Chapter 11
Securing and Prioritizing Health Information in TETRA Networks

Konstantinos Siassiakos
University of Piraeus, Greece

Athina Lazakidou
University of Peloponnese, Greece

ABSTRACT

Cost reduction pressures and the need for shortened in-patient stays are promoting the use of wireless patient monitoring systems in hospitals. Their contribution to better process management, superior flexibility and increased efficiency within hospitals is further underlining the appeal of wireless networking options for patient monitoring systems. Wireless connectivity has encouraged an overall rise in productivity through improved workflow and data management. Wireless patient monitors have also supported enhanced flexibility within the hospital environment by enabling remote monitoring of patients. TETRA technology provides several ways of protecting the privacy and security of communication, such as authentication, air interface encryption and end-to-end encryption. The objective of this chapter is to study how simply can a healthcare professional collect physiological data from mobile and/or remote patients and how securely and reliably health information can be transferred from emergency places to hospitals through a TETRA network.

INTRODUCTION

Today's healthcare professionals need to be connected to the network always. Continuous connectivity is the watchword of these demanding users, who need to communicate over the network seamlessly and stay connected everywhere in emergency cases.

Telemedicine applications, including those based on wireless technologies, span the areas of emergency health care: telecardiology, teleradiology, telepathology, teledermatology, teleophtlalmology, teleoncology, and telepsychiatry. In addition, health telematics applications, enabling the availability of prompt and expert medical care, have been exploited for the provision of healthcare services at understaffed areas, such as rural

DOI: 10.4018/978-1-61692-895-7.ch011

health centers, ambulance vehicles, ships, trains, and airplanes, as well as for home monitoring.

The primary problem with tiny, low power sensors is to establish and maintain wireless links in the presence of so many high power devices that radiate noise. This noise will change through out the day so that a continuously adapting routing technique is needed. Unfortunately, several challenges exist such as:

1. Deploying sensors to provide proper sensor coverage.
2. Balancing resource usage to maximize sensor lifetime.
3. Communicating messages reliably among the nodes (i.e. healthcare provider, patient, emergency vehicles) using multihop paths.
4. Prioritizing routing messages, e.g., emergency call vs. outgoing patients.
5. Authenticating data links as well as securing the data to ensure patience confidentiality.

BACKGROUND

High quality health care requires individuals to share sensitive personal information with their doctors and other healthcare professionals. This information is necessary to make the most accurate diagnoses and provide the best treatment. It may be shared with others, such as insurance companies, pharmacies, researchers, and employers, for many reasons. If patients are not confident that this information will be kept confidential, they will not be forthright and reveal accurate and complete information. If healthcare providers are not confident that the organization that is responsible for the healthcare record will keep it confidential, they will limit what patients add to the record. Either of these actions is likely to result in inferior healthcare. The privacy and security of personal health information has become a major public concern.

Safety is always a first priority, followed closely by concern for the environment. Effective communication during an emergency evacuation, shut-down or man-down alarm is a clear instance where the right wireless communications technology is required.

A wireless communications system is also a tool that will be used to help protect investments and personnel against criminal or even terrorist threat. However, today's criminals are tech-savvy, thus any system must be secure, against potential mis-use, if it was to fall into the wrong hands.

Requirements fall into six key areas: Flexibility & Scalability; Efficient Communications, Reliability and System Availability; Data Communications; User Environment & Interface; and Operations and Maintenance. So what is TETRA and how does it meet expectations in each of these vital areas?

The most common information security problem within the healthcare systems is the access of the employees (inside threat). Specifically people who work in a hospital have the ability to view protected health information (PHI) of anybody. This raises the probability for a legal action, which cause major impacts. It is conceivable how important it is to enforce security policies. It is important to introduce security policies, which guide the decisions made by people who have the authority and set the boundaries under which the staff could operate. Apart from the inside threat, damage in a healthcare system may occur by an outside threat such as hackers. In this case it is very important to develop mechanisms which minimize the risk. So we must not allow any insecure Internet connection in the internal network of the healthcare system.

The ***first security risk*** is the failure to protect sensitive data beyond encryption.

The ***second security risk*** is the inability to accurately manage mobile computer assets. Under HIPAA, healthcare organizations must be able to audit how many computers they have in their