Secure Data Transmission Protocol for Medical Wireless Sensor Networks

Soufiene Ben Othman
UR PRINCE, ISITcom, Hammam Sousse
University of Sousse, Tunisia
Email: ben_oth_soufiene@yahoo.fr

Abdullah Ali Bahattab
Computer Technology Department
College of Telecom & Electronics
Jeddah, Saudi Arabia
Email: abahattab@yahoo.com

Abdelbasset Trad, Habib Youssef
UR PRINCE, ISITcom, Hammam Sousse
University of Sousse, Tunisia
Email: trad.abdelbasset@gmail.com

Abstract—Wireless Sensor Networks (WSN) have attracted much interest in the last decade. It opened a new range of applications such as large area monitoring including environmental monitoring, wildlife exploration, and real time patient medical data which is collected by using wireless sensors. The WSN provides the options of flexibilities and cost saving for patients and healthcare industries. At the same time, there is a growing concern about the hospitals’ ability to provide effective care during disaster events. For these reasons, tools that automate patient monitoring have the potential to greatly improve efficiency and quality of health care. In hospitals, medical data sensors which monitor patients produce an increasingly large volume of real-time data. The transmission of this data through wireless networks in a hospital becomes a crucial problem because the medical information of an individual is highly sensitive. It must be kept private and secure. The purpose of this paper is to present our initial effort in building a flexible strategy to achieve secure data transmission in medical wireless sensor networks.

Keywords—component; Medical Wireless Sensor Network (MWSN); Healthcare; Security; Data Transmission; Hospital.

I. INTRODUCTION

Wireless Sensor Networks are systems composed of sensing elements embedded with wireless communication ability and a variable part of autonomy. These wirelessly connected sensor networks are often given functionality such as data collection to the gateway nodes which are known as sink points, sensor heterogeneity, or even actuation abilities [1]. One can employ a WSN to detect intrusions in a specific area, and trigger adapted alarm systems or even take countermeasures. The same technology can be used for monitoring a patient’s vitals to alert a medical crew when something goes out of chart such as an abnormal pulse rate. Thus, WSN is a new basis for emerging products and applications. However, there is not a single solution for all applications, but rather a framework serving as a starting point for developing application specific solutions [2]. Also, a multitude of sensor measurements and actuator control is possible with the WSN. A full-scale pilot deployment is extensively experimented to show the performance results. Currently, the pilot network is in use at the hospital.

Current health care systems are structured and optimized for reacting to crisis and managing illness because they are facing new challenges: a rapidly growing population of elderly and rising health care spending. Restructuring healthcare systems toward proactive managing of wellness rather than illness emerge as the answers to these problems. Wearable systems for continuous health monitoring are the key technology in helping the transition to more proactive and affordable healthcare [3].

One promising application is the area of health care and patient monitoring [3]. The integration of sensing and usage of technologies in consumer’s electronics would allow people to be constantly monitored. One important benefit is to help stem rising health care costs by increasing health observability and doctor-to-patient efficiency. Moreover, constant monitoring will increase early detection of adverse conditions and diseases for patients at risk, potentially saving more lives. This ability is right around the corner and its beginning will be ushered in with incremental integration of wireless sensor networks and consumer’s electronics [4].

Security is a vital aspect in WSN applications [6]. The implementation of security policies is a complex and a challenging issue because of constrained nodes resource. Short distance transmission reduces some of the security threats, but still there are risks, for example, in spoofing, message altering and replaying, flooding, and wormhole attacks [7]. Therefore, it is important to consider security solutions that guarantee data authenticity, freshness, replay protection, integrity, and confidentiality.

In healthcare applications for wireless sensor networks, security issues have been always part of active research. Also security issues in general wireless sensor networks are a major area of research in recent times. Some researches such as [5, 6, 7, and 9] and others [10, 11, 12, 14, and 15] have specifically addressed security issues with respect to healthcare applications.

For the hospital security, WSN user requirements are wireless devices with room-level localization, reliable low-latency alarming, long lifetime network, and ease of installation and maintenance.

- **Wireless Devices with Room-Level Localization.** The wireless sensors are continuously carried by the hospital personnel. This requires fully wireless small devices operating with small batteries. The sensors should respond as quickly as possible by a security guard
and other personnel on-site. Thus, the sensors devices should be localized within rooms.

- **Long Lifetime Network.** For easy maintenance, the network should have long lifetime for years. This includes all devices in the network whether they are mobile or static.

- **Ease of Installation and Maintenance.** The network can be installed and used in many locations. Thus, it should be possible to be installed and maintained by the personnel on-site without the need of rigorous guidance for the network operation.

In this paper, we present a novel design called hospital WSN security. With this hospital WSN security, we identify the requirements of data security in Medical Wireless Sensor Networks (MWSNs). In particular, we point out the necessity of secure data transmission.

The rest of this paper is organized as follows. In Section 2, we give an overview of some related works. Section 3 describes the proposed architecture while in section 4, we describe our proposed protocol. We discuss the results of security performance analysis in section 5 and section 6. Finally, Section 7 ends up with final considerations and future works.

II. **RELATED WORK**

In healthcare applications for sensor networks, security issues have been always part of active research. Security issues in general wireless sensor networks are a major area of research in recent times. Some works such as [5, 6, 7, and 9], and others like [11, 12, 14, and 15] have specifically addressed security issues with respect to healthcare applications.

TinySec is proposed in [16] as a security solution in biomedical sensor network to achieve link-layer encryption and data authentication. TinySec [17] is a software based security architecture that implements link-layer encryption. It is a component of the official TinyOS release. TinySec is very popular in the wireless sensor community and even it has been implemented on a variety of custom hardware. TinySec encrypts the data packet with a group key which is common to the sensor nodes and computes a message authentication code (MAC) for the entire packet including the header. This group key is shared network-wide and manually programmed into the nodes prior to deployment. This network-wide key presents a single point of vulnerability. TinySec does not protect against node capture. If a node is compromised and its key material revealed, the entire network can be compromised. However, in the case of WBAN, we proposed that node capture is not as easy as it may be in traditional wireless sensor network where nodes may be left unattended for long period of times. In WBAN, nodes are either on or implanted in the body, hence, node capture will mean a compromise of physical security.

Instead of using software encryption as the case in TinySec, hardware encryption can be implemented utilizing the ChipCon 2420 ZigBee compliant radio frequency (RF) Transceiver. The CC2420 is able to execute IEEE 802.15.4 security operations with AES encryption using 128-bit keys. These operations include the counter (CTR) mode encryption and decryption, CBC-MAC authentication, and CCM encryption plus authentication [18].

Hardware encryption has been implemented in a WBAN project with off-the-shelf ZigBee platform [19]. In this project, it was determined that the hardware encryption does not significantly increase power consumption in the sensor platform. This was attributed to the efficient on-chip hardware support for encryption in the wireless controller and the dominant power consumption of the RF unit when compared to the processing circuitry. However, the drawback of this method is that it is dependent on the specific sensor platform. Not all sensor nodes hardware offer hardware encryption support.

Elliptic curve cryptography (ECC) has emerged as a viable option for public key cryptography in wireless sensor networks. The main reason for this is its comparatively fast computation, small key size, and compact signatures. There have been several noteworthy contributions in the past few years. One of the earliest works utilizing ECC in sensor networks was done by Malan et al. [20]. In this work, a public key infrastructure, using ECC, was implemented and evaluated on a Mica2 sensor mote platform supported by TinyOS. Uhsadel et al. [21] proposed an efficient implementation of ECC. Recently, Szczepaniak et al. proposed NanoECC [22], which executes comparatively faster than existing ECC implementations but typically requires significant amount of ROM and RAM.

Although ECC has been successfully implemented in several variations, it is still not the top choice for WBAN. This is because its energy requirements are still significantly higher than symmetric systems. This being the case, others have proposed that ECC can be implemented only for infrequent and security-sensitive operations such as a key establishment during the initial setup of the network or code updates. In line with this thinking, Malasri et al. [23] proposed a solution for medical wireless sensor networks that uses: (i) an ECC-based secure key exchange protocol to set up shared keys between sensor nodes and base stations, (ii) symmetric encryption and decryption for protecting data confidentiality and integrity, and (iii) an authentication scheme for verifying data source.

Oliveira et al. [24] proposed TinyTate, a lightweight Identity-Based Encryption (IBE) security solution for traditional wireless sensor networks. Tan et al [25] proposed an Identity-Based cryptographic solution for WBAN. In their work, the sensor nodes compute public keys by applying a hash function on an arbitrary number of dependent application self-generated keys. These keys are stored on their flash memory and are used to execute elliptic curve encryption/decryption using Elliptic Curve Digital Signature.
Algorithm (ECDSA). This approach has several drawbacks: higher execution time, greater energy consumption due to increased computational overhead, and higher storage requirement for the flash ROM as a result of the public key storage.

III. SYSTEM ARCHITECTURE

Depending on the application scenario, medical wireless sensors are used in an autonomous. An autonomous medical wireless sensors network consists of small wireless nodes on or immediately near to the patient's body, supplying collectively the functions of treatment required by the application. In the simplest scenario, a Central PC collects and stores the readings of the sensors such as ECG, EMG, EEG, SpO2, and blood pressure (systolic and diastolic).

- **Network model**

In Medical Wireless Sensor Networks, security has become very much important as these networks handle the sensitive data. So, security services like authentication and confidentiality must be provided for MWSN. We model the network within the hospital as a three-tiered hierarchy. Figure 1 displays an overview of the hospital network. The purpose of our new scheme is to deliver secure data.

The first level of networking consists of wireless sensors associated with each patient and a Patient's Personal Aggregator (PPA). The PPA processes the data it receives and identifies the occurrence of meaningful medical events. Here, most placed medical wireless sensor networks inside the body that communicate wirelessly with external control devices to automatically monitor and treat physiological conditions to manage a broad range of ailments. For example, the glucose level in the blood can be sensed by implanted glucose sensors. Motion sensors are placed around the body and attached to clothes.

In our network, wireless sensors are used for sensing the patient data. These sensors use the Zigbee protocol for data transmission and can typically transmit data over a maximum distance of about ten meters. As mentioned, wireless sensor nodes have a limited communication range. Depending on the size of the coverage area required, a large number of routing nodes may be needed. The strategy is using the Controllers Rooms that provide paths for sensor nodes to send data to or receive data from the server. The second level of networking is the network that runs throughout the hospital, and it consists of the Rooms Controllers (RCs) associated with the rooms in communication with a server. It serves as a bridge between the PPAs and Server to enable interaction between patients and remote healthcare providers, forwarding or routing the medical data and control messages. If any anomalies are detected in the readings from the sensors, the warnings and patient's location can be immediately identified and declared to the healthcare provider. The Rooms Controllers is further connected to the Server PC through a suitable wired network.

On the server side, level three, the user can view a GUI; the same GUI can also be used to send commands and queries to the motes in the network, allowing medical professionals to monitor their patients' health status remotely in a mobile real-time environment. All health parameters can be stored for later reference. By combining these data with real-time health parameters, doctors and caregivers can provide useful medical assistance to their patients. This is a particularly valuable feature in emergency situations, as it enables the provision of better medical assistance with least inconvenience. These sensor measurements of people's health data should be kept private and hidden from other people during transmission with aggregation to the server.

As shown in Figure 1, a tiered MWSN consists of three kinds of nodes, i.e. Sensors Nodes, Patient's Personal Aggregator, Room Controller and Server PC. Sensors monitor interesting events and, due to their limited storage, periodically send raw readings to the storage nodes with a RF communication channel.

Three roles are defined in the network as:

- **Sensing Nodes (SN):** which consist of small wireless nodes on or immediately near to the patient's body, these sensors sense the patient data, such as ECG, EMG, EEG, SpO2, and blood pressure (systolic and diastolic).

- **Patient's Personal Aggregator (PPA):** Patient's aggregator is attached to the bed. It allows performing aggregation on encrypted data, and verifies the correctness of the encrypted messages.

- **Room Controller (RC):** It is responsible to provide paths for sensor nodes to send data to or receive data from the server.

- **Server PC:** The Server receives all data packets from all the Room's Controllers in the network. The server processes the data, stores it in a database, and presents the data in an adequate form on the interface. The platform is an open and extendable platform so that sensor devices from different vendors can be easily integrated. The core of the system is a Java-based module with interfaces for the communication with wireless sensors.

![Figure 1. Hospital Network Architecture.](image-url)
IV. PROPOSED PROTOCOL

In medical wireless sensor networks, the criticality of data transmitted varies in contrast with other applications of sensor networks. For example, the monitoring of the physical activities of patients is less critical than the heart rate monitoring. Even more critical is sending an alarm in case the patient is in an emergency. Consequently, the threats are different in each case which requires different security levels. The provision of such a service by the link-layer security protocol could lead to a better management of the node’s resources and extend their lifetime. The main focus of this work is the secure transmission of data from SNs to the Server. The proposed scheme is discussed into five phases.

- **Phase 1: System Setup**

  For a short period after deployment, the network is reliable such that each sensor initializes to (i) determine its PPA, its RC, and send the reports to the PC server. In this phase, each node (sensors or PPAs) broadcasts several hello messages. A sensor collects these messages and knows its PPA and RC. Each sensor sends message (ID) which includes sensor node ID and node coordinate.

  These IDs are encrypted and sent through the PPA and RC to the PC server. At the end of this phase, the PC server can establish a mapping table to record the PPA for each sensor. Considering the dynamic behavior of WSNs, the PC server needs to periodically invoke the system setup process to update the mapping table. Since performing such a process requires additional expenditure of energy, the PC server must deliberate whether to do it or not. In this paper, we assume the sensors are quasi-static after being scattered. Therefore, the neighbor relationships between sensors are relatively stable. It means that the PC server only needs to invoke the system setup process when there are some new sensors to be deployed.

- **Phase 2: Compressed Sensing**

  Our aim is to try to reduce the energy cost in all possible aspects including sample energy cost, communication cost, and computation complex.

  The signal samples are first compressed using Compressed Sensing (CS). Then, they are encrypted before getting sent over the channel. Also, they are integrity-protected using a hash algorithm to prevent malicious modifications. The combination of CS theory with WSNs holds promising improvements to some of these limits [27, 28]. The CS optimizes energy consumption which is an important factor in WSNs [29].

  In our model, we consider a sensor network consisting of N nodes. Each node is assigned an integer ID, n, which is in the range of 1 to N. We assume that all the readings generated by sensor nodes (Personal health information (PHI)) are positive real numbers. We also assume that time is divided into equal-sized time slots. With the Centralized Exact algorithm, during each time slot, every sensor node probes the environment and forwards the reading to the PC server. As a result, N readings can be collected at the PC server for each time slot. For T time slots, N × T readings can be gathered. These readings can be organized into an N × T matrix X, where the row and column number correspond to the node ID and time slot number respectively. As a result, only a fraction of the readings from each node are transmitted to the PC server, leading to a variety of different benefits such as reduced traffic and prolonged lifespan.

Below are the details of our encoding algorithm at each sensor.

**Step 1:** Each sensor node randomly generates a binary sampling position vector PN with only q (q<N) non-zero entries. Here, we call λ = \[\frac{q}{N}\] the MC (Matrix Completion) sample ratio.

**Step 2:** Each sensor node then scans the binary sampling position vector and only samples when the corresponding entry is non-zero. At the end, those sampled readings form a vector\(x_q \in \mathbb{R}^q\). At this step, MC based compression is applied. Each node only sample q readings instead of N which results to \(\lambda = \frac{q}{N}\) compression ratio. Thus the energy cost of sampling is reduced.

**Step 3:** At the first time, each sensor node generates and stores the same sparse binary matrix \(B_{p \times q}(p<q)\) using the seed K pre-shared among all sensors and sinks. There are only small numbered \(p > d \geq 1\) non-zero elements random located in each column of \(B_{p \times q}\). Also, we call \(p = \frac{p}{q}\) the CS compression ratio.

**Step 4:** Each sensor node gets CS measurements \(y_p\) from \(x_q\) according below operation: \(y_p = B_{p \times q} \times x_q\)

After sending out \(y_p\) and the sampling position vector PN will be sent out, goes back to step 1.

At this step, since our measurement matrix is a sparse binary matrix, the energy expenditure for this CS compression is only involves simple addition operation. Although \(x_q\) is randomly sampled from N continuous readings, due to the temporal correlation, we find that \(x_q\) can still be sparse under certain transform basis. That is why we can still using CS to compress the readings after Matrix Completion based compression.

At the end, each sensor only needs to send out \(p\) readings instead of \(N\), which results to \(\frac{p}{q} = \lambda \times p\) total compression ratio. In order to ensure more secure transmission, messages should be encrypted.

- **Phase 3: Encryption**

  This phase proposes an extremely lightweight algorithm to update individual keys. For each sensor, the individual key is iteratively XORed with the hash value of the transmitted personal health information (PHI) to dynamically update the key. The idea of using the PHI for key agreement comes from the observation that the human body is dynamic and complex, and the PHI state of a patient is quite unique at a given time. Thus, the PHI is used to update the individual key to provide a good degree of randomness so that an adversary would not be able to guess it and compromise the security of the system easily.
In the end of round \( r \), the individual key of node \( S_i \) is computed as,
\[
K^r_i = K^{r-1}_i \oplus h(\text{PHI}^r_i) \quad r = 1, 2, ..., \quad (1)
\]
Where \( \text{PHI}^r_i \) denotes the PHI from node \( SN_i \) to PPA at round \( r \) while \( h(\bigoplus) \) is a one-way hash function which is publicly known.
Then, \( K^{r-1}_i \) is securely erased. Recall that \( K^0_i (= K) \) is the initial individual key using the polynomial share, we reinterpret (1) as
\[
K^r_i = K^{r-1}_i \oplus h(\text{PHI}^r_i) = K^0_i \oplus \bigoplus_{r=1}^{r-1} h(\text{PHI}^r_i) \quad (2)
\]
Equation (3) is the same as Shannon’s one time pad encryption. When key leakage happens (e.g., node \( S_i \) is compromised), the adversary knows \( K^0_i \). In this case, \( \bigoplus_{r=1}^{r-1} h(\text{PHI}^r_i) \) acts as the one time pad to prevent the adversary from deducing \( K^r_i \).
Assume that at round \( r \), a biosensor node, say \( SN_i \), hopes to deliver the data item \( \{\text{data}^r_i\} \) to PPA. Node \( SN_i \) generates the cipher text \( c^r_i \) as follows:
\[
c^r_i = E((\{\text{data}^r_i\}, r), K^{r-1}_i, h(\text{data}^r_i, K^{r-1}_i)) \quad (3)
\]
From (1) and (3), we can see that PHI encryption keys are updated whenever new PHI is received. Encryption keys are never reused. Thus, minimizing the risk of key discovery attacks.
Then, node \( SN_i \) delivers \( \{c^r_i, ID_{SN_i}, ID_{PPA}\} \) to PPA. Note that PPA can update the individual key with node \( SN_i \) in the same way. The above algorithm is implementation-friendly because bitwise-XOR and hash function are readily supported by most computing hardware. Moreover, the computational cost is very low due to the simplicity of the algorithms.

- **Phase 4: PPA to RC\(_i\) Aggregation**
Each PPA collects messages from all sensors in its Patient. Due to the use of PHI, PPAs and RCs must be able to aggregate encrypted data directly. Medical wireless sensor networks are composed of tiny devices with limited computation and energy capacities. For such devices, data transmission is a very energy consuming operation. It thus becomes essential to the lifetime of a MWSN to minimize the number of bits sent by each device. We use an additive privacy homomorphism to allow aggregation of encrypted data. The goal of additive privacy homomorphism scheme is to provide energy efficient data collection by reducing redundant transmitted messages. The data packet is optimized to work with homomorphic encryption. Many homomorphic cryptosystems and their variants can be found in the literature [30, 31 and 32]. [35] Proposes a simple and provably secure homomorphically stream cipher that allows efficient aggregation of encrypted data.
The main idea of the scheme presented in [10] is to replace the XOR (Exclusive-OR) operation typically found in stream ciphers with modular addition (+). Now, we provide a brief description on this cryptosystem.

Let \( q \) be a large integer and \( k \) be a secret key. To encrypt message \( m \equiv q \) with \( k \), we calculate,
\[
E_M(m, k) = (m + k) \mod q \quad (4)
\]
To decrypt a cipher-text \( c \) with \( k \), we calculate:
\[
D_M(c, k) = (c - k) \mod q \quad (5)
\]
It is obvious that the modular encryption is additively homomorphic, i.e.
\[
E_M(m_1, k_1) + E_M(m_2, k_2) = E_M(m_1 + m_2, k_1 + k_2) \quad (6)
\]
Data aggregation is performed using the sum operator and the result is transmitted as soon as the aggregator receives data from all its sensors. A timeout is used to avoid the aggregator waiting indefinitely. The wait time is dependent upon the position of the aggregator in the network.

- **Phase 5: RC\(_i\) to PC Server Aggregation**
Each RC collects aggregated data from all PPAs in Patients. Each RC transmits the aggregated data to the PC Server after a time length of \( T \). So RCs should wait for a longer time than PPAs. We denote the difference as time interval difference \( \Delta t \), which set up in setup phase.
The server receives only one data packet which consists of one cipher-text corresponding to the PHI of all the sensors in the network. First, the server decrypts the data and gets serials of PHIs. Then, each RC generates a unique ID corresponding to the PHI of all the sensors in the network. Each RC assigns a unique ID to each sensor present in its Patient. Similarly, each PPA has a unique ID and each RC has also a unique ID too. It is to be noted that the number of PPAs and RCs deployed over the network is small as compared to the number of sensors (SN). Besides, their storage, power, and computational capabilities are higher than the SN. If the verification above fails or matches, then a warning message is generated.

V. **SECURITY ANALYSIS**
The safety and security of the medical care environment must be assessed and quantified. This is important if a sensor based environment is introduced in hospitals. In this section, we give the security model and define the services that are ensured by our architecture. Our architecture guarantees the following security services:

- **Integrity and authenticity:** The integrity in our approach can be ensured using hash function which computed and joined to each sent packet between the PC Server and any sensor over the network.
Confidentiality: This aspect is ensured by the use of symmetric encryption to encrypt the exchanged traffic between the PC Server and sensor nodes. The confidentiality is enforced using automatic key update.

Availability: Our solution ensures availability of service for legitimate users when they need it, and it is resilient when large groups of legitimate users access at the same time. Furthermore, it is resilient to Denial of Service attacks.

Patient anonymity: The patient’s privacy is very important in a healthcare system, so patient anonymity is guaranteed by the system. An attacker can only retrieve the ID_PPA at phase4. But this phase does not allow an attacker to determine the identity of a patient.

Fine-grained Access control: Our solution ensures healthcare information confidentiality and scalable fine-grained access control to data stored on the server. Furthermore, it ensures access control in multi-writers access mode on medical data. This protocol ensures backward and forward secrecy. The scheme prevents user to access the plaintext before providing the required attributes that satisfy the access policy. On the other hand, any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged, unless the other attributes that he/she is holding satisfy the access policy. This ensures backwards and forward secrecy.

Collusion resistance: An eavesdropping attacker aims at accessing the private and sensitive patient’s medical data. This attack may be happened during the communication between the patient to server care provider or server care provider to the health cloud. Our solution enforces the access control system and guarantees that users (patients/healthcare/staffs) cannot collude together to get illegitimate access to medical data. Our architecture resists against the collusion attacks to avoid any unauthorized access to medical data.

VI. PERFORMANCE EVALUATION

In this section, we evaluate the performance of our proposed scheme through simulations. The topology of our network is as shown in figure 1, where each node has an ID. We run simulations with 100 patients who are placed in 10 rooms and each patient with a corresponding PPA. This protocol was developed by using the TinyOS 2.0 simulator (TOSSIM) [35, 36] and its variant Power TOSSIM [34].

Our aim is to provide desired level of security while utilizing the least amount of additional energy as overhead. In order to evaluate the energy consumption of the computational overhead for security in communication, we consider two metrics for the performance evaluation: system energy consumption and communication overhead.

As shown in Figure 2, energy consumption of the whole network is evaluated for different values of compression ratio. Simulation results shows, that our protocol consumes less energy till 75% when λ is between 0.6-0.9. It demonstrates that the proposed scheme consumes the least energy compared to the benchmarked schemes. These presented results indicate that the total wireless transmission energy is largely reduced through data compression. It reflects the general case in most sensor networks. Most energy is consumed in RF communications instead of in local CPU processing due to the expensive issuing of power antenna and many hops of data relay.

The Compressed Sensing phase can guarantee the balanced energy costs of nodes by adjusting quantities of data transmission, therefore, it can prolong the lifetime of the network.

This value includes energy spent on calculation and communication, but not energy spent on pre-computations and the user interface; the latter may be several times more depending on the user interface configuration (which is outside the scope of this paper).

In our work, we combine Compressed Sensing with well-established cryptographic algorithms and with an objective of greatly reducing their overhead, because less data is needed to be exchanged. Because most of the energy in sensor networks is consumed due to data transmission, it is critical to mitigate data redundancy and to detect false data as early as possible.

The total amount of data transmission in the network is measured for different values of λ. Fig. 3 shows that when λ is within 0.6-0.9, the reduction of communication overhead the protocol is 30-55% of the payload size, because less data is needed to be exchanged. With the Compressed Sensing and updated individual keys, we ensure data integrity and authenticity with minimal overhead.

By limiting the amount of data, more sensor’s data can be fitted in a data packet leading to less packets being transmitted and, therefore, an overall reduction in energy consumption can be expected.
Another factor that affects the total amount of data transmission in the network is the bit error rate. In [37], a real-world wireless sensor network experimental study shows that bit errors occur in bursts and there are usually 200 or more consecutive error-free bits between two consecutive burst errors. We followed the same loss model in [37] and evaluated the effect of the bit error rate on the total amount of data transmission in the network.

The results are presented in Figure 4, which shows that increasing the bit error rate also increases the amount of data transmission in the network. This is due to the employment of the retransmission mechanism under a high number of frame errors.

VII. CONCLUSIONS

Recent advances in the area of medical wireless sensor networks have enabled the idea of remote patient monitoring. We have outlined how wireless sensor network advancements bring a new dimension to healthcare applications and we have discussed the security issues that arise when integrating this new technology into health care systems. In this paper, we consider the problem of wireless sensor data transmission in medical wireless networks. The security analysis has shown that our approach is feasible for real applications. At the time of this writing, we are planning to begin involving participants from a hospital ward. This hospital ward has both operating theatres and intensive care. We are currently planning a new workshop where we are going to test the current version of the prototype described above. At this workshop, we will be using people acting as patients. More work need to be put into the protocol. In particular, we need to formalize and prove the security properties.

VIII. REFERENCES