IK* and K_c and replaces those equations with two

Equations (3.8), and (3.11) which both use a hash function. We also create a simple request/response protocol to generate a new *CK*, *IK* pair generated from Equation (3.11) to be used in future communication. The changes we have proposed will help resolve the insecurity brought about by the legacy integration of the GSM equipment and protocols into the new UMTS system. This integration was required due to the large and growing install-base of GSM devices.

Out of the two solutions proposed we recommend the solution of a GSM hash since it changes the protocol that has introduced the problems with a minimal amount of effort. GSM already has cryptographically strong hash functions available for use and should be able to be modified to do the single hash of the K_c value to increase the security of communication. We have not done a full evaluation of the security scheme but it does resolve the issues that come about due to the GSM and UMTS integration as shown in the previous sections. The modification should be easily applied to UMTS devices in their support of the GSM protocols and add the increased security that the change would provide. The other advantage of this modification is that when the GSM protocols are removed when they are no longer required in the future, this change will then be removed as well making it much more self contained than the changes to the UMTS protocol that we propose. The deployment of this solution would require software updates to be done over multiple world wide networks and would need to be a large managed project for the network operators.

Chapter 4

Authentication for Medical Wireless Sensor Networks

Authentication is the first step in ensuring the safety, privacy and security of user information in a medical wireless sensor network system. The following sections will detail a scenario on usage of an M-WSN and how each component will authenticate to the secure system. Please note that the scenario will have areas that are numbered for future reference during discussion of our protocol.

4.1 Scenario: Patient Monitoring after Surgery

1 - A patient John Smith has just undergone a surgical procedure - coronary artery bypass surgery. The attending physician, Dr. Michael Jones, wishes to monitor John Smith

for any issues that could arise after the surgery. The sensor network that the physician wishes to deploy consists of multiple sensors (blood pressure, EKG, heart rate, and temperature) and a single smart control node which are then placed on John Smith shortly after the surgery to be able to monitor his critical health metrics related to the surgery.

2 - The clinical staff will have the smart control node in an unassigned state authenticate to the clinical server. The staff will then log into the server during a secure encrypted session and then select the patient during this session on the device.

3 - The clinical staff will then take each sensor and place it in close proximity to the smart control node and depress the reset button on the sensor node. The sensor will send a registration request to the smart control node which will then display information on a screen that will need user input to approve the sensor. The staff will verify that the sensor is the correct sensor and approve the connection of the sensor to the MWSN. The sensor will authenticate against the smart control node which will use information from the clinical server to complete the authentication. The registration will be maintained in both the smart control node and the clinical server. 3 will be repeated for each sensor.

4 -This session on the smart control node will then be terminated by the clinician. This ends the sensor and smart control node registration phase.

5 - The smart control node will then authenticate to the clinical server using the selected patient identity of John Smith. A command will be sent to the sensors to begin sending information to the smart control node which will process the information and send the telemetry recorded from the sensor nodes to the clinical server.

Chapter 4:

Authentication for Medical Wireless Sensor Networks

John Smith is very quickly back on his feet and able to roam throughout the hospital for the remainder of his stay; the physical activity and freedom increase his happiness and rate of recovery. During his roaming John will move from one Wi-Fi hotspot to another within the hospital. The smart control node will use the same session information from the previous authentication to continue communicating with the clinical server. The information from the sensors has shown that John has no critical issues in the two days following the surgery and is recovering very well. Instead of requiring all 4 days of recovery the patient is allowed to return to his home with the sensor network (sensors and smart control node) attached and monitoring his vital signs for the next two weeks to ensure that there are no issues.

6 - During the two weeks the smart control node runs out of power and requires recharging; the loss of power requires the smart control node to re-authenticate against the clinical server.

7 – The power loss also requires the sensors to re-authenticate against the smart control node. This is done without a need to authenticate the sensor against the clinical server.

8 - While John is moving from the hospital to his home the smart control node will continue to communicate with the clinical server over cellular networks as well as John's home network (The configuration to use the Wi-Fi in John's home is available on the smart control node).

9 - On the twelfth day John has an arrhythmia. The sensors send the encrypted EKG information to the smart control node which then deciphers that the data is an arrhythmia. The smart control node sends this alert information to the clinical server. The clinical server notifies Dr Jones of the issue and he takes all necessary precautions in ensuring the safety of his patient. The clinical system also notifies relevant hospital staff; they dispatch a less expensive patient transfer service to pick up Mr. Smith without requiring the use of an emergency service ambulance which would be better deployed to a more critical health event.

Mr. Smith is notified by smart control node that he should seek medical assistance and that a transport service is on route to pick him up at his current location (GPS functionality) and that he should not drive due to his condition. The smart control node also sends commands to the sensors to increase their rate of monitoring and communication to have better information during the clinical event.

The sensors allow Dr. Jones to have long term monitoring of the recovery of his patient while freeing the patient not only from the restriction of a recovery room/bed but also of the requirement of being in the hospital for an extended period simply for observation. The sensors also decrease the nursing effort currently required to gather patient telemetry in hospital.

When Dr. Jones had the sensor nodes applied to Mr. Smith the sensors were configured to start sending the data to the smart control node. The smart control node would do some minor processing of the data to see if there are any critical alerts or

maintenance alerts that need to be given to the patient such as data indicating a health emergency or a sensor that is no longer properly placed or out of power. The smart control node then sends the clinical information to the clinical server for storage and further processing. The clinical server can then create alerts or be accessed by user applications or other systems; this foreign access will not be discussed. To achieve the goals of security, privacy and safety of the patient and the information sent over the network, in Section 4.1 and 4.2, we will be discussing the authentication of the smart control and sensor nodes against each other and the clinical server.

As described there are 3 different types of devices considered in this scenario. The clinical server maintains the keys of the sensor nodes, and smart control nodes as well as the clinical information gathered from those nodes. The smart control node gathers the data from the sensor nodes, processes that data to a minor extent for alerts and other immediate uses, and forwards that data to the clinical server while migrating over wireless networks and the internet. The sensor nodes collect the clinical patient data and forward that data to the smart control node.

The solution we are proposing is a general solution that will meet the requirements of the scenario presented and other possible uses for clinical requirements. The scenario is to be used to understand the application of the sensor network system and how it is both novel and applicable to the needs of health systems worldwide.

4.1.1 Smart Control Node Authentication

Chapter 4:

Authentication for Medical Wireless Sensor Networks

The communication routing between the smart control node and the clinical server can go over wireless and physical networks, as well as the internet. The smart control node will already have been connected wirelessly to the network in the hospital using their supported Wi-Fi protocols. The clinical staff will establish a connection to the clinical server to select the patient for the smart control node to monitor shown in Figure 4.1which is how this protocol is used to support the security requirement mentioned in our scenario number 2. The SmartId and K_{Smart} are preloaded onto the smart control node before distribution to the clinical environment. These two preloaded values act similarly to the IMSI and *K* in the UMTS authentication protocols as shown in Section 3.2.2 and Figure 3.2. To create this connection the smart control node will use the value of -1 along with a timestamp and K_{Smart} to generate the SmartRES, the ClinRES`, K_{SE} and K_{SI} as output from the secure hash functions A1, A2, A3 and A4 described at the end of this section.

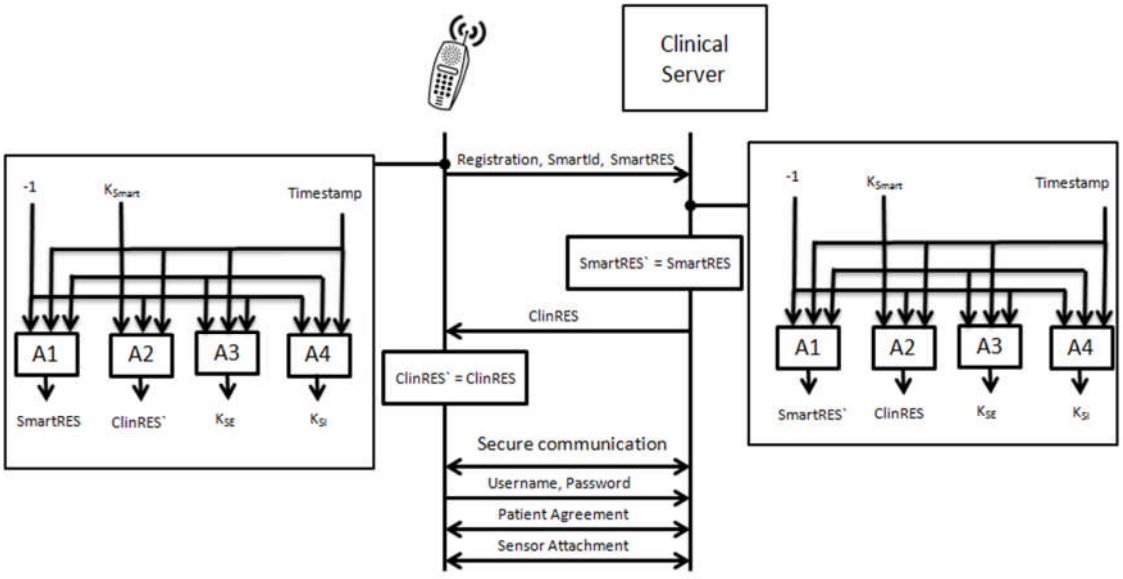


Figure 4.1: Initial authentication of smart control node to do patient agreement and sensor attachment.

The smart control node will then send a registration message with the SmartId and the SmartRES to the clinical server. The clinical server will use the SmartId to locate the K_{Smart} and generate the SmartRES` to authenticate the smart control node. Then clinical server will generate the other values and respond to the smart control node with the ClinRES. The smart control node will then validate the ClinRES and the mutual authentication and session key generation will be complete. The session will be created and the keys K_{SE} and K_{SI} are used to encrypt and perform integrity on the remaining steps in the patient and sensor registration process.

The clinical staff will then enter a username and password into the smart control node for the server to verify their credentials. The clinical staff will then be able to select the patient from a list available on the clinical server and confirm the linking of the patient to the device. After the patient has been selected, the clinical staff can then proceed to link each sensor to the smart control node. By depressing a reset button on the sensor, the SenseId will be broadcast by the sensor node and the control node will display the SenseId and sensor type. The clinical staff can then accept that sensor as linked to the smart control node which will then have the smart control node store the SenseId and the clinical server will create and store the relationship between the smart control node and the sensor node. This process is shown in the next section. This is number 3 in the scenario. Once the patient has been confirmed and the sensors added to the device, the registration session will be terminated as described in number 4 in the scenario.

Chapter 4:

Authentication for Medical Wireless Sensor Networks

To authenticate the smart control node to the clinical server after the initial patient agreement and sensor node attachment, the following protocol shown in Figure 4.2 will be used. This protocol supports the security requirement mentioned in number 5 and 6 of the scenario. The smart control node will use the shared key K_{Smart} along with a current timestamp as well as the patientID to create the session encryption key (KSE), the session integrity key (KSI), the smart control node response (SmartRES), and the clinical server expected response (ClinRES`) using the cryptographic hashing algorithms A1, A2, A3, and A4 (these functions are described in Section 4.1.2 below) with the exception of -1 being replaced by patientID. The smart node will send the SmartId, and SmartRES to the clinical server. The Clinical Server will receive the information and verify the timestamp as larger than the last authentication timestamp within a pre-defined time skew. Then it will use the SmartId to find the shared key KSmart which is then used along with the Timestamp to create the SmartRES` to verify the SmartRES as having originated from the appropriate smart control node. The clinical server will also generate a ClinRES which is sent encrypted back to the smart control node. The smart control node will then verify the ClinRES by using the previously generated ClinRES`.

Chapter 4:

Authentication for Medical Wireless Sensor Networks

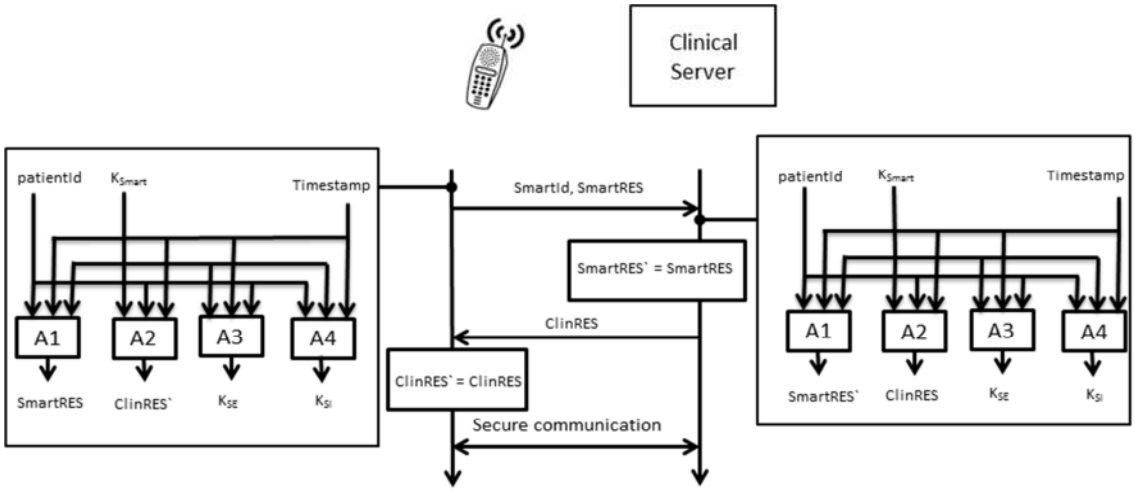


Figure 4.2: Authentication of smart control node while collecting patient telemetry.

4.1.2 Cryptographic Hash Functions

The hash functions used, shown in Figure 4.3, are at the discretion of the provider of the smart control node depending on the limitations of the hardware and requirements of the system. The hash could be SHA-3 or another cryptographically secure hashing algorithm. We show the equations with the desired input into each hash function shown below. The string input is used to create different hash output values for each of the different algorithms.

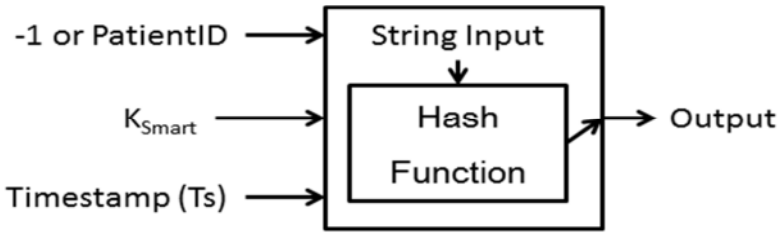


Figure 4.3: Hash Function used to create authentication values.

The hashing equations show how each will create the desired value such as the expected responses from each of the smart control node or the clinical server or the keys used for encryption or integrity when communicating after authentication.

$$\text{SmartRES} = A1(-1, K_{Smart}, Ts) = h(\text{“SmartRES”}, -1, K_{Smart}, Ts) \quad (4.1)$$

$$\text{ClinRES} = A2(-1, K_{Smart}, Ts) = h(\text{“ClinRES”}, -1, K_{Smart}, Ts) \quad (4.2)$$

$$\text{KSE} = A3(-1, K_{Smart}, Ts) = h(\text{“KSE”}, -1, K_{Smart}, Ts) \quad (4.3)$$

$$\text{KSI} = A4(-1, K_{Smart}, Ts) = h(\text{“KSI”}, -1, K_{Smart}, Ts) \quad (4.4)$$

4.1.3 Sensor Node Authentication

Sensor nodes will authenticate to the Smart control node to send confidential clinical patient data over wireless spectrum securely as shown in Figure 4.4. The authentication shown here is number 3 in the scenario. The sensor will have an identifier (SenseID) and a pre-shared key (Ksense). Using a fresh and valid Timestamp (Ts) the sensor will use the B1, B2, B3, B4 and B5 functions to create the KeyGen, EK, IK, SenseMAC and SenseRES. Similar to the A hashing functions on the smart control node the actual implementation of the function is left to the provider. The functions are shown in the equations below:

$$\text{GenKey} = B1(\text{KSense}, Ts) = h(\text{“Registration”}, \text{KSense}, Ts) \quad (4.5)$$

$$\text{EK} = B2(\text{GenKey}, Ts) = h(\text{“EK”}, \text{GenKey}, Ts) \quad (4.6)$$

$$IK = B3(GenKey,Ts) = h(\text{“IK”},GenKey,Ts) \quad (4.7)$$

$$SenseMAC = B4(GenKey,Ts) = h(\text{“SenseMAC”},GenKey,Ts) \quad (4.8)$$

$$SenseRES = B5(GenKey,Ts) = h(\text{“SenseRES”},GenKey,Ts) \quad (4.9)$$

The sensor will send an authentication request with the SenseID as well as the generated SenseMAC to the smart control node. The smart control will forward the SenseID and SenseMAC to the clinical server over the existing secured communication channel. The clinical server will use the pre-shared KSense and a timestamp to generate a key (KeyGen), an encryption key EK and the SenseMAC`. The clinical server will verify the SenseMAC from the sensor against the generated SenseMAC`. Then the KeyGen and EK will be sent to the smart control node. The smart control node will use KeyGen and a timestamp to generate IK and SenseRES. SenseRES will be sent to the sensor node for verification against SenseRES` and secure communication can commence.

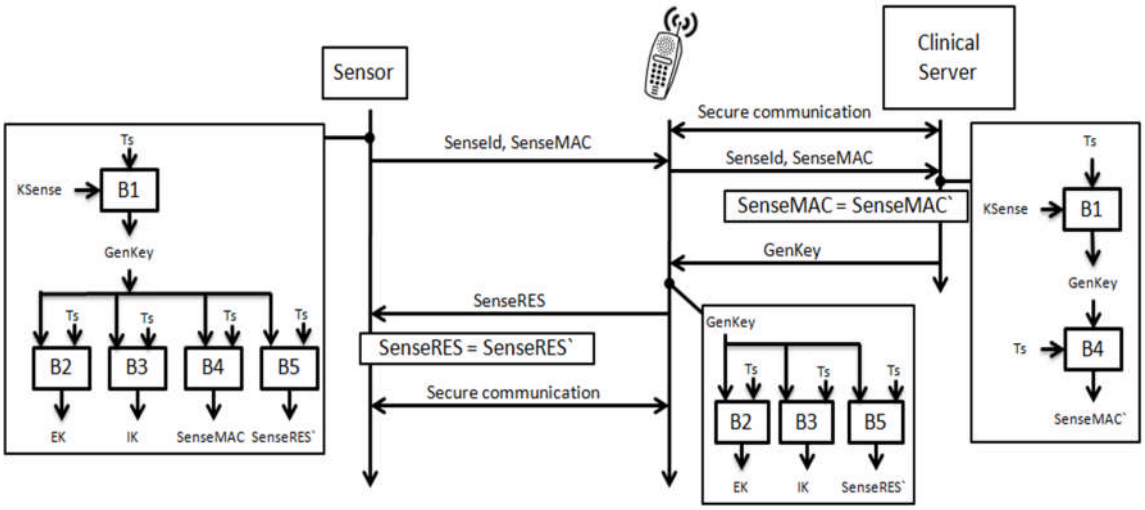


Figure 4.4: Sensor node initial authentication.

Chapter 4:

Authentication for Medical Wireless Sensor Networks

Future authentication between the Sensor and the smart control node, shown in Figure 4.5 will use the previously generated GenKey to create EK, IK, SenseMAC, and SenseRES on both the sensor and the smart control node removing requests to the clinical server. This allows for the sensors to be able to re-authenticate against the smart control node in situations where the communication link to the clinical server is down.

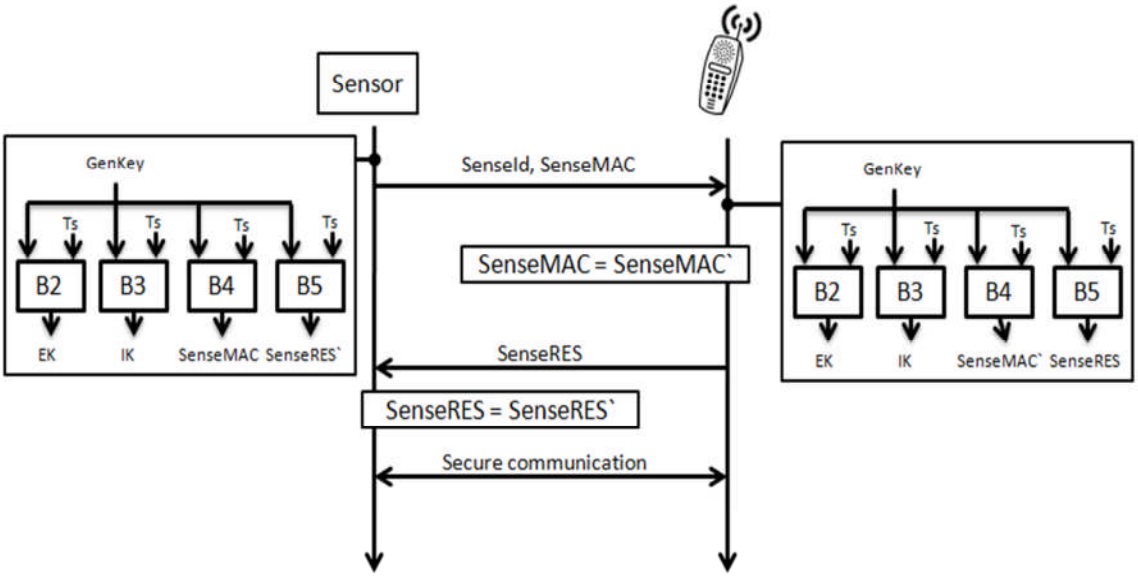


Figure 4.5: Sensor node re-authentication.

4.2 Formal Protocol Analysis

To ensure the protocols we have developed are secure we will use Burrows-Abadi-Needham logic (BAN logic) [40]. BAN logic has been used to help verify the quality of different authentication protocols including UMTS authentication [41]. Many other protocols have been analyzed using BAN analysis [42],[43],[44]. Sadly there was no BAN analysis done of the GSM/UMTS integration algorithms which may have lead to the problems with that integration being discovered before deployment. Those issues were

discussed in Chapter 3 and two different solutions were proposed to solve the problem with integration. The BAN logic will help us determine whether or not our exchanged information is trustworthy, and secured against eavesdropping. They attempt to answer the following questions with their logical framework:

1. What does this protocol achieve?
2. Does this protocol need more assumptions than another one?
3. Does this protocol do anything unnecessary that could be left out without weakening it?
4. Does this protocol encrypt something that could be sent in clear without weakening it?

To answer these questions about our protocol we will proceed to use BAN logic to analyze our different authentication protocols to formally verify their quality. BAN uses the following constructs:

$P \mid\equiv X$: P believes X, or P would be entitled to believe X.

$P \lhd X$: P sees X.

$P \mid\sim X$: P once said X.

$P \mid\Rightarrow X$: P has jurisdiction over X.

$\#(X)$: The formula X is fresh.

$P \overset{K}{\longleftrightarrow} Q$: P and Q may use the shared key K to communicate.

$P \overset{X}{\rightleftharpoons} Q$: X is a shared secret known only to P and Q.

Chapter 4:

Authentication for Medical Wireless Sensor Networks

The protocol analysis is performed as follows:

- The idealized protocol is derived from the original one showing each of the messages sent and received.
- Assumptions about the initial state are written
- Logical formulas are attached to the statements of the protocol as assertions about the state of the system after each statement
- The logical postulates are applied to the assumptions and the assertions in order to discover the beliefs held by the parties in the protocol

Initial assumptions are required to guarantee the success of our protocol. We assume that none of the devices in the protocol have been compromised. We assume that the encryption, integrity and hashing algorithms are secure. We assume that there are checks on the timestamps used so that there can be no replay attacks.

The intent of each of our protocols is to achieve mutual authentication and key agreement which is represented by the following four statements.

$$P \mid\equiv P \overset{K}{\longleftrightarrow} Q \tag{4.10}$$

$$Q \mid\equiv P \overset{K}{\longleftrightarrow} Q \tag{4.11}$$

$$P \mid\equiv Q \mid\equiv P \overset{K}{\longleftrightarrow} Q \tag{4.12}$$

$$Q \mid\equiv P \mid\equiv P \overset{K}{\longleftrightarrow} Q \tag{4.13}$$

Statements (4.10) and (4.11) show that P believes that P and Q share a key and that Q believes that as well. Statements (4.12) and (4.13) show that P believes that Q believes that they share a key K and that Q believes that P believes that they share a key K. Showing that they both believe these 4 statements shows that a protocol achieves mutual authentication.

4.2.1 BAN analysis of the Smart Control Node Authentication

The authentication protocol involves the smart control node which will be represented by P and the clinical server represented by S. The intent of the first authentication protocol is for mutual authentication between the smart control node and the clinical server which allows those devices to generate session keys for encryption and integrity to allow the clinical staff to securely log in, select the patient, and assign the sensor nodes. The intent of the second authentication protocol is for mutual authentication which allows the smart control node to send the telemetry from the sensors in a securely encrypted manner with integrity to the clinical server and allow the clinical server to send commands back to the smart control node with the same security. The two different cases of authentication will be described with their BAN analysis.

Case 1: Authentication for Registration

To analyze the protocol we first give the assumptions:

$$P \mid\equiv P \overset{K_{Smart}}{\rightleftharpoons} S \tag{4.14}$$

$$S \mid\equiv P \overset{K_{Smart}}{\rightleftharpoons} S \tag{4.15}$$

$$P \mid\equiv \#(Ts) \tag{4.16}$$

$$S \mid\equiv \#(Ts) \tag{4.17}$$

$$S \mid\equiv P \mid\Rightarrow (P \xleftrightarrow{K_{SE}} S, \#(K_{SE})) \tag{4.18}$$

$$S \mid\equiv P \mid\Rightarrow (P \xleftrightarrow{K_{SI}} S, \#(K_{SI})) \tag{4.19}$$

Assumptions (4.14) and (4.15) show that S (clinical server) and P (smart control node) both share a secret K_{Smart}. The assumptions (4.16) and (4.17) show S and P believe the freshness of the timestamp Ts. Assumptions (4.18) and (4.19) are that S believes that P has jurisdiction over the initiation of the session and the creation of the session encryption and integrity keys and that those keys are fresh. Once the assumptions have been declared we can proceed to verify the idealized version of the protocol shown in Figure 4.1 which has two messages first sent from the smart control node to the clinical server (4.20) and a second message sent from the clinical server to the smart control node (4.21).

Message 1 $$P \rightarrow S : registration, SmartID, SmartRES \tag{4.20}$$

Message 2 $$S \rightarrow P : ClinRES \tag{4.21}$$

The BAN analysis can proceed on the protocol by considering the previous assumptions as well as the idealized protocol. Before P sends the first message to S it will use a fresh timestamp to create the desired keys for communication during the session.

$$P \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.22}$$

$$P \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.23}$$

Then P sends the SmartRES to S as shown in Message 1. The results on the clinical server S are shown below.

$$S \lhd registration, P, A1(-1, K_{Smart}, Ts) \tag{4.24}$$

When S receives the message shown it will then proceed to use the identity of P to reference K_{Smart} to be used in the hashing functions. We see that the addition of the registration string to the protocol is not required answering question 3; we leave in the string to allow easy understanding of the protocol. S will then be able to verify that A1(-1, K_{Smart} ,Ts) is equal to the SmartRES. Once that has been verified the other values can be believed to be true by S as shown below.

$$S \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.25}$$

$$S \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.26}$$

$$S \mid\equiv P \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.27}$$

$$S \mid\equiv P \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.28}$$

We see that S believes both of the session encryption and integrity keys but that S can also believe that P believes both of those keys as well since S was able to verify the request from P. The clinical server S can then respond to P with the ClinRES.

$$P \lhd A2(-1, K_{Smart}, Ts) \tag{4.29}$$

P will then verify ClinRES against A2(-1,K_{Smart},Ts) and proceed to believe the following statements. If P is able to verify ClinRES then it can be certain that the S is the appropriate clinical server.

$$P \mid\equiv S \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.30}$$

$$P \mid\equiv S \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.31}$$

Therefore we can see that mutual authentication and key agreement is achieved with the protocol using BAN analysis shown by statements (4.27), (4.28), (4.30), and (4.31). The keys can then be used for the secure communication that follows in the registration protocol.

Case 2: Patient Authentication

To analyze the protocol we first give the assumptions:

$$P \mid\equiv P \overset{K_{Smart}}{\rightleftharpoons} S \tag{4.32}$$

$$S \mid\equiv P \overset{K_{Smart}}{\rightleftharpoons} S \tag{4.33}$$

$$P \mid\equiv P \overset{PatientID}{\rightleftharpoons} S \tag{4.34}$$

$$S \mid\equiv P \overset{PatientID}{\rightleftharpoons} S \tag{4.35}$$

$$P \mid\equiv \#(Ts) \tag{4.36}$$

$$S \mid\equiv \#(Ts) \tag{4.37}$$

$$S \mid\equiv P \mid\Rightarrow (P \xleftrightarrow{K_{SE}} S, \#(K_{SE})) \tag{4.38}$$

$$S \mid\equiv P \mid\Rightarrow (P \xleftrightarrow{K_{SI}} S, \#(K_{SI})) \tag{4.39}$$

The assumptions (4.32) and (4.33) state that S and P share the secret K_{Smart}. Assumption (4.34) and (4.35) are that S and P both have a unique shared patient identifier. The next two assumptions (4.36) and (4.37) state that P and S both believe the freshness of the timestamp. The final two assumptions are that S believes that P has jurisdiction over the initiation of the session and the creation of the session encryption and integrity keys and that those keys are fresh. Once the assumptions have been declared we can proceed to verify the idealized version of the protocol showing the two messages sent as seen in Figure 4.2.

Message 1 $$P \rightarrow S : SmartID, SmartRES \tag{4.40}$$

Message 2 $$S \rightarrow P : ClinRES \tag{4.41}$$

We proceed to do the protocol analysis. Before P sends the first message to S it will use a fresh timestamp to create the desired keys for communication during the session.

$$P \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.42}$$

$$P \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.43}$$

Then P sends the SmartRES to S as shown in Message 1. The results on the clinical server S are shown below.

$$S \lhd P, A1(PatientID, K_{Smart}, Ts) \tag{4.44}$$

When S receives the message shown it will then proceed to use the identity of P to reference K_{Smart} to be used in the hashing functions. S will then be able to verify that A1(PatientID, K_{Smart} ,Ts) is equal to the SmartRES. Once that has been verified the other values can be believed to be true by S as shown below.

$$S \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.45}$$

$$S \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.46}$$

$$S \mid\equiv P \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.47}$$

$$S \mid\equiv P \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.48}$$

We see that S believes both of the session encryption and integrity keys but that S can also believe that P believes both of those keys as well since S was able to verify the request from P. The clinical server S can then respond to P with the ClinRES.

$$P \lhd A2(PatientID, K_{Smart}, Ts) \tag{4.49}$$

P will then verify ClinRES against A2(PatientID,K_{Smart},Ts) and proceed to believe the following statements. If P is able to verify ClinRES then it can be certain that the S is the appropriate clinical server.

$$P \mid\equiv S \mid\equiv P \xleftrightarrow{K_{SI}} S \tag{4.50}$$

$$P \mid\equiv S \mid\equiv P \xleftrightarrow{K_{SE}} S \tag{4.51}$$

Therefore we can see that mutual authentication and key agreement is achieved with the protocol using BAN analysis. The keys can then be used for the secure communication for the patient telemetry.

4.2.2 BAN analysis of Sensor Node Authentication

The authentication protocol involves the sensor node (N), smart control node (P) and the clinical server (S). The first protocol discussed will describe the method of registering the sensor node with the smart control node by doing an initial authentication with the clinical server. The second protocol will describe the re-authentication of the sensor node against the smart control node.

Case 1: Authentication and Registration of Sensor Node

To analyze the protocol we first give the assumptions:

$$N \mid\equiv N \overset{KSense}{\rightleftharpoons} S \tag{4.52}$$

$$S \mid\equiv N \overset{KSense}{\rightleftharpoons} S \tag{4.53}$$

$$N \mid\equiv \#(Ts) \tag{4.54}$$

$$P \mid\equiv \#(Ts) \tag{4.55}$$

$$S \mid\equiv \#(Ts) \tag{4.56}$$

$$S \mid\equiv N \mid\Rightarrow (N \overset{EK}{\longleftrightarrow} P, \#(EK)) \tag{4.57}$$

$$S \mid\equiv N \mid\Rightarrow (N \overset{IK}{\longleftrightarrow} P, \#(IK)) \tag{4.58}$$

$$P \mid\equiv N \mid\Rightarrow (N \overset{EK}{\longleftrightarrow} P, \#(EK)) \tag{4.59}$$

$$P \mid\equiv N \mid\Rightarrow (N \overset{IK}{\longleftrightarrow} P, \#(IK)) \tag{4.60}$$

$$P \mid\equiv P \overset{K}{\longleftrightarrow} S \tag{4.61}$$

$$S \mid\equiv P \overset{K}{\longleftrightarrow} S \tag{4.62}$$

The assumptions (4.52) and (4.53) represent the fact that S and N both have a shared secret KSense. The next 3 assumptions (4.54), (4.55) and (4.56) relate to each S, N and P having the freshness of a timestamp. The next 4 assumptions (4.57), (4.58), (4.59), and (4.60) are that S and P believe that N has jurisdiction over the creation of EK, IK and the freshness of those keys. The final two assumptions (4.61) and (4.62) show that P and S have already authenticated each other and both share a key(s) for secure communication.

Once the assumptions have been declared we can proceed to verify the idealized version of the protocol showing all four messages shown in Figure 4.4.

Message 1 $$N \rightarrow P : SenseID, SenseMAC \tag{4.63}$$

Message 2 $$P \rightarrow S : \{SenseID, SenseMAC\}_K \tag{4.64}$$

Message 3 $$S \rightarrow P : \{GenKey\}_K \quad (4.65)$$

Message 4 $$P \rightarrow N : SenseRES \quad (4.66)$$

The protocol shall then be analyzed. N will create a fresh timestamp to be used in the hashing functions to generate the expected shared keys as well as the hashes for authentication. This leads N to believe the following statements.

$$N \models N \xleftrightarrow{EK} P \quad (4.66)$$

$$N \models N \xleftrightarrow{IK} P \quad (4.66)$$

Then N sends the SenseMAC to P as shown in Message 1. P then forwards the same message to S over the secure channel.

$$P \lhd SenseID, B4(GenKey, Ts) \quad (4.67)$$

$$S \lhd SenseID, B4(GenKey, Ts) \quad (4.68)$$

P does nothing with the received message other than forward it on to S. S can then use the SenseID to find KSense to generate GenKey for the B4 hashing function and verify the SenseMAC. We see that the message sent from P to S need not be encrypted and can be sent in the clear answering question 4; but as we use the secure channel for all other communication we will leave the message encrypted. If the SenseMAC is verified S can be certain of the identity of N and send GenKey securely to P as shown below.

$$P \lhd GenKey \tag{4.69}$$

When P sees GenKey it can then generate the EK and IK for communication as well as the SenseRES. It is required that this message be encrypted to protect the value of GenKey. P can also safely make the following belief statements.

$$P \mid\equiv N \overset{EK}{\longleftrightarrow} P \tag{4.70}$$

$$P \mid\equiv N \overset{IK}{\longleftrightarrow} P \tag{4.71}$$

$$P \mid\equiv N \mid\equiv N \overset{EK}{\longleftrightarrow} P \tag{4.72}$$

$$P \mid\equiv N \mid\equiv N \overset{IK}{\longleftrightarrow} P \tag{4.73}$$

P will then send the following message to N to complete the protocol.

$$N \lhd SenseRES \tag{4.74}$$

N can then verify the sent SenseRES with the hash of B5(GenKey,Ts). This verification will allow N to make the following belief statements.

$$N \mid\equiv P \mid\equiv N \overset{EK}{\longleftrightarrow} P \tag{4.75}$$

$$N \mid\equiv P \mid\equiv N \overset{IK}{\longleftrightarrow} P \tag{4.76}$$

Therefore mutual authentication between the sensor node and the smart control node is complete and secure communication can commence.

Case 2: Re-Authentication of Sensor Node

There is one less actor in this protocol as S is not required for the re-authentication. To analyze the protocol we first give the assumptions:

$$N \mid\equiv N \overset{GenKey}{\rightleftharpoons} P \tag{4.77}$$

$$P \mid\equiv N \overset{GenKey}{\rightleftharpoons} P \tag{4.78}$$

$$N \mid\equiv \#(Ts) \tag{4.79}$$

$$P \mid\equiv \#(Ts) \tag{4.80}$$

$$P \mid\equiv N \mid\Rightarrow (N \overset{EK}{\longleftrightarrow} P, \#(EK)) \tag{4.81}$$

$$P \mid\equiv N \mid\Rightarrow (N \overset{IK}{\longleftrightarrow} P, \#(IK)) \tag{4.82}$$

The first two assumptions (4.77) and (4.78) are that P and N both have a shared secret GenKey. The next 2 assumptions (4.79) and (4.80) relate to N and P having the freshness of a timestamp. The final 2 assumptions (4.81) and (4.82) are that P believes that N has jurisdiction over the creation of EK, IK and the freshness of those keys.

Once the assumptions have been declared we can proceed to verify the idealized version of the protocol.

Message 1 $$N \rightarrow P : SenseID, SenseMAC \tag{4.83}$$

Message 2 $$P \rightarrow N : SenseRES \tag{4.84}$$

The protocol shall then be analyzed. N will create a fresh timestamp to be used in the hashing functions to generate the expected shared keys as well as the hashes for authentication. This leads N to believe the following statements.

$$N \mid\equiv N \xleftrightarrow{EK} P \tag{4.85}$$

$$N \mid\equiv N \xleftrightarrow{IK} P \tag{4.86}$$

Then N sends the SenseMAC to P as shown in Message 1.

$$P \lhd SenseID, B4(GenKey, Ts) \tag{4.87}$$

P then uses the SenseID to find GenKey for the B4 hashing function and verify the SenseMAC. If the SenseMAC is verified P can be certain of the identity of N and P can then generate the EK and IK for communication as well as the SenseRES. P can also safely make the following belief statements.

$$P \mid\equiv N \xleftrightarrow{EK} P \tag{4.88}$$

$$P \mid\equiv N \xleftrightarrow{IK} P \tag{4.89}$$

$$P \mid\equiv N \mid\equiv N \xleftrightarrow{EK} P \tag{4.90}$$

$$P \mid\equiv N \mid\equiv N \xleftrightarrow{IK} P \tag{4.91}$$

P will then send the following message to N to complete the protocol.

$$N \lhd SenseRES \tag{4.92}$$

N can then verify the sent SenseRES with the hash of B5(GenKey,Ts). This verification will allow N to make the following belief statements.

$$N \mid\equiv P \mid\equiv N \xleftrightarrow{EK} P \tag{4.93}$$

$$N \mid\equiv P \mid\equiv N \xleftrightarrow{IK} P \tag{4.94}$$

Therefore mutual re-authentication between the sensor node and the smart control node is complete and secure communication can commence.

4.3 Summary

The protocol developed for authentication for the smart control node creates an understanding between the smart control node and the clinical server of shared keys for authentication and integrity to be used for communication. The original protocol allows a clinician to attach a patient to the smart control node for collection of telemetry. The second protocol allows the patient telemetry to be sent from the smart control node to the clinical server in a secure manner and for command and control instructions to be sent in either direction. The BAN analysis of the protocols shows that mutual authentication and key agreement is achieved for both of these protocols. We have limited messages and use hashing functions to limit the resource usage.

Chapter 4:

Authentication for Medical Wireless Sensor Networks

The protocol developed for the sensor nodes allows the smart control node to communicate securely with the sensors to send or receive information. Mutual authentication and key agreement is achieved between the smart control node and the sensor node while using the clinical server as a mediator. The re-authentication allows for the sensors to communicate securely with the smart control node even in the absence of a connection to the clinical server. All of the protocols use minimal resources and messaging to achieve the desired results as can be seen with the BAN analysis.

Chapter 5

Patient Privacy : Study and Recommendations

Patient privacy is of the utmost concern in any clinical system. Clinicians will try to gather as much data as possible since any minor facet of a patient's life can have an impact on their health. To have a full picture and be able to fully analyze the problems a patient is having, health care providers would prefer to have knowledge of even the most minor of details. There are many different types of health information that heathcare providers will try to record and collect about a patient to be able to have a robust picture of their health as

shown in Table 5-1. Other data that clinicians try to collect may not seem to be immediately medically relevant but demographic information can also be used in patient diagnosis. Some of the types of demographic information stored by healthcare providers are listed in Table 5-2.

Table 5-1: Types of clinical data stored in clinical systems.

Diseases	Disabilities	Predicted Health Indicators
Medications	Mental Health	Psychological Stability
Psychological Therapy	Diet	Drug Use (Legitimate and illicit)
Exercise Habits	Genetic Code	Sexual Habits (disclosed or supposed)
Treatments	Allergies	Family Disease History
Height	Weight	Laboratory Test Results
Imaging		

Table 5-2: Types of demographic data stored in clinical systems.

Education	Employment (and History)	Marital Status
Family Relationships	Address (and History)	Phone Number (and History)
Birth Date	Religion	Language
Sexual Orientation	Health Card Number	Drivers License Number
Race	GPS Location	

Healthcare providers try to collect and store the most intimate details of our lives to be able to properly diagnose any health issues a patient may experience. This information could be put to many nefarious uses if it gets into the hands of the wrong people. To limit patient exposure to black mail and other undesired effects of the release of this information it is required that patient privacy be maintained.

Patient Privacy must be maintained to limit the release of this private information to only those clinicians directly responsible for the care of a patient. This implies that the sensitive information will not be released to clinicians not responsible for the care of the patient or to any outside party that should not have access to or knowledge of the sensitive information. Both the Canadian and American governments have tried to tackle the issue of patient privacy by crafting laws that apply to the care and control of patient information. As mentioned in section 2.1 Canada has developed the Personal Information Protection and Electronic Documents Act and the United States has enacted the Health Insurance Portability and Accountability Act. This legislation calls for the utmost care to be taken with patient/personal information.

When considering new advances in clinical care and with the advent of wireless technology, the amount of information that is collected by clinical providers is growing massively. It is now possible for many different methods to breach patient privacy. A passive observer can simply record the information a patient system is transmitting to discern the location of the patient. If the information is transmitted without care for the confidentiality of the information then the observer can have direct access to that information. Active attacks on privacy can come from many directions. The wireless communication medium is particularly attractive to attack. Other active attacks on patient privacy can be carried out by employees and clinicians related to the health care provider that abuse their privileges to discover the personal information of a patient for which they do not provide care. These types of attacks need to be addressed by defining the types of privacy that should be afforded to the patient.

Chapter 5:

The location of a patient can be used to discern some personal information because it is possible to surmise the sexual orientation of a patient that visits establishments known for homosexual or heterosexual activity. The home address of a patient can be discovered or the work address can be found simply by observation of the communication sent by the patient. Protecting the patient location from observers and attackers will be referred to as location privacy.

Patient identity can also be discovered by tracking the identity of the wireless devices if they are brought into an environment where the identity of the patient can be learnt. Then the identity of the patient can be associated with the wireless identity for the entire time the wireless device uses those identities. This type of protection of privacy that hides the identity will be referred to as identification privacy.

The information stored in a system can be used to inappropriately breach the privacy of a patient. If the information is anonymized or unlinked from the patient then it could be protected from unauthorized access if the methodology for anonymizing or unlinking still allows authorized users to access the data. Creating this anonymous linkage will be referred to as information privacy.

5.1 Location Privacy

The location of a patient can be used to infer many different aspects about their personal life and health. If that location is not kept private it is possible for observers and attackers to discern private information that should be protected.

5.1.1 Mist Protocol

Chapter 5:

Maglogiannis, et al. [45] describe a modified Mist protocol, originally designed by Al-Muhtadi, et al. [46] that is used to keep the location of the patient private. The patient will perform a registration phase with the system to select the desired Lighthouse that has knowledge of the patient identity but does not know the location of the patient as shown in Figure 5.1 which shows the 4 steps to complete the registration process required to begin the process of creating a Mist circuit. The user sends a request for registration to the Mist portal. The portal replies with a list of routers within the hierarchy that are available as lighthouses for the user. The user then selects the desired lighthouse where ones closer to the user will increase the efficiency of communication at the cost of a potential loss in privacy and choosing a lighthouse closer to the root of the hierarchy will increase privacy while causing a loss in communication efficiency. After the selection of the chosen Mist router to act as a lighthouse a Mist circuit is then established between the user and the lighthouse.

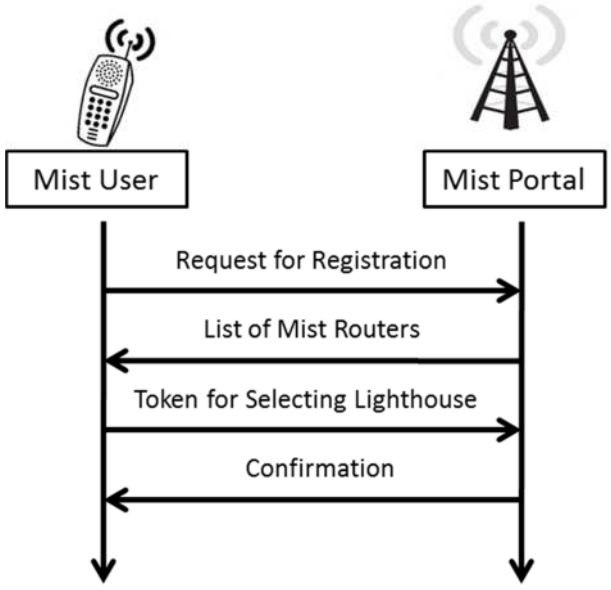


Figure 5.1: Registration in MIST protocol.

To create the Mist circuit the user will send

The Mist Portal that the patient is attached to knows the location of the patient but not the identity. Any communication with the patient is initiated with the lighthouse node (any routing node can be the lighthouse) in the MIST network. The lighthouse node then relays the information through the Mist routing nodes to the portal node. Each of these Mist routing nodes will have an identity lookup table for routing the information to the next router until the portal node is finally reached. The portal knows the location of the patient and will send the information to the patient devices but the portal does not know the identity of the patient that is used to identify them in the system. The path of communication is shown in Figure 5.2.

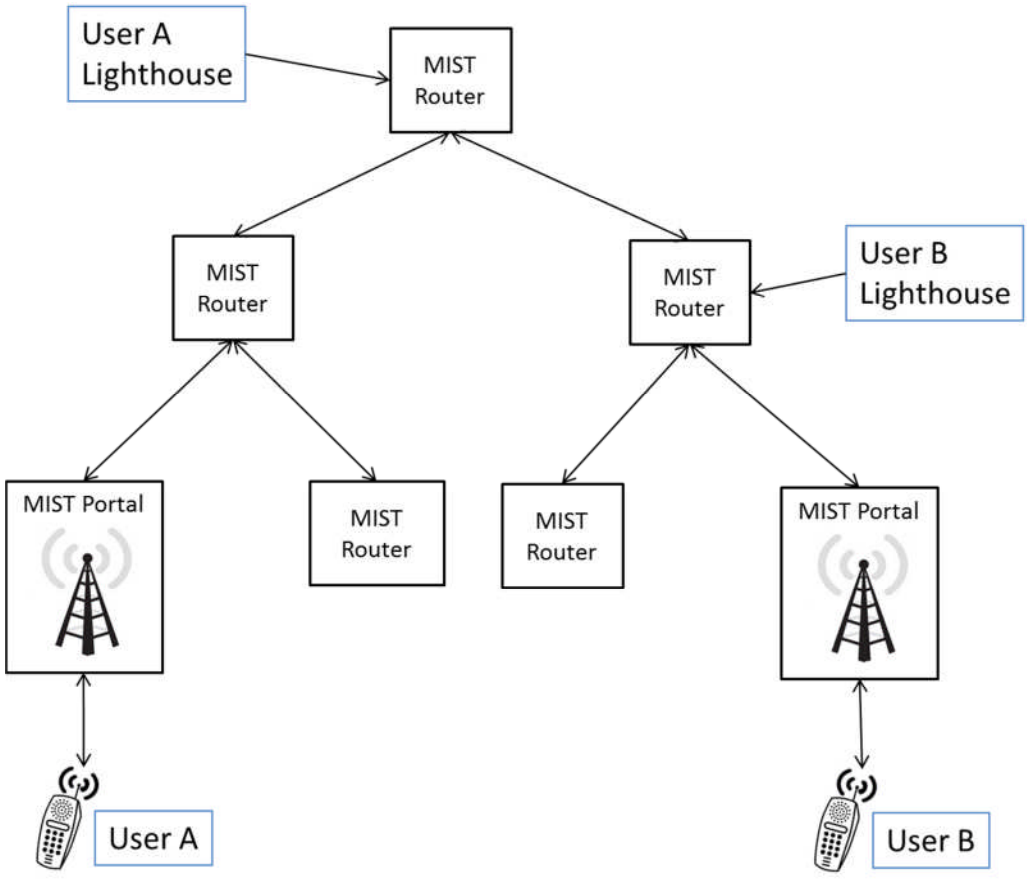


Figure 5.2: Path of communication in MIST protocol.

The figure shows two different devices that are going to communicate over a MIST enabled network. The MIST routers can either act as a router or lighthouse for communication purposes. When acting as a router the router maintains a table of aliases for each device that is lower on the tree. The Users A and B can be any combination of patient or clinician in the system that wish to have real time information from the other user available for their use. When user B attempts to communicate with user A they use their lighthouse to send the information and will discover the lighthouse of User A as the destination.

The resulting communication network allows for communication with the patient while protecting the location of the patient from discovery. The modification proposed by Maglogiannis, et al. [45] allows for different lighthouses to be used for outbound messaging instead of the one that the patient system registers with to hide their location. This increases the difficulty in discovering the location of the patient if most information is inbound into the system from the patient location. The basic principle in this architecture is that each Mist router acts as a proxy removing the identifying information and replacing it with information stored in a lookup table.

5.1.2 The Onion Protocol (TOR)

Outside of a controlled clinical environment the Mist routing protocol will not be able to address location privacy due to the usage of the internet as a communication channel between the patient sensor system and the clinical server and the lack of control over the devices outside of the clinical environment. TOR [47] is a widely deployed network

overlay that provides online anonymity to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis.

TOR helps protect privacy by distributing transactions over several places on the internet so that no single attacker can link the patient to the hospital. The patient creates a private network pathway by building a circuit of encrypted connections through different relays in the TOR network. The relays never know the complete path that a data packet has taken. The nature of the TOR network creates location anonymity and privacy for the patient.

TOR also allows for the creation of hidden services that are only available within the TOR network. This allows the hospital to create a protected service which protects the location of the service. Hiding the services lets the patient know that the fact they are communicating with the hospital will be hidden from any attackers.

5.2 Identification Privacy

When using any technology there is usually some identity applied to ensure that the client technology can be properly recognized by the servers. This identity can be related to the patient and then used to gather information on the patient or to track the patient causing a breach of their privacy. To conceal this identity Garcia-Morchon, et al. [48] use privacy aware identification. The framework they have developed requires a smart tamper resistant healthcare card (HCC) as an integral part of their security. The healthcare card contains the Unique Patient Identifier (UPI) which can be used in any clinical system to identify the patient similar to an Ontario health insurance plan number or social security number. The privacy aware identification creates a hierarchy of pseudonyms which are derived from the

UPI but cannot be linked back to the UPI without authorization of the patient or central healthcare authority which prevents unauthorized users from linking the patient identity to the data generated in the Personal Area Network (PAN). The $ID_{PAN|MSN}$ is a master session identifier for the PAN and MSN relationship which is the only identifier known to the MSN (the MSN has no knowledge of the UPI). The $ID_{PAN|MSN}$ is generated with a hash function of the UPI, the MSN identifier (ID_{MSN}) and the PAN master symmetric key ($K_{Master\text{-}UPI}$). The $K_{Master\text{-}UPI}$ is a secret symmetric key kept on the HCC.

$$ID_{PAN|MSN} = h(UPI||ID_{MSN}||K_{Master-UPI}) \tag{5.1}$$

$$ID_{PAN|MSN-i} = h(ID_{PAN|MSN}||h(K_{Master-UPI}||ID_{MSN})||S_i) \tag{5.2}$$

The equations are used to generate the identification of the Personal Security Manager when connecting to any telemetry system on the patient. The identity will change with each communication session (S_i) to hide the identity over a long period of communication as shown in equation 5.2. Equation 5.1 will be used while the MSN communicates with the PSM to generate $ID_{PAN|MSN}$ this is done over Body Coupled Communication (BCC) to ensure it is not discovered. The identifiers are updated with the change of the session which keeps the patient identifier private.

5.3 Information Privacy

One of the more difficult areas of privacy to maintain is information privacy. To maintain the anonymized or unlinked information from the patient while still being able to have a usable system takes extreme care and effort. The major concern to information privacy is the inappropriate use of access and collaborative use of access to compromise

patient privacy. Clinicians that can see one patient in most patient systems can usually see all of the patients in a system. This can lead to a clinician searching and breaching the privacy of patients that the clinician is not treating. Sun, et al. [49] attempt to preserve information privacy during Emergency Response situations with Wireless body sensor networks. The scheme presented protects patient information from undesired breaches of privacy after access has been given to the emergency medical technician (EMT). The EMT needs access to the immediate (based on a time period) and relevant clinical information of the patient but does not need as much historical information or other non-emergency information. The scheme involves the unlinkability of information in the systems that store the medical data causing anonymity of the data.

The patient PDA is initially registered with a central credential authority where the patient obtains an anonymous credential for future authentication with the remote server. The PDA stores the monitored medical data collected in each time period with an unlikable sequence number that the EMT cannot link to the medical data collected in other time periods unless authorized by the patient. When the PDA gains knowledge of a possible emergency from abnormal signals from the body sensors it will contact the primary physician who will evaluate the situation and request emergency services if required. The EMT that responds will demand the necessary medical data from the PDA which may accept only a reasonable date range for the request. The PDA will then give the desired identifiers to the EMT to gain access to the requested data. The identifiers given cannot be used to retrieve other patient information and cannot be linked to other data on the patient.

Chapter 5:

The data storage on the remote server that both the patient and the EMT use requires the patient PDA to follow a preparation phase on the data to create the unlinkability. The PDA selects a random secret seed (RSS) as input into a pseudo random number generator (PRNG). The PRNG will generate pseudorandom serial numbers ($s_1 \ldots s_n$) for each update period (3-5 days) of clinical data. The PDA will then compute tags as a hash of each serial number where $t_i = h(s_i)$. Those tags are then sent to the server with the medical data to be used for identification of the data by the EMT. When the EMT requests access to the data the PDA will use the RSS for the desired and approved periods to generate the serial numbers and then the tags. The tags are sent to the EMT to be able to retrieve the desired data. The EMT is unable to generate other tags that are related to the patient from the tags given which shows the unlinkability but the EMT can gain access to the required data to properly handle the medical emergency.

Chapter 6

Concluding Remarks and Future Work

The application of wireless communication to the medical field will have many beneficial and far reaching impacts on the way healthcare is delivered. The legislated requirements relating to the handling of clinical and personal information require that security be at the core of any system developed for a clinical application. HIPAA in the United States of America and PIPEDA in Canada are two examples of government legislation that have a direct impact on the way that health and personal information can be collected and transmitted. Major issues are the confidentiality and integrity of the information collected and transmitted which requires a strong method of authentication and key agreement. To address these privacy and legislated issues authentication, key

agreement, encryption, and integrity hashing are required technologies that need to be implemented in any Medical Wireless Sensor Network.

The existing wireless authentication frameworks are investigated; these networks are currently deployed and have undergone extensive testing and have withstood a great number of real world attacks. The authentication in WEP, WPA and WPA2 are discussed, showing the problems that existed in the older protocols and how they were overcome by the next generation of technology and protocols. The issues in WEP are not related to the encryption algorithm but the implementation of the protocol that cause the weaknesses. We also investigate the mobile wireless network protocols, showing the different evolutionary constraints on the systems that are deployed and developed. A major issue with the integration of GSM and UMTS security protocols is revealed and two solutions are proposed showing how to increase the security by using simple hashing techniques.

The information gained from examining the existing wireless protocols gave a foundation for the protocols designed in this thesis. The protocols are designed to achieve mutual authentication and key agreement for secure communication between the smart control node, clinical server and sensor nodes use minimal messages. The protocols also avoid public key encryption due to the increased processing and resources required to implement public key protocols. The protocols are analyzed using BAN analysis showing that they are secure and achieve the desired result of mutual authentication and key agreement.

Other aspects of privacy are then investigated with possible methods of addressing the privacy issues. Location privacy is of large concern and will need to be addressed and

the MIST and TOR protocols meet some of the needs of location privacy. The issues of identification and information privacy are also discussed with an overview on possible solutions to address those problems.

The protocol developed is an excellent foundation for the implementation of wireless sensors for healthcare. This thesis addresses the legal requirements of privacy required by both Canada and the United States. The protocols developed will allow for the application of sensors to many different areas of clinical telemetry.

6.1 Future Work

The further development of the protocols presented in this thesis, to meet the growing privacy needs of both patients and clinicians, is a worthwhile avenue of research. The intent of this researcher is to attempt to create a practical working product for use in clinical environments and to begin to properly leverage wireless communication within the healthcare environment.

Bibliography

1. U. S. Government, “Health insurance portability and accountability act,” 1996. [Online]. Available: http://www.gpo.gov/fdsys/search/pagedetails.action?granuleId=CRPT-104hrpt736&packageId=CRPT-104hrpt736.
2. G. of Canada, “Personal information protection and electronic documents act,” April 2000. [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html.
3. G. of Ontario, Canada, “Personal Health Information Protection Act,” 2004. [Online]. Available: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.
4. G. of Ontario, Canada, “Freedom of Information and Protection of Privacy Act,” 1987. [Online]. Available: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm.
5. J. Polastre, R. Szewczyk, and D. Culler, “Telos: Enabling ultra low power wireless research,” in Proc. 4th Int. Symp. Inf. Process. Sensor Netw., Los Angeles, CA, 2005, pp. 364–369.
6. MICA Sensors, http://gyro.xbow.com/Products/Wireless_Sensor_Networks.htm.
7. P. Levis et al., “TinyOS: An operating system for sensor networks,” in Ambient Intelligence, W. Weber, J. Rabaey, and E. Aarts, Eds. Berlin: Springer, 2005, pp. 115–148.
8. V. Shnayder, B. Chen, K. Lorincz, Thaddeus R. F. Fulford J. and M. Welsh, Sensor Networks for Medical Care, Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2005, ftp://ftp.deas.harvard.edu/techreports/tr-2005.html.
9. B. Sarikaya, M. A. Alim, and S. Rezaei, “Integrating wireless eegs into medical sensor networks,” in Proceedings of the 2006 international conference on Wireless communications and mobile computing, ser. IWCMC ’06. New York, NY, USA:

ACM, 2006, pp. 1369–1374. [Online]. Available: http://doi.acm.org/10.1145/1143549.1143823

10. P. Kumar, Y.-D. Lee, and H. Lee, “Secure health monitoring using medical wireless sensor networks,” in Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on, aug. 2010, pp. 491 – 494.
11. H. Lee and K. Chen, “Pingpong-128, a new stream cipher for ubiquitous application,” in Convergence Information Technology, 2007. International Conference on, nov. 2007, pp. 1893 –1899.
12. M. Sain, P. Kumar, and H. J. Lee, “Secure authentication and communication in ubiquitous healthcare middleware,” in Advanced Communication Technology (ICACT), 2011 13th International Conference on, feb. 2011, pp. 173 –178.
13. A. B. Waluyo, I. Pek, X. Chen, and W.-S. Yeoh, “Design and evaluation of lightweight middleware for personal wireless body area network,” Personal Ubiquitous Comput., vol. 13, pp. 509–525, October 2009. [Online]. Available: http://dx.doi.org/10.1007/s00779-009-0222-y
14. N. S. Agency, “Skipjack and kea algorithm specifications,” Tech. Rep., May 1998. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf
15. K. Singh and V. Muthukkumarasamy, “Authenticated key establishment protocols for a home health care system,” in Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on, dec. 2007, pp. 353–358.
16. S. Bellovin and M. Merritt, “Encrypted key exchange: password-based protocols secure against dictionary attacks,” in Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on, may 1992, pp. 72 –84.
17. B. Tong, S. Panchapakesan, and W. Zhang, “A three-tier framework for intruder information sharing in sensor networks,” in Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON ’08. 5th Annual IEEE Communications Society Conference on, june 2008, pp. 451 –459.

18. M. Kim and K. Chae, “Adaptive authentication mechanism using node reputation on mobile medical sensor networks,” in Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, vol. 1, feb. 2008, pp. 499 – 503.
19. K. Malasri and L. Wang, “Addressing security in medical sensor networks,” in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, ser. HealthNet ’07. New York, NY, USA: ACM, 2007, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/1248054.1248058
20. K. Ren, W. Lou, K. Zeng, and P. Moran, “On broadcast authentication in wireless sensor networks,” Wireless Communications, IEEE Transactions on, vol. 6, no. 11, pp. 4136 –4144, November 2007
21. X. Du, S. Guizani, Y. Xiao, and H.-H. Chen, “Nis01-1: An efficient key management scheme for heterogeneous sensor networks,” in Global Telecommunications Conference, 2006. GLOBECOM ’06. IEEE, 27 2006-dec. 1 2006, pp. 1 –5
22. S. Camtepe and B. Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks,” Networking, IEEE/ACM Transactions on, vol. 15, no. 2, pp. 346 –358, April 2007.
23. O. Morchon and H. Baldus, “Efficient distributed security for wireless medical sensor networks,” in Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on, dec. 2008, pp. 249 – 254.
24. R. L. Rivest, “The rc5 encryption algorithm,” in Fast Software Encryption, 1994, pp. 86 –96.
25. D. E. Eastlake and P. E. Jones, “US secure hash algorithm 1 (SHA1),” Tech. Rep. [Online]. Available: http://www.ietf.org/rfc/rfc3174.txt?number=3174
26. NIST Special Publication 800-38A, [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
27. Digital cellular telecommunications system (Phase 2+), "Security mechanisms for SIM application toolkit; Stage2", (3GPP TS 03.48 version 8.8.0 Release 1999).

28. Eric Southern, Abdelkader Ouda and Abdallah Shami, “Wireless Security: Securing Mobile UMTS Communications from interoperation of GSM”, submitted to Special Issue on “Security in Wireless Ad Hoc and Sensor Networks with Advanced QoS Provisioning”, Wiley Journal on Security and Communication Networks.
29. ”Brief History of GSM & the GSMA”, GSM Association. 2008; http://www.gsma.com/aboutus/history/ (19 June 2012).
30. GSM 02.09, “Digital cellular telecommunications system (Phase 2+); Security Aspects”, version 6.1.0, Release 1997.
31. A Kerckhoff, “La cryptographie militaire,” Journal des sciences militaries, vol. IX, p. 538, Jan 1883.
32. A. Biryukov, A. Shamir, and D. Wagner, “Real time cryptanalysis of a5/1 on a pc,” in In FSE: Fast Software Encryption. Springer-Verlag, 2000, pp. 1-18..
33. E.Barkan, E. Biham, and N. Keller, “Instant ciphertext-only cryptanalysis of gsm encrypted communication.” Springer-Verlag, 2003, pp. 600-616.
34. 3GPP, “Secuirty Objectives and Principles,” https://www.3gpp.org/ftp/Specs/html-info/33120.htm, 3rd Generation Partnership Project (3GPP), TS 33.120, (Apr. 2001).
35. O. Dunkelman, N.Keller, and A. Shamir, “A practical-time attack on the a5/3 cryptosystem used in third generation gsm telephony,” Cryptology ePrint Archive, Report 2010/013, 2010.
36. G. Mapp, M. Aiash, A. Lasbae, and R. Phan, “Security models for heterogeneous networking,” in Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, July 2010, pp.1-4.
37. Scott Fluhrer, Itsik Mantin, and Adi Shamir. “Weaknesses in the key scheduling algorithm of RC4”, Lecture Notes in Computer Science, 2259:1–24, 2001.
38. 3GPP TS 33.102, “3G Security; Security architecture”, Release 9, 2009.
39. 3GPP TS 33.401, “3G security; Security architecture, 3GPP System Architecture Evolution (SAE); Security architecture”, Release 11, 2011.
40. M. Burrows, M. Abadi, R. Needham. “A logic for authentication,” DEC System Research Technical Report No 39, Feb 1989.

41. 3GPP TR 33.902, “Formal analysis of 3G authentication and key agreement protocol”, V4.0.0, 2001-09.
42. Shi Shi-ying; Mao Yu-ming; , "An Improvement Key Distribution Protocol and Its BAN Analysis," Future Computer and Communication, 2009. ICFCC 2009. International Conference on , vol., no., pp.381-384, 3-5 April 2009
43. Cai Qingling; Zhan Yiju; Wang Yonghua; , "A Minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis," Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on , vol.2, no., pp.449-453, 3-4 Aug. 2008
44. Abdellatif, R.; Aslan, H.K.; Elramly, S.H.; , "New real time multicast authentication protocol," Computer Engineering & Systems, 2008. ICCES 2008. International Conference on , vol., no., pp.245-250, 25-27 Nov. 2008
45. Maglogiannis, I.; Kazatzopoulos, L.; Delakouridis, K.; Hadjiefthymiades, S.; , "Enabling Location Privacy and Medical Data Encryption in Patient Telemonitoring Systems," Information Technology in Biomedicine, IEEE Transactions on , vol.13, no.6, pp.946-954, Nov. 2009
46. Al-Muhtadi, J.; Campbell, R.; Kapadia, A.; Mickunas, M.D.; Seung Yi; , "Routing through the mist: privacy preserving communication in ubiquitous computing environments," Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on , vol., no., pp. 74- 83, 2002
47. R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The SecondGeneration Onion Router,” in Proc. of the 13th USENIX Security Symposium, 2004.
48. Garcia-Morchon, O.; Falck, T.; Heer, T.; Wehrle, K.; , "Security for pervasive medical sensor networks," Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International , vol., no., pp.1-10, 13-16 July 2009
49. Jinyuan Sun; Xiaoyan Zhu; Yuguang Fang; , "Preserving Privacy in Emergency Response Based on Wireless Body Sensor Networks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE , vol., no., pp.1-6, 6-10 Dec. 2010

VITA

Name:	Eric Southern
Post-secondary Education and Degrees:	**Bachelor of Engineering Science – Software Engineering** University of Western Ontario, London, ON **Bachelor of Science – Computer Science** University of Windsor, Windsor, ON
Honours and Awards:	Ontario Scholar (1996) Admission Scholarship UWO (1996)
Related Work Experience:	**Commissioner** London Transit Commission, London, ON **Senior Software Developer** London Health Sciences Centre, London, ON **Programmer Analyst** London Health Sciences Centre, London, ON
Publications:	

1. Eric Southern, Abdelkader Ouda and Abdallah Shami, "Wireless Security: Securing Mobile UMTS Communications from interoperation of GSM", Special Issue on " Security in Wireless Ad Hoc and Sensor Networks with Advanced QoS Provisioning", Wiley Journal on Security and Communication Networks. (Accepted)

2. Eric Southern, Abdelkader Ouda and Abdallah Shami, "Securing USIM-based Mobile Communications from Interoperation of SIM-based Communications", the International Journal for Information Security Research (IJISR), Volume 2, Issues 1/2, pp. 313-324, ISSN 2042-4639, March/June 2012.

3. Eric Southern, Abdelkader Ouda and Abdallah Shami, "Solutions to Security Issues with Legacy Integration of GSM into UMTS", the 6th International Conference on Internet Technology and Secured Transactions (ICITST 2011, Abu Dhabi, United Arab Emirates (UAE), December 2011.