Security and Authentication Architecture Using MPEG-21 for Wireless Patient Monitoring Systems

Wolfgang Leister and Truls Fretland
Norsk Regnesentral
Oslo, Norway
email: {wolfgang.leister, truls.fretland}@nr.no

Ilangko Balasingham
Interventional Center
Rikshospitalet University Hospital
Oslo, Norway
email: ilangkob@medisin.uio.no

***Abstract*—Privacy and security are two major concerns in the ubiquitous deployment of wireless patient monitoring systems, where wireless sensor networks become an integral part of the monitoring process. To address and handle threats which arise from the use of wireless sensors, we propose a framework using MPEG-21. MPEG-21 is an architecture that can handle end-to-end management of multimedia content in diverse networks. We propose and evaluate a framework that is designed to protect patient monitoring systems using resource-constrained wireless sensor networks. The analyses show that security architectures based on the MPEG-21 framework can handle a variety of threats. We also present a test bed in which our framework is about to be implemented.**

***Index Terms*—MPEG-21, security, biomedical sensor networks, medical digital item**

I. Introduction

Patient monitoring systems are one of the major data sources in a health care environment. These typically consist of sensors which are connected to the patient, communicate by wire or wirelessly to a bedside monitoring device. Furthermore, the sensor data are stored in databases, which are connected to the health care enterprise's information infrastructure for storage, maintenance and retrieval of data. Health Care information systems can be interconnected in order to exchange data, where patient monitoring systems become an integral part of the networked infrastructure. This facilitate data to be available to the different user terminals and systems both inside and outside the enterprise. Therefore, an end-to-end security mechanism is needed to protect the medical data, as we presented recently [1].

Wireless technology is increasingly used in health care enterprises to eliminate the use of cables in patient monitoring systems, providing mobility advantages for patients and medical personnel. In this case the sensors communicate wirelessly with monitoring systems, which are located close to the patient. However, wireless communication can be intercepted easily. Threats to security goals like confidentiality, integrity, and availability of data still apply, and weaknesses of the system treating health care data could be exploited by attackers.

A biomedical sensor network (BSN) can be considered a special case of a wireless sensor network (WSN). A WSN often comprises tiny, low-cost wireless electronic devices, capable of gathering vital signs and environmental information and forwarding them to a base station. The limited computational and communication capabilities, their reduced cost, and enforced size introduce resource-related challenges in their function, efficiency, and security. Attacks can compromise system security with negative consequences for both the patient, the health care enterprise, and third parties. This exhibits that the security requirements need careful consideration during design, development and deployment for the whole infrastructure including the patient monitoring systems and BSN.

State-of-the-art systems in health care enterprises employ technical approaches [2] such as service-oriented architectures (SOA) [3], [4], in order to address re-usability, interoperability, and portability. For some application areas standards such as DICOM [5], [6] are used. However, none of these technologies addresses content adaptation taking into account of characteristics of end user terminals (screen size, resolution, real time rendering capabilities, etc.), the user's preferences (automatic update, popup menu and functions, etc.), and wireless channel conditions (bandwidth, data rate, packet loss, interference environment, etc). However, MPEG-21 is one potential technology which can support a set of quality of service metrics, security features as well as the above mentioned adaptation features to internal factors. Therefore MPEG-21 appears to be a far better solution for wireless sensor networks than other above mentioned standards and technologies.

MPEG-21 [7], [8] is an international standard on multimedia services and provides a multimedia framework at the application level to enable transparent and augmented use of multimedia resources across a wide range of networks and devices. MPEG-21 addresses sharing and transferring digital media content, including management, adaptation of resources, protection of privacy, integrity, and digital rights.

The contribution of this paper is a novel approach to protect the application layer of medical data in patient monitoring systems using BSN. The paper is organised as follows: Section III gives an overview of security issues for wireless patient monitoring systems and biomedical sensor networks, including a generic system model. Section IV discusses the security assumptions and requirements for such systems, which lead to a short threat assessment in Section V. Section VI reviews the relevant parts of MPEG-21 which are used in our proposed

architecture that is presented Section VII. In Section VIII we discuss the employed security mechanisms and the suitability before concluding the paper.

II. Related Work

Regulations for handling health care data are strict in most parts of the world. This is manifested by the relevant legislation in Norway [9] and the European Union [10]. Especially the issues of privacy and data integrity are stated in these documents.

The security issues of wireless sensor networks (WSN) have become an important research topic. We base our work on an overview of security goals, threats, attacks and countermeasures on all communication layers [11] and perform analyses on BSNs given their constraints using literature on security issues in WSN [11], [12], [13]. There are still many unsolved security issues, such as the integrity of the collected data and the privacy of the patient [14], [15].

One of the ongoing works is the IEEE 802.15.6 standard for body area sensor network [16]. The submitted proposals so far on security provisions discuss issues related to outgoing and incoming frame security procedures, higher layer security functions in the medium access (MAC) layer, common and different information elements across layers, encryption key usage, handling and update, etc. Incorporation of parts of the MPEG-21 in this proposed standard may become beneficial to handling security provisions as well as quality of services in a single framework.

The recently approved standard IEEE 1451.5 [17] envisions encryption and security functionalities in the presentation layer of sensor networks. The framework proposed in this paper uses MPEG-21, which also addresses issues in the presentation layer. Therefore, a combination of MPEG-21 and IEEE 1451.5 can be interesting.

It will be a challenging task to design and deploy appropriate security mechanisms that take availability, user friendliness, high throughput of data, etc. into consideration. Early work on using MPEG-21 as a framework in health care has been conducted by Landén [18], which has been recently extended [19] to include the hospital infrastructure. After a threat analysis of patient monitoring systems [20] we extended this architecture to include BSN [1].

Other approaches to use MPEG-21 in health care use the IPMP part of MPEG-21 for patient records [21]. Recently, a framework for using MPEG-21 IPMP components for a security framework for pervasive health care architectures has been presented [22], including wireless communication between personal digital assistants (PDA). While this work introduces MPEG-21 for medical applications, our work includes the use of MPEG-21 for BSN and uses a generic model to analyse the threats.

III. Patient Monitoring Systems

Patient monitoring systems and BSNs can be applied in a variety of health care scenarios ranging from paramedic, diagnostic, surgical, to post-operative phases. In general, patient monitoring systems comprise of different kinds of sensors, data communication, storage, processing, and presentation of medical data. In order to articulate the security requirements we identify three important scenarios: (1) hospital scenario (using an array of biomedical sensors for diagnostics, surgical, and post operative phases), (2) nursing and citizen homes (patients equipped with wireless biomedical sensors triggering alarms; surveillance of patients after being discharged from hospital), and (3) paramedic.

A. Biomedical Data

While a health care information system must handle all types of medical data, we concentrate on biomedical sensor data. The sensor nodes measure biomedical signals, process them and transmit the results to a sink node. Typical biomedical data measured by biomedical sensors can be electrocardiogram (ECG), electroencephalography (EEG), blood oxygen saturation, blood pressure, temperature, and sound. They are data samples at a given sampling resolution and sampling rate with typical data rates from some few bits per second (bps) up to 12000 bps. The sampling rate and resolution are examples of biomedical metadata, that is, data that contain information about the biomedical measurements. In the near future also images and video, will emerge as data types from BSN.

Biomedical data can be described as streamed multimedia data with corresponding requirements about confidentiality, integrity, availability, as well as data authenticity, service quality and adaptation.

The biomedical sensor data consist of one or several tracks of sampled measured values, supplemented with metadata, e.g., a time-stamp and the identity of the sensor. The biomedical data must be protected against modification and deletion. While it is necessary to implement a detection mechanism for modification and deletion, the reconstruction of data destroyed by an attacker would be desirable, in order to provide the availability of data.

B. A Model for Wireless Patient Monitoring Systems

A generic system model for the overall patient monitoring system and threat analysis have been proposed [20], where the components and communication channels have been identified.

The generic system model, shown in Fig. 1, illustrates that patient data are generated by sensors attached to a patient. In a concrete instance of this model, each abstract component can be realised by means of several physical components, and a physical component again can be realised as several abstract (sub-)components. A biomedical sensor network consists of several sensor nodes that measure biomedical data. These data, accompanied by metadata, are transmitted by a wireless network (Channel A) to the sink of the wireless network and to the patient data collector (PDC). The PDC collects different data streams for a patient and forwards data to the health care information system at the hospital (Channel B), or to the patient data accessing unit giving data access to the medical staff on site (Channel E). The ID data mapper functionality

(Channel G) is necessary to handle patients, where the identity might not be known. To implement Channel G no real communication needs to be involved while the system is in use. Retrieval of patient data from the health care information system involves Channel D.

The **components** of the generic system model are:

- *Sources* of patient data, e.g., sensors, storage units, or user input devices. Each source is attached to only one patient at a time. A source is assumed to have very limited capabilities of protecting the communication.
- *Patient Data Collectors (PDC)* collect patient data from one or more sources. A PDC is trusted to handle unencrypted, personally identifiable patient data.
- The *Health Care Information System (HCIS)* receives patient data for processing or storage.
- The *Patient Data Accessing Unit (PDAU)* receives patient data and presents these to the medical staff.
- The logical element *ID-data mapper* determines the identity of the patient to whom patient data pertains and sends the identity to the PDC or the HCIS. The ID-data mapper is usually implemented as an interface rather than a separate entity.

The generic model model includes the following **channels**:

- Channel A between the source and the PDC, is based on a short-range wired and/or wireless communication links. The Channel A might be implemented by a wireless biomedical sensor network.
- Channel B is a long-range wired or wireless communication link between the PDC and the HCIS. Channel B can be implemented in a trusted environment or possibly over untrusted public networks by external providers, e.g., GSM, GPRS, UMTS, WiMAX or PSTN networks.
- Channel D may be implemented as any type of communication link, possibly over a public network.
- Channel E may be an internal interface or a wired/wireless short-range communication link. Long-range communication between PDC and PDAU should be provided via the HCIS.
- Channel G is implemented as an internal interface in one of the components used to retrieve the patient identity.

C. Applying the Generic Model

The generic model is applied to the relevant scenarios in various ways, where the components and channels of the generic model can be implemented differently. Therefore, the threats might be different depending on the chosen scenario. The security requirements for Channel A are equal in all scenarios, and are therefore treated separately in the course of our work.

In a hospital scenario (Scenario 1) the PDC, PDAU, and HCIS might be part of an approved protected infrastructure and authenticated to each other, e.g., implemented by using a virtual LAN. In such an environment, Channel A needs specific attention regarding security. In different sub-scenarios the PDC might be implemented as a bedside terminal serving just one patient, or as a base station that might serve an entire hospital corridor. The threats affecting the patient monitoring system differ for these cases.

For a nursing and citizen homes scenario (Scenario 2) most channels might be outside the protected infrastructure of a hospital. Channels B, D, and E are implemented various short- and long-range technologies, possibly using third party providers like telecommunication providers. The PDC might be implemented in connection with a set-top box in the patient's home.

For a paramedic scenario (Scenario 3) the PDC might be implemented in an ambulance, serving one or several patients. Channels B and D might be non-existent or implemented by the means of a long distance communication possibly using third party providers. Channel E is implemented in most cases using a short-range scenario. The paramedic scenario has the most stringent requirements, since emergency routines must be available, e.g., in case a sensor must be replaced or moved to another patient, or the patient's identity might be unknown.

Common for all scenarios is that Channel A is implemented by the means of a WSN, the placement of the sensors is done under the responsibility of authorised personnel using approved routines, and that channels which are not part of a protected environment are secured properly. Whether the PDC handles one or several patients might have an impact on threats, but the architecture should be able to address these.

D. Implementation of Selected Communication Channels

The channels in the generic system model can be implemented in a variety of communication technologies. When not within a trusted infrastructure, these channels must be protected. A threat analysis gives answers on what to protect, and possible countermeasures to specific threats, for instance by the use of virtual private networks (VPN). Since securing the single technologies against these threats will not result in a uniform architecture, we advocate for handling most threats in the application layer.

For long-distance communication public networks based on different technologies (GSM, SMS, GPRS, UMTS, WiMAX, etc.) are used, which includes the transfer of data through the networks of external providers. Since it is not allowed to transfer medical and sensitive data unsecured, measures must be taken to protect these data, e.g., by using a VPN, securing the application layer, or other means [6]. Here, the Channels B or D are considered as long-distance communication channels.

The Bluetooth technology is emerging as communication technology for parts of the wireless infrastructure for short-range communication, designed to facilitate communication without the need of wires. In our scenarios (parts of) the Channels A, B, D, and E can be implemented using Bluetooth, using a point-to-point connection.

E. Biomedical Sensor Networks

Biomedical sensor networks [11], [20] can be a part of a patient monitoring system, located as source, (parts of) Channel A, and possibly the PDC. BSNs comprise of one

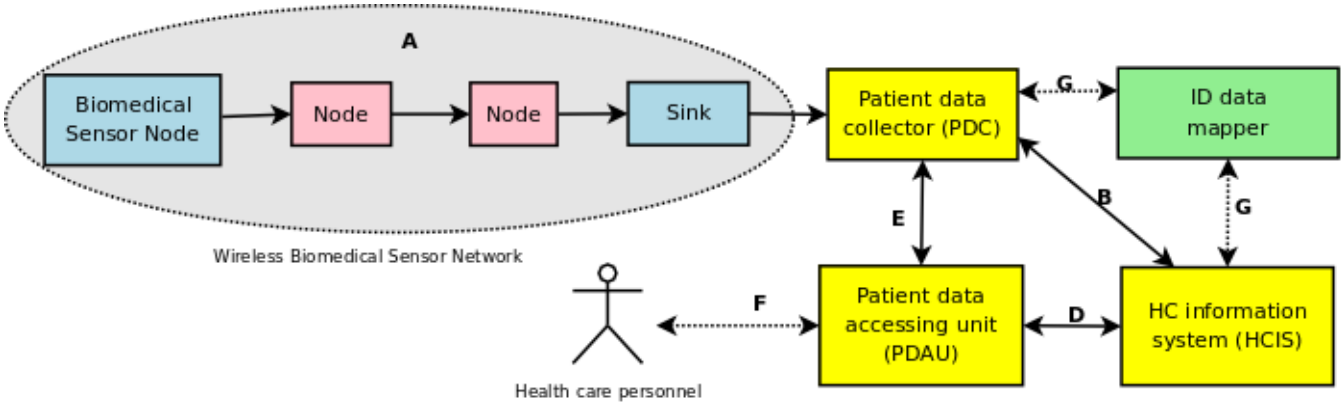

Fig. 1. Generic system model with Channel A shown in detail.

or several sensor nodes, possibly several *transfer nodes*, and one or more sink nodes which are attached to the PDC.

A biomedical sensor node is an electronic device which performs the tasks of sensing, processing, sending, and/or receiving biomedical data. The sensor node can be decomposed into four abstract parts: sensor, receiver, processing unit, and transmitter. Technically, a sensor node is built up of an MCU or CPU, memory, a wireless communication device, biomedical sensors, and a power supply often based on a battery. The functionality of a biomedical sensor node is controlled by software, usually consisting of firmware, operating system, and specific application software for treating the biomedical signals and their transfer.

An extensive list of constraints that apply to sensor networks have been given in a report by DARPA [23], classified as (a) sensor node constraints and (b) networking constraints. Many of these constraints, like small memory resources, imposes limitations to the implementation of traditional security mechanisms on sensors. However, not all of these constraints apply to the special case of a *biomedical* sensor network. In particular the unattended operation constraint does usually not apply, since the sensors will be attached to patients that are conscious or supervised by health care personnel.

As shown in Fig. 1 a BSN also can contain transfer nodes that forward the medical data from the source to the PDC. These transfer nodes are used to enlarge the distance for reaching the PDC even for sensor nodes that cannot reach the PDC directly. This is especially important for devices that have little battery capacity, and thus limited transmission power.

Despite of the scarce resources of the sensor nodes, lightweight implementations for encryption of data have been developed, e.g., Sizzle [24].

IV. Security Assumptions and Requirements

Generally, from the requirements and the nature of the application or system, an analysis results in a list of threats. These threats are then analysed, and countermeasures and recommendations will then be used in the design, implementation, and deployment of systems. For the various parts of a complex system like a patient monitoring system we analyse the characteristics of the components and channels in the generic system model, before considering security aspects of the entire model. Presenting the identification of security aspects to wireless patient monitoring systems, it is customary to take into account the different abstraction levels [20], such as the stakeholder level, the application level, the communication level, and the technical level. While we recognise that it is important to analyse all levels in a health care enterprise, we concentrate on the technical aspects in the application and communication levels.

A. Security Requirements for Patient Monitoring Systems

For a patient monitoring system the security goals are (a) *availability*, the intended receiver are able to read the data; (b) *data confidentiality*, only the intended receiver are able to read the data; (c) *data integrity*, the received data has not been tampered with or destroyed, and violations of this must be detectable; and (d) *data authenticity*, the sensor data are linked to the correct patient. Note that linking data to the wrong patient could lead to wrong diagnosis and eventually mistreating the patient, and we do not consider safety requirements, like radiation, or other physical effects having an impact on the patient.

For those parts of a patient monitoring system that communicate within a trusted environment, we consider all technical security requirements to be fulfilled, since the regulations for the use of ICT systems in health care enterprises require this to be approved. For channels or components outside a trusted environment, we consider the Dolev-Yao threat model [25], where the attacker can overhear, intercept, and synthesise any message, and is only limited by the constraints of the cryptographic methods used. For certain use cases we consider a selection of components to be trusted, i.e., we assume that such components are not compromised. Also certain channels, e.g., those within a protected infrastructure within a health care enterprise are considered to be secure.

For all channels, personally identifiable patient data shall be protected from eavesdropping and unauthorised modifications

when transmitted across open networks, in order to provide confidentiality and integrity. Additionally, Channels D and E shall authenticate the user; Channel D shall additionally authenticate the HCIS, and Channel E shall authenticate the PDC. All components that handle unencrypted data must deny unauthorised access of any kind, such as viewing, insertion, transformation, deletion of patient data.

The HCIS as a part of the hospital infrastructure shall (1) verify the integrity of patient data, (2) authenticate the PDC, (3) know the identity of the patient, (4) know to whom the patient data pertain, and (5) know the type of source used to produce the patient data. The PDAU shall in addition to the requirements for all components verify the integrity of the patient data.

For all components where emergency access functionality is available, the invocation of emergency access shall override the restriction on read access. For all components, except the source, an emergency access shall trigger extended monitoring of relevant events to enable the detection of unnecessary access.

B. Security Requirements for BSN

Related to the generic system model the wireless BSN is a specific implementation of Channel A. The characteristics of Channel A include that the signals are not limited to a controlled area or device, and hence are accessible to anybody in the proximity with the appropriate equipment. Authentication and measures against eavesdropping are therefore a necessity.

While security measures for BSN must be available at all communication layers most of the security requirements can be handled on the presentation layer. However, some issues, e.g., tied to routing and consequently refer to the requirement of availability, are better handled at the network layer. We refer to the layer model shown in Fig. 2 where the security measures are placed in the presentation layer.

Using the Dolev-Yao threat model [25] to analyse a BSN we consider the source, and the sink to be trusted, while Channel A, including possible transport nodes could be in the control of the attacker. The possible intrusion by an Dolev-Yao attacker implies that the existence of transfer nodes must be considered, also in a one-hop environment. A potential attacker could provide an extra node without anybody knowing about it, often denoted as “man in the middle” or proxy attack. The use of time and distance bounding protocols [26] on the network level can counter such threats.

The existence of fake nodes must be considered, why authentication of sensors must be mandatory, so that data sent from a sensor are not disclosed, and fake data are recognised.

Since the data source has limited storage it shall not store data longer than necessary. Due to limited battery capacity unnecessary communication, both sending and receiving, shall be avoided.

Even if the sensor data are encrypted, the sensor encryption is lightweight and can be broken given sufficient time and resources. Hence, the data sent from the sensor to the PDC should not contain person-identifiable data such as a social security number. Instead, the sensor data should be linked to the corresponding person in the PDC, by using the ID-data mapper. Person-identifiable data may be included at the PDC, since it has more resources available, and can implement stronger encryption algorithms and longer keys than an ordinary sensor node.

An adversary shall not be able to inject data packets without these being detected. Re-played data packets must be detected to ensure data freshness. Since characteristics of routing and forwarding make it necessary to detect duplicate arriving packets the the network layer or above must offer detection mechanisms using counters or other identifying data.

On the network layer attacks to WSN, and BSN in particular, include attacks to routing and forwarding. On the upper network layers such attacks are recognisable by missing, defect, manipulated, duplicated, or delayed packets. While these attacks can be detected they cannot be prevented on the presentation layer.

We assume that deploying a sensor, key establishment, assigning an identity to a sensor, and coupling the sensor node to a patient identity is done in a routine ahead of the normal operation of the sensor network; trusted medical personnel performs this operation, e.g., by coupling the sink and the sensor node.

The sink node has rather large computation and communication properties in order to perform data aggregation, validity check, identity assignment, etc. Transfer nodes are not supposed to perform these tasks, and hence do not need keys to decrypt sensor data.

Any form of data aggregation on transfer nodes should be avoided by two reasons: (1) data aggregation on these nodes would need extra resources; and (2) data aggregation would make it necessary that data are decrypted unless privacy transformations [27] are employed. For aggregation in the transfer nodes the key distribution problem would be much more complex. Therefore, we do not foresee data aggregation mechanisms within Channel A.

In contrast to a general wireless sensor, the biomedical sensors are in a rather controlled environment, so that we do not consider destruction or tampering with the sensors. Compromise of a sensors key does not affect the rest of the network, since its key is shared only with the sink node.

Communication on Channel A shall be short-range, while the transmitted data shall be protected from eavesdropping. Integrity protection of the transmitted data is necessary, since interferences from other medical instruments are possible. Automatic roaming to other PDCs shall not be allowed.

The PDC shall in addition to the requirements for all components: (1) verify the correct identity of the source, (2) not modify the patient data, except for aggregation or other defined transformations, and (3) not store data longer than necessary to ensure successful transmission of patient data to the HCIS.

To provide flexibility we must consider security challenges for software upgrades via the wireless network, reconfiguration, self-organisation, and device-mobility (e.g.,

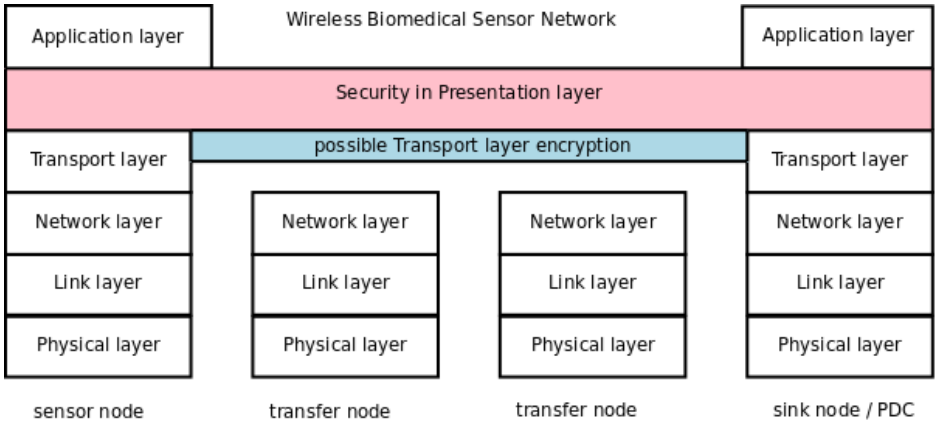

Fig. 2. Layer model for BSN.

handovers on different layers). Configuration control (e.g., check whether versions of hardware and software fit together, verify whether the patient is in the correct situation) shall be employed.

Aspects of availability are often neglected, which include scalability, quality of service (QoS), and power consumption. A power outage of a sensor may compromise the availability of data and thus threaten the patient. QoS includes mechanisms to provide an agreed service level regarding parameters such as network bandwidth, data throughput, signal quality, response time, latency, packet delivery rate, jitter, and power consumption. In complex communication environments, mechanisms should be employed to mitigate interference from co-existing wireless networks and various medical applications, which requires robust error detection and correction algorithms in packet transmission procedures.

V. Threat Assessment of Patient Monitoring Systems

The general threats and attacks to these security objectives are eavesdropping, denial of service, masquerading, and disclosure. For the components the threats and associated factors include (1) compromised or fake components (physical or logical attack), (2) destroyed, malfunctioning, lost, or stolen component, (3) software errors (e.g., failure in security mechanisms, routing, etc.), (4) misuse of emergency access, and (5) denial of service attacks (physical or logical attacks, bad quality, accidents, etc.). For the channels threats include: (6) compromised or fake (components of) communication infrastructure (physical or logical attack), (7) unstable communication infrastructure (physical or logical attack, bad quality, accidents), and (8) eavesdropping of communication. These threats and vulnerabilities may lead to the unwanted consequences that information or equipment might be unavailable, incorrect information is received (medical data, patient identity, sensor type, etc.), sensitive information is leaked, and eventually damage to the patient, operators or equipment.

Many of the security mechanisms of the generic system model employed as countermeasures are distributed over several components. These components include (1) the key generation service for session keys; (2) security protocols that support authentication, confidentiality, integrity, key establishment, and the associated cryptographic algorithms; (3) signature generation and verification services, along with a local storage for credentials and keys; (4) access enforcement services for both users and system components; (5) the log collector to collect metadata about events; and (6) front-ends for various services, such as security administration and authentication.

An architecture for patient monitoring systems must address patient identification and identity management of patients, devices and personnel. Other elements include device administration (which requires key management), user administration, authorisation policy, mandatory encryption for data stored on mobile devices, communication encryption, communication and data source authentication, data manipulation detection, and logging of critical events [28].

A. Vulnerabilities in Communication Channels

For short- and long-range communication the channels not residing in the secure enterprise infrastructure include wireless short-range, wired and wireless long-range communication. When security mechanisms are not offered, e.g., when using a channel over a public network, presentation or application layer mechanisms must be employed, e.g., using authentication and encryption mechanisms offered by the protocols of the appropriate layer.

Bluetooth, which often is used for short-range communication, employs rather weak encryption based on the assumption that the communication is short-range. However, this argument may be questionable since well equipped attackers using signal amplification and directional antennae can enlarge the communication range substantially. Also the fact that the Bluetooth devices often are very mobile and can contact many other Bluetooth devices short-range while passing by, is a substantial threat.

The sole secret credential in a Bluetooth network is the PIN code of the device. While weaknesses in the cryptographic

protocol can be neglected, there are different implementation weaknesses for the equipment of some vendors. When these are exploited, devices and sessions can be taken over by an intruder [29].

Since communication over SMS is not reliable, the use of IP over GPRS, EDGE, 3G, or similar technologies is recommended. An encryption scheme and intruder detection must be employed in order to provide privacy. Note that the risks for attacks are different whether an attack affects one patient or many patients. While there are several PKI solutions available, the use of keys stored in the SIM cards reflects the security needs for mobile patient monitoring systems.

B. Threats Affecting BSNs

The general threats for biomedical sensor networks can be characterised into the following domains: (1) the entity domain, (2) the network domain, (3) the routing and forwarding domain, and (4) the specific protocol domain.

Any adversary can eavesdrop on the traffic, inject new messages, replay or change previous messages. The biomedical sensors do not trust each other; while each sensor node trusts itself. Base stations (gateways) are assumed not to be compromised. However, compromising them could render the entire sensor network useless. Thus the base stations are a necessary part of the trusted computing base, and all sensor nodes trust the base station.

A sensor network should be both preventive and resilient to severe types of attacks regarding both control traffic and data traffic. Typical examples of control traffic are routing, monitoring whether a node is awake, asleep, or dead, topology discovery, and distributed location determination. Control traffic attacks include blackhole attacks, wormhole attacks [30], rushing attacks [31], sybil attacks and compromised sensors [32], [33], sinkhole attacks [34], and HELLO flood attacks [34]. Control attacks are especially dangerous because they can be used to subvert the functionality of the routing protocol and create opportunities for a malicious node to launch data traffic attacks such as dropping all or a selective subset of data packets. A sensor network should be both preventive and resilient to severe type of attacks such as wormhole attack, the Sybil attack, and compromised sensors [35].

While secure routing ensures that data are forwarded to the correct recipient, it does not include confidentiality and protection against replay attacks. This is caused by underlying spoofed, altered or replayed routing information, selective forwarding, acknowledgement spoofing, and the attacks mentioned above.

At the sensor node domain, an attack could change settings in a sensor or transmitter unit, its software or data, resulting in a threat. Consequences might be exposure to increased heating or radiation from the device. The general attacks by a malicious entity can therefore be classified as fake emergency warnings, prevention of legitimate warnings from being reported, battery power depletion, excessive heating in the tissue of the patient, and radiation from the entity.

Countermeasures to threats affecting a BSN are often specific to the employed communication technology, and thus security mechanisms should be implemented in communication layers below the transport layer [20]. Since BSN use technologies that are introduced in the market, the implementation of lower communication layer countermeasures are not always viable in a health care enterprise. However, countermeasures to avoid that attackers exploit weaknesses include link layer encryption and authentication using symmetric keys, the use of packet counters to avoid replay attacks, encryption, verification of identities, and various countermeasures on the link-layer [34].

In order to meet the challenges that the threats impose we propose that countermeasures are employed on the presentation layer, which are not specific to the underlying communication technology. Since not all threats on the lower layers can be prevented on the presentation layer, such as attacks to routing or denial of service, inconsistencies should be at least detectable at the application layers. Measures at the application layer to be taken should include encryption, measures for data integrity and authenticity.

For the sake of scalability, authorisation schemes must be role-based (as opposed to being individual-based). The authorisation database stores information about roles and their assigned privileges, which might be constrained by contextual information. Session keys are preferably generated during the authentication protocol, while confidentiality is established through encryption, and integrity is established through a signature generation service. Since the HCIS cannot authenticate all sources, such as biomedical sensors, these sources must be authenticated by a proxy, i.e., the PDC identifies the source, and guarantees its authenticity towards the HCIS.

Since broadcast channels are used in BSNs and energy consumption by the device is an issue, security mechanisms must be carefully designed. Some security mechanisms, such as encryption, use extra computing cycles and therefore consume extra energy. The broadcast of unnecessary data consumes extra energy at both the sender and the receiver nodes in a BSN. Wherever a sufficient security mechanism is offered at lower layers in the communication stack, these should be employed, since these are better fitted to the employed technology than higher level mechanisms. However, there should be a minimal set of mechanisms in the application level that protect the data.

While the relationship between the patient and the patient data must be given at all times, it is not recommended that data that identify the patient are transmitted over unsecured channels. Instead, the relationship between patient and patient data is achieved by authenticating the device or sensor.

VI. MPEG-21 in Patient Monitoring Systems

MPEG-21 is a general framework for handling multimedia, from the content provider to the end-user. It aspires to be a unifying framework in the media industry facilitating multimedia transactions, and to equip the content providers with a tool to restrict illicit use of copyrighted material. Given the

recent battles between copyright holders and people illegally sharing the copyrighted material, this is still an unresolved issue. Despite this, MPEG-21 is not only suited for enforcing copyright, it can also be used to protect the life cycle of patient data.

The vision of MPEG-21, defined in ISO/IEC 21000, is *to enable transparent and augmented use of multimedia resources across a wide range of networks and devices* [8]. Since medical data qualify as multimedia resources this vision suits well within a patient monitoring system with its wired and wireless networks, portable and stationary devices, and a variety of multimedia resources. MPEG-21 also provides means to protect the content, so that the desirable level of privacy can be achieved. While not all of the eighteen parts of MPEG-21 are suited for our purpose, the most relevant parts will be presented briefly in the following.

A. Relevant Parts of MPEG-21

The most fundamental concept in MPEG-21 is that of a digital item (DI), which is described in Part 2 of MPEG-21. The DI is a structured object, represented as an XML-description, that contains the multimedia resources (or references), and metadata that describe these resources. Attempts have been made to adapt the DI to the health care sector as medical digital item (MDI) [18].

To identify a DI, Part 3, Digital Item Identification (DII), offers a shell where users can choose their own relevant identifier regime, for example patient identity or sensor identity.

A protected form of the DI is provided by the intellectual property management and protection (IPMP) components in Part 4 of MPEG-21. Parts of a DI can be encrypted and digitally signed, and hence confidentiality, authenticity and integrity of patient data can be provided assuming that the system, including keys, protocols and algorithms, is secure. However, the specific tools to encrypt and sign are not provided by the standard, and must therefore be implemented by the application or middleware components.

Expressing the digital rights, i.e., the rights to access specific data under given circumstances, is governed by Parts 5 and 6 of MPEG-21, the rights expression language (REL) and the rights data dictionary (RDD), respectively. Combined with IPMP the usage of patient data can be restricted, e.g., by giving a specific nurse the permission to view a specific patient's blood pressure during a specified time interval.

In order to make the DIs available on networks and devices with different capabilities, and to users with different preferences in various environments, Part 7 of MPEG-21 defines the digital item adaptation (DIA). In this context a user can refer to a person, a group or an organisation. Adaptation can be useful in a health care environment, e.g, to give different views of the same data on terminals with different screen sizes and network bandwidths [19].

Transmitting the DI as a potentially large XML-representation is not convenient on a resource and bandwidth constrained network like BSN. To address this, MPEG-21 Part 16, entitled "MPEG-21 binary format", describes how to binary encode the XML representation in order to significantly reduce the bit rate [7], [36]. The technology for encoding the XML representation is provided by ISO/IEC 23001 Part 1, "Binary MPEG format for XML" or shortly BiM [37]. The BiM encoding is standardised in MPEG-7 [38], [39] and adapted for use in MPEG-21.

In general, MPEG-21 is agnostic to which concrete algorithms are used; the digital items only refer to the algorithms, and contain the respective payload. An evaluation of different cryptographic algorithms for the use in WSN has been carried out elsewhere [40].

B. Representing Medical Data with MPEG-21

The Digital Item defined by MPEG-21 has previously been adapted for use in the health care sector [19] as medical digital item (MDI). The MDI can contain both the biomedical data as defined in Section III-A, and the metadata. The metadata originating from the sensor node comprise of (1) the sensor id; (2) the stream id; (3) time stamps; (4) sequence numbers; (5) descriptive metadata, like sampling rates; and (6) encryption-related data.

To keep the amount of data processed and sent from the sensor nodes at a minimum we introduce the concept of the *lightweight MDI* for the sensor (μMDI) that solely contains the necessary biomedical data and corresponding metadata. For privacy reasons data that can identify the patient are not included in the μMDI. Except the sensor id, all these data are represented encrypted, and packaged efficiently using BiM before being sent to the PDC. An example of a very simple μMDI is given in Fig. 3.

C. Efficient Encoding of XML

As XML-representations of data are known to have a huge overhead, the use of the Binary MPEG format for XML (BiM) is a necessity for the resource constrained sensors, thus the sensors will only have to process and transfer a binary encoded version of the μMDI. The major properties of BiM include that it represents a schema oriented encoding method using a preparsed, typed binary format; it also allows different refresh rates of sub-parts of the XML document. BiM uses a tree representation of XML, where the tree nodes can be addressed, and operations containing the payload can be applied. A BiM-encoded template reduces the size of the XML-code by 90-95% [36].

On the source node the data are encoded by an automaton, which can be generated from the XML schema describing the μMDI that is used on this sensor node. On the PDC, the code to decode the μMDI is generated from the same XML schema. Transfer nodes and other sensor nodes are not aware of the MDI schema, since the content is not supposed to be processed there.

To further reduce the amount of transmitted data, not all metadata need to be included in every packet. This is possible since BiM allows different refresh rates of the XML document. Descriptive metadata, such as bitrate, could be sent out less often than critical metadata like time stamps, and stream id.

```
<DIDL xmlns="urn:mpeg:mpeg21:2002:02
-DIDL-NS" xmlns:dii="urn:mpeg:mpeg21:
2002:01-DII-NS">
 <Container id="test">
  <Item id="myitem">
   <Descriptor>
    <Statement mimeType="text/xml">
     <dii:Identifier>
      urn:grid:a1-abcde-9873216540-f
     </dii:Identifier>
    </Statement>
   </Descriptor>
   <Descriptor>
    <Statement mimeType="text/xml">
     <dii:Type>
      urn:sensor:bloodpressure
     </dii:Type>
    </Statement>
   </Descriptor>
  </Item>
  <Item id="bloodpressure">
   <Component id="systole">
    <Resource mimeType="text/plain">
     160
    </Resource>
   </Component>
   <Component id="diastole">
    <Resource mimeType="text/plain">
     80
    </Resource>
   </Component>
  </Item>
 </Container>
</DIDL>
```

Fig. 3. Example of a simple MDI for blood pressure in XML.

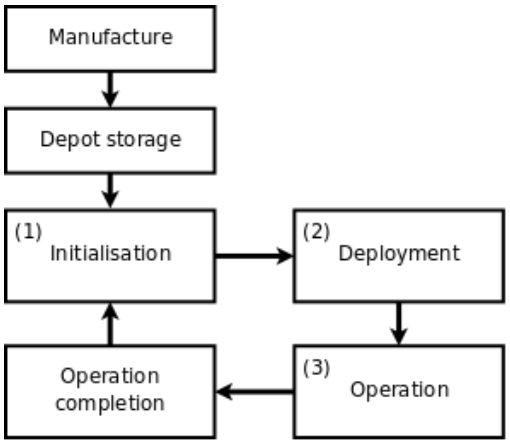

Fig. 4. Lifecycle of a biomedical sensor node (adapted from [23]).

VII. Proposed Architecture

Our architecture builds on the medical digital items (MDI) introduced in a health care environment for patient monitoring systems [18], and suggested for BSN [19]. Our architecture envisages that all medical data use the MDI in the presentation layer of all channels of the generic model. When used between all components this enables security and adaptivity of health

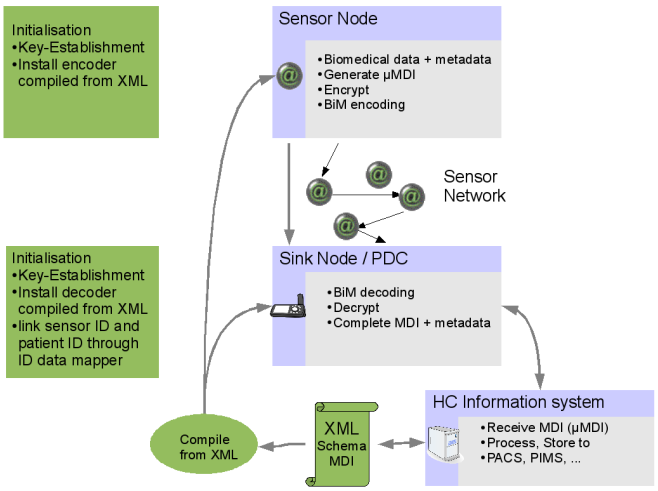

Fig. 5. Proposed architecture showing the initialisation and deployment phases (green) and operation phase (blue).

care data, including medical data and metadata. Generally, all medical data sent over the channels are encoded using the MDI schema, while the components use the tools defined by MPEG-21 to handle the medical data.

As outlined previously the properties of Channel A of the generic model require a refinement of the general architecture due to resource limitations and other properties of this channel. We will elaborate on how to implement our architecture for Channel A by the means of a BSN in the following.

Even though the BSN has limited resources we encode the biomedical data and the relevant metadata into MDI containers to transfer these from the sensor node to the PDC. Due to the resource constraints in BSN we use additionally BiM to reduce the data rate, and select carefully which portions of the medical data to transfer at which rate, and which data to protect.

Fig. 4 shows a diagram of the entire life cycle of a sensor node [23], which we have adapted to the health care area. We focus on the three phases that are numbered in this diagram, namely the initialisation, the deployment, and the operation of a sensor node.

For a more detailed view on these three phases, including the overall architecture and data flow, we refer to Fig. 5. During the initialisation phase the sensor nodes receive the appropriate software and keys in a secure manner shown in the green elements of this diagram. The initialisation is facilitated by installing software including the right credentials on the sensor node. This software is compiled from the XML schema to produce the μMDI efficiently. The sink-node receives the credentials and decoding-software accordingly, while there is no need to install extra software or credentials on the transfer nodes. The relationship between patient and sensor node is established in the deployment phase through the ID data mapper.

During the operation phase, denoted as the blue elements in

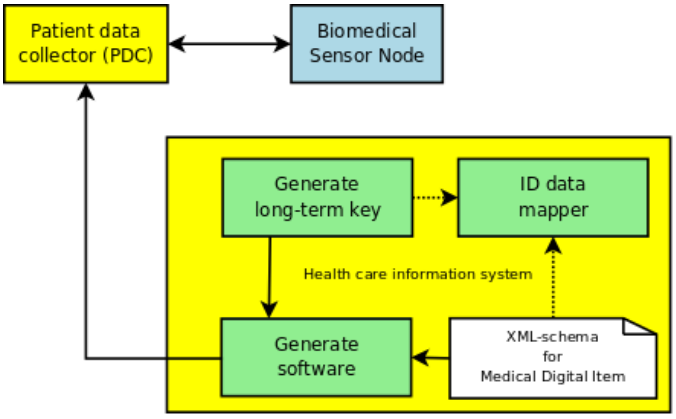

Fig. 6. Initialisation of a sensor node.

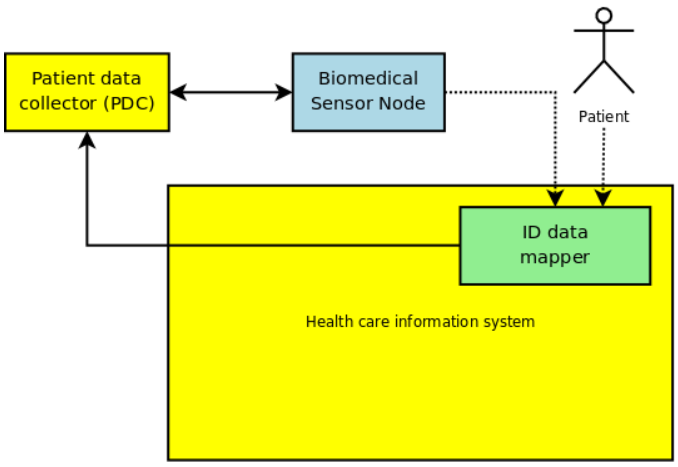

Fig. 7. Deployment of a sensor node.

Fig. 5, the medical data and metadata are sent from the sensor nodes to the PDC, and further to the other channels. The data are produced in the sensor node and forwarded as μMDI to the sink node. There, the μMDI is completed to form a full MDI and forwarded to the HCIS and the PDAU.

A. Initialisation of Sensor Nodes

Prior to deployment of the sensor nodes, the initialisation phase performs the following tasks: (a) key-establishment; (b) installation of XML-generated code on the sensor nodes. Fig. 6 illustrates the initialisation.

Due to the limited computing resources on the sensors, we avoid the usage of public key algorithms, which is reflected also for the key-establishment [41]. We propose that each sensor and the PDC share a long-term, pair-wise, symmetric key that is used to establish session keys.

The long-term key has to be securely pre-distributed from the hospital infrastructure. This provides a challenge, since, on most sensors, the communication interface is wireless, and the pre-distribution will be broadcast for everyone to listen. As a countermeasure to eavesdropping, the key establishment could be performed using a special device, e.g., installed in a Faraday cage, which will shield the electromagnetic signals so that a potential eavesdropper is unable to intercept the long-term key. The long-term key is supposed to last the entire lifetime of a sensor, or until it is compromised or exchanged routinely to renew the keys. Hence the initialisation procedure does not have to be performed every time a sensor is deployed on a patient.

The pair-wise symmetric *session* key will then be established by using a key establishment protocol that utilises a pre-distributed symmetric key, such as Authenticated Key Exchange Protocol 2 (AKEP2) [42], [43]. Thus, a node will only be able to read messages encrypted by the PDC with their shared key, and not messages encrypted by other nodes. The PDC will be able to read messages encrypted by all nodes that have their keys securely stored in the PDC.

Due to the limited capabilities of the sensor nodes these are unsuited to handle the full complexity of encoding and parsing XML-documents. A more viable approach for BSN is to deploy software into the sensor nodes during the initialisation phase that is able to produce a μMDI from a template. More powerful devices without the constraints of sensor nodes, e.g., the PDC, will then receive and process these data using the full capabilities of XML.

B. Deployment of Sensor Nodes

In the deployment phase all identities are linked together within the ID data mapper. A schematic view on this phase is given in Fig. 7. The dotted lines indicate that the ID of the entity is sent to the ID data mapper. The PDC stores the sensor and stream identities and links them to the patient identity during deployment of the sensor. We distinguish between stream ID and sensor ID to support multi-sensors capable of handling several data streams simultaneously. Before attaching a sensor to a patient a manually initiated procedure assigns sensor and stream identities in order to identify each stream uniquely. By also including an examination identity, the patient identity and examination are linked to the sensor and streams. This information is resident in the PDC, and is communicated to the hospital infrastructure via an MDI.

C. Operation of Sensor Nodes

During the operation of a sensor node the following workflow takes place: (1) *Measurement*, the sensor measures biomedical data from a patient, (2) *packaging*, the biomedical data and the associated metadata are encrypted, encoded, packaged and signed in the μMDI template, and finally, (3) *sending*, the μMDI is sent to the PDC.

Steps (2) and (3) are illustrated in Fig. 8. The encryption in Step (2) uses a symmetric session-key that is shared only between the originating sensor and the PDC. This secured μMDI is then binary encoded using BiM. The sensor node sends the encrypted, encoded and signed version to the PDC, possibly via transfer nodes which will not be able to learn any of the contents since these are not in the possession of the decryption key.

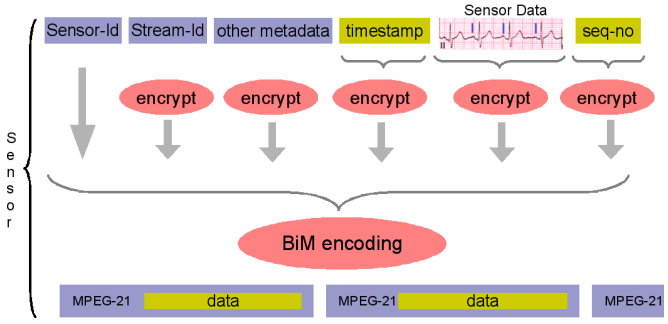

Fig. 8. Operational phase of the sensor node. Biomedical and metadata are encrypted, encoded and packaged into a μMDI.

After the μMDI arrives at the PDC it is decoded, decrypted and the signature is verified. The content of the μMDI, all relevant context information, such as references to the XML-schema in use, and patient data are then aggregated to produce a full MDI. This MDI might also include data from other sources about the same patient, before being sent further along the channels described in the generic system model.

VIII. Discussion

Our framework uses an international and open multimedia standard for end-to-end content management to meet the security goals of data confidentiality and integrity of medical data in patient monitoring systems using a BSN. An important argument for our choices is to use MPEG-21 as a mechanism in the entire work flow of the health care information system. However, due to the resource restrictions in BSN we need to show that the use of MPEG-21 is viable, and to what extent our architecture meets the security requirements stated previously.

A. Security

The security mechanisms proposed in our architecture are applied on the presentation layer, and address integrity and confidentiality requirements. Threats on the network layer or below, such as routing attacks, denial of service attacks or hardware failures are not addressed, nor are attacks on cryptographic primitives, since we assume the Dolev-Yao attacker model. Further, we cannot exclude that an attacker might receive a limited amount of information from the existence of messages and additional knowledge that the attacker might have from the context or from access to the patient. Additionally, message rate, message size and sensor frequency might reveal confidential information. Therefore, measures to achieve 'transactional confidentiality' [44] must also be considered.

We claim that the use of MPEG-21 can protect against confidentiality threats, such as eavesdropping the original medical data, by encryption using a symmetric key. Since the key establishment is performed using physical security measures the medical data and most of the metadata remain as secure as the employed cryptographic method permits, and the keys are not compromised.

Since the strength of the employed cryptographic methods is limited due to the resource limitations of the sensor nodes, the μMDI does not contain data which directly identify the patient. Note that this is in contrast to frameworks that do not consider the use of BSN explicitly [22], where the patient ID is not even protected.

To address the integrity of the medical data and metadata the MDI is protected by an encrypted hash value, as employed in MPEG-21 IPMP. This and the use of sequence numbers for packets enable the detection of injected, re-played, deleted or modified data packets. Altering and injection of messages would be detected since the Dolev-Yao-attacker would not be able to correctly sign messages.

B. Encryption Scheme

The encryption methods as such are not part of MPEG-21. In principle, all schemes and implementations can be used in combination with MPEG-21. However, encryption schemes are a vital part of the protection of medical data and metadata. The use of symmetric keys, rather that public/private key pairs, can inflict potential issues of authentication, key-distribution and key-management [45]. However, we argue that our proposed scheme resolves these issues since, in contrast to general WSN, both initialisation and deployment are performed in a physically controlled environment by humans.

Pair-wise symmetric key pairs allow data source authentication. Since each sensor only needs to store one key, the memory requirements on the sensor are limited to the key-size. On the PDC the memory requirements are proportional to the number of sensors that are connected to it. Assuming a symmetric key-size of 128 bits, 20 patients with 25 nodes each, the key storage will require around 8 kB on the PDC. Even if the pre-distributed keys might be used for a long time, and be subject to cryptanalysis by an adversary, a brute-force attack is considered to be infeasible on keys with 128 bits.

C. Suitability for BSN

Since the sensor nodes are resource restricted the use of XML on the sensor nodes is not viable due to space constraints. Instead BiM-encoding is used. On the sensor nodes parsing of message content is avoided. As a consequence, XML is processed only outside the sensor nodes.

The software to BiM-encode the MDIs in the sensor node is generated outside the sensor node from XML schemas, and uploaded to the sensor node during the initialisation phase. This software is typically implemented as a rather simple automaton which has a small fingerprint. Since the μMDI structure is constant while operating a sensor node, a bitstream binding language [36] which could provide a more flexible framework is not necessary.

Compared to sending the medical data and metadata in a fixed packet format with pre-defined fields we gain much flexibility with MPEG-21 to the cost of an overhead. Additionally to the payload the BiM-encoded messages contain path information which increases the packet length. Benchmarks show that we can expect a considerable overhead for the

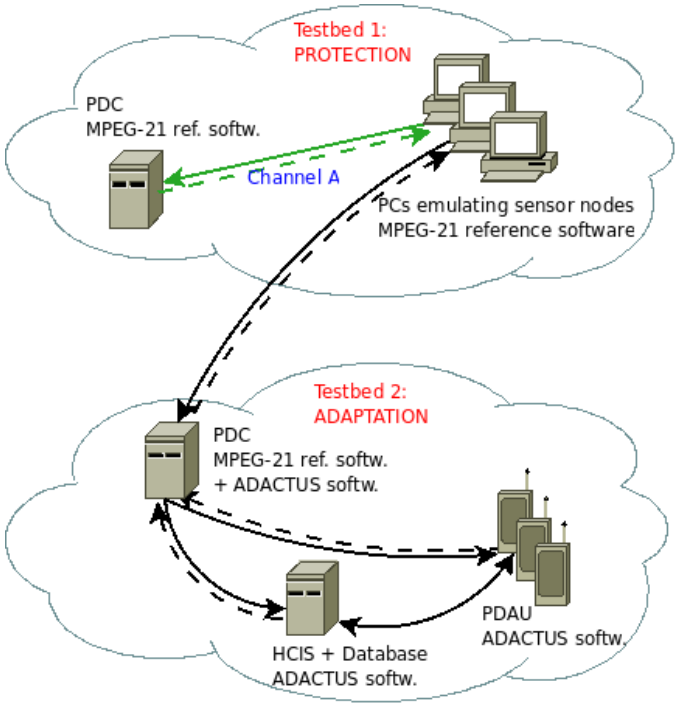

Fig. 9. Test bed for evaluating MPEG-21 for use in Patient Monitoring Systems and BSN.

general case [38]. Therefore the layout of the XML-tree to represent the μMDI has been carefully designed in order to minimise the overhead in the BiM-encoding. Also the ratio between payload, i.e., measured data, and the data necessary to secure the μMDI must be balanced.

D. Trust

Sensor nodes can fail by other means than communication, e.g., deliver bogus data, be misplaced on the body, etc. While our proposed framework does not protect against these threats, we recognise the importance of a sanity checks of data in health care applications. For proofs and adequate evidence about creator, creation, and historical process of data the term evidential value [46] is used. Methods to maintain the evidential value must be employed on devices that have enough capabilities to perform these operations. Our architecture architecture contributes to trust by using the measures of authentication, hash values and encryption as outlined in Section VIII-A. Other elements of the evidential value can be embedded in the μMDI when the sensor is able to provide these.

E. Evaluation Test Bed

To evaluate the different aspects of MPEG-21 we have developed a test bed shown in Fig. 9. This test bed consists of one part for evaluating properties of data protection and security, especially for Channel A; and of another part for evaluating properties of adaptation which is most relevant for presenting data at the PDAU. In Test Bed 1 we use parts of the reference software for MPEG-21 [47], and reference software for MPEG-7 [48] for BiM encoding running on PCs. In the Test Bed 2 we also employ software from ADACTUS [49] to evaluate adaptation issues which are beyond the scope of our paper. Both parts together implement a test bed that represents a patient monitoring system with all components and channels of the generic system model.

During our experiments with the test bed the reference software for MPEG-21 could be installed and used without greater obstacles, while the reference software for MPEG-7 BiM needed several XML files which were no longer available at their original locations. Both software packages use XML code that is partially incompatible, leading to the need of developing XML files that can be used in both reference software packages. We succeeded in encoding and decoding μMDI messages, and could confirm the estimates for the compression ratio using BiM as known from the literature [36].

Since the reference software for MPEG-7 BiM is demonstration software only, the production of a μMDI in our test bed is done via XML, instead of directly encoding the sensor data as outlined in Section VI-C.

IX. Conclusion and Future Work

We propose a framework for BSN that uses MPEG-21 for transmitting the biomedical data from sensor nodes to the hospital infrastructure. The tools within MPEG-21 have the capabilities of encrypting the patient data and assigning detailed rights to them. In addition, it is suitable for handling multimedia data on different devices and networks, which can be used to enhance the perceived quality of service (QoS) for a user. The proposed BiM-encoding technique facilitates a way to incorporate MPEG-21 resources in a resource-constrained BSN.

The scalability in terms of larger networks with many sensor nodes and user terminals, denoted as clients, can easily be handled in the application and presentation layers. Furthermore, implementation of our framework in the test bed and on real sensor nodes, with careful design of the μMDI will provide an efficient way of optimising wireless data transmission, data processing, power consumption, and memory usage in the sensor nodes with adequate security mechanisms. Incorporating Part 7 of MPEG-21 (DIA) into our security framework can be considered in future.

We anticipate a large scale testing of the proposed framework using the test bed described in Section VIII-E. The simulation of a BSN and evaluating packet size, overhead from the BiM encoding, and resource consumption will be useful prior to deploying such a system.

We also envisage the use of formal methods [50] as a proof of the correctness of our framework, its implementation and the employed security protocols. This includes the analysis of attacks on the BiM-encoded packets under given assumptions, authentication, and integrity of the medical data.

To study the impact of small footprint of the software to be deployed in the initialisation phase, an implementation on real sensor nodes (motes) can be considered. For generating the software code for the sensor nodes, a framework for code

generation [51] that allows generation of code from an abstract model to several potential sensor node types can be used. We are confident that simulations in the test bed, and the implementation of the framework on real BSN will open for a secure deployment of wireless technologies in health care applications.

ACKNOWLEDGEMENTS

This work is funded by the SAMPOS project in the VERDIKT programme of the Norwegian Research Council. We appreciate the help of Thomas Skjølberg and Peder Drege at ADACTUS. The authors wish to thank Habtamu Abie, Arne-Kristian Groven, and Lothar Fritsch for contributions and discussions in previous versions of this paper.

REFERENCES

[1] Wolfgang Leister, Truls Fretland, and Ilangko Balasingham. Use of MPEG-21 for security and authentication in biomedical sensor networks. *Proc. ICSNC'08, International Conference on Systems and Networks Communication*, 0:151–156, 2008.

[2] Integrating Healthcare Enterprise. http://www.ihe.net. Last accessed: May. 15, 2009.

[3] S.C. Chu. From component-based to service oriented software architecture for healthcare. In *Proc. 7th Annual International Workshop on Enterprise networking and Computing in Healthcare Industry, HEALTHCOM 2005*, pages 96–100, 2005.

[4] Eric Newcomer and Greg Lomow, editors. *Understanding SOA with Web Services*. Addison Wesley, 2005. ISBN 0-321-18086-0.

[5] Digital Imaging and Communications in Medicine (DICOM). http://medical.nema.org/dicom/, 2008. Last accessed May 15, 2009.

[6] Ilangko Balasingham, Halfdan Ihlen, Wolfgang Leister, Per Røe, and Eigil Samset. Communication of medical images, text, and messages in inter-enterprise systems: A case study in Norway. *IEEE Transactions on Information Technology in Biomedicine*, 11(1):7–13, 2007.

[7] I. Burnett, F. Pereira, R. van de Walle, and R. Koenen, editors. *The MPEG-21 Book*. John Wiley & Sons, 2006. ISBN 0-47001011-8.

[8] ISO/IEC TR 21000-1: 2004. information technology - multimedia framework (MPEG-21) - part 1: Vision, technologies and strategy, November 2004.

[9] The Government of Norway. Act of 18 may 2001 no. 24 on personal health data filing systems and the processing of personal health data (personal health data filing system act). Stortinget, 2002.

[10] Article 29 Data Protecting Working Party of Directive 95/46/EC. Working document on the processing of personal data relating to health in electronic health records (EHR), 2007. Adopted on 15 February 2007, European Commission, Directorate General Justice.

[11] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary. Wireless sensor network security: A survey. In Yang Xiao, editor, *Security in Distributed, Grid, and Pervasive Computing*, chapter 17. Auerbach Publications, CRC Press, 2006.

[12] H. Yang, H. Luo, S. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: Challenges and solutions. *IEEE Wireless Communications*, 11(1):38–47, 2004.

[13] R. Savola and J. Holappa. Self-measurements of the information security level in a monitoring system based on mobile ad hoc networks. In *Proc of the 3rd International Workshop in Wireless Security Technologies 2005 (IWWSXT'05)*, 2005.

[14] R.S.H. Istepanian, E. Jovanov, and Y.T. Zhang. Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity. *IEEE Transactions on Information Technology in Biomedicine*, 8(4):405–414, 2004.

[15] L Schwiebert, S.K.S. Gupta, and J. Weinmann. Research challenges in wireless networks of biomedical sensors. In *Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 2001.

[16] IEEE 802.15.6 Body Area Network. https://mentor.ieee.org/802.15/documents, 2009. Last accessed May 15, 2009.

[17] IEEE 1451.5 draft standard for a smart transducer interface for sensors and actuators - wireless communication protocols and transducer electronic data sheets (TEDS) formats, 2006. March 26, 2007.

[18] M. Landén. An MPEG-21 approach to creating the first multimedia electronic patient journal system. Master's thesis, NTNU, 2003.

[19] Arne Lie, Knut Grythe, and Ilangko Balasingham. On the use of the MPEG-21 framework in medical wireless sensor networks. In *Proc. of the IEEE 1st Int Symp on Applied Sciences in Biomedical and Communication Technologies (ISABEL)*, Aalborg, Denmark, 25.-28. October, 2008.

[20] W. Leister, H. Abie, A.-K. Groven, T. Fretland, and I. Balasingham. Threat assessment of wireless patient monitoring systems. In *Proc. ICTTA'08*, Damascus, Syria, 2008.

[21] Georg A Brox. MPEG-21 as an access control tool for the national health service care records service. *Journal of Telemedicine and Telecare*, 11 Suppl 1:23–5, 2005.

[22] Anastasios Fragopoulos, John Gialelis, and Dimitrios Serpanos. Security framework for pervasive healthcare architectures utilizing MPEG-21 IPMP components. *International Journal of Telemedicine and Applications*, 2009:1–9, 2009.

[23] D.W. Carman, P.S. Kruus, and B.J. Matt. Constraints and approaches for distributed sensor network security (Final). *DARPA Project report, (Cryptographic Technologies Group, Trusted Information System, NAI Labs), September*, 1, 2000.

[24] V. Gupta, M. Millard, S. Fung, Zhu Yu, N. Gura, H. Eberle, and S.C. Shantz. Sizzle: a standards-based end-to-end security architecture for the embedded internet. In *Third IEEE conf on Pervasive Computing and Communications, PerCom 2005*, pages 247–256, 2005.

[25] D. Dolev and A.C. Yao. On the security of public key protocols. In *Proc. of the IEEE 22nd Annual Symposium on Foundations of Computer Science*, pages 350–357, 1981.

[26] Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyán. Mobility helps security in ad hoc networks. In *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 46–56, New York, NY, USA, 2003. ACM.

[27] Stanley R. M. Oliveira and Osmar R. Zaïane. A privacy-preserving clustering approach toward secure and effective data analysis for business collaboration. *Computers & Security*, 26(1):81–93, 2007.

[28] R. Arnesen, J. Danielsson, J. Vestgården, and J. Ølnes. Wireless health and care security requirements. Research note DART/01/05, Norsk Regnesentral, 2004.

[29] Hans Jakob Rivertz. Bluetooth security. Research note DART/05/05, Norsk Regnesentral, 2005.

[30] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proc. INFOCOM 2003*, pages 1976–1986, 2003.

[31] Y. Hu, A. Perrig, and D. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proc. WISE 2003*, pages 30–40, 2003.

[32] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: Analysis and defenses. In *Proc. IPSN 2004*, pages 259–268, 2004.

[33] J. Douceur. The sybil attack. In *Proc. IPTPS 2002, LNCS Vol. 2429*, pages 251–260, 2002.

[34] C. Karlof and D. Wagner. Secure routing in sensor networks: Attacks and countermeasures. In *Proc. SNPA 2003*, pages 113–127, 2003.

[35] L. Lazos and R. Poovendran. Serloc: Secure range-independent localization for wireless sensor networks. In *ACM Workshop on Wireless Security*, 2004.

[36] J. Thomas-Kerr, I. Burnett, and P. Ciufo. Bitstream binding language - mapping XML multimedia containers into streams. In *IEEE International conference on Multimedia and Expo, 2005, ICME 2005*, pages 626–629, 2005.

[37] P. de Cuetos, C. Seyrat, and C. Thienot. BiM white paper. http://www.chiariglione.org/mpeg/technologies/mpb-bim/index.htm, January 2006. Last accessed May 15, 2009.

[38] U. Niedermeier, J. Heuer, A. Hutter, W. Stechele, and A. Kaup. An MPEG-7 tool for compression and streaming of XML data. In *Proc. 2002 IEEE Intl. Conf. on Multimedia and Expo*, pages 521–524, 2002.

[39] S. Devillers, C. Timmerer, J. Heuer, and H. Hellwagner. Bitstream syntax description-based adaptation in streaming and constrained environments. *IEEE Transactions on Multimedia*, 7(3):463–470, June 2005.

[40] R. Roman, C. Alcaraz, and J. Lopez. A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. *Mobile Networks and Applications*, 12(4):231–244, 2007.

[41] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler. Spins: Security protocols for sensor networks. *Wireless Networks*, 8:521–534, 2002.

[42] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2001.

[43] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In *CRYPTO '93: Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, pages 232–249, New York, NY, USA, 1994. Springer-Verlag New York.

[44] S. Pai, S. Bermudez, S.B. Wicker, M. Meingast, T. Roosta, S. Sastry, and D.K. Mulligan. Transactional confidentiality in sensor networks. *Security & Privacy, IEEE*, 6(4):28–35, 2008.

[45] Chieh-Yih Wan, Mark Yarvis, and Jens Mache. Lightweight key distribution for sensor networks. http://www.freshpatents.com/Lightweight-key-distribution-and-management-method-for-sensor-networks-dt20081127ptan20080292105.php. Last accessed: May. 15, 2009.

[46] Jianquiang Ma, Habtamu Abie, and Torbjørn Skramstad. Preservation of trust and security in long-term record management. In *Proc. 6th Annual Conference on Privacy, PST2008, Security and Trust, Graduate Student Symposium, Fredericton, New Brunswick, Canada*, 2008.

[47] ISO/IEC 21000-8: 2008. information technology - multimedia framework (MPEG-21) - part 8: Reference software, 2008.

[48] ISO/IEC 15938-6: 2003. information technology - multimedia content description interface (MPEG-7) - part 8: Reference software, 2003.

[49] ADACTUS. http://adactus.no, 2009. Last accessed May 15, 2009.

[50] Anders Moen Hagalisletto, Lars Strand, Wolfgang Leister, and Arne-Kristian Groven. Analysing protocol implementations. In Feng Bao, Hui Li, and Guilin Wang, editors, *ISPEC*, volume 5451 of *Lecture Notes in Computer Science*, pages 171–182. Springer, 2009.

[51] M.M.R. Mozumdar, F. Gregoretti, L. Lavagno, L. Vanzago, and S. Olivieri. A framework for modeling, simulation and automatic code generation of sensor network application. In *Proc. 5th Annual IEEE Communication Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON'08*, pages 515–522, 2008.