Towards Efficient and Secure in-Home Wearable Insomnia Monitoring and Diagnosis System*

S. Tmar-Ben Hamida[+], E. Ben Hamida[++], B. Ahmed[+], and A. Abu-Dayya[++]

Abstract—**Sleep disorders, such as insomnia can seriously affect a patient's quality of life. Sleep measurements based on polysomnographic (PSG) signals and patients' questionnaires are necessary for an accurate evaluation of insomnia. Due to recent innovations in technology, it is now possible to continuously monitor a patient's sleep at home and have their sleep data sent to a remote clinical back-end system for collection and assessment. Most of the research on sleep reported in the literature mainly looks into how to automate the analysis of the sleep data and does not address the problem of the efficient and secure transmissions of the collected health data. This paper provides an experimental evaluation of communication and security protocols that can be used in in-home sleep monitoring and health care and highlights the most suitable protocol in terms of security and overhead. Design guidelines are then derived for the deployment of effective in-home patients monitoring systems.**

I. Introduction

Studies have shown that insomniacs have a risk of hypertension that is 350 percent higher than normal sleepers. Insomnia is also a risk factor for diabetes [1]. Chronic insomnia also increases the chances of developing anxiety and depression. Treatment for all these problems will be limited unless the confounding influence of risk factors such as insomnia is accurately assessed on an individual basis. Sleep studies are considered complicated and uncomfortable for patients and healthy subjects particularly when they need to spend several nights sleeping in unfamiliar surroundings and without privacy. There is thus a need for a wearable, effective insomnia monitoring system which can be used by patients in the comfort of their homes over long periods of time. Driven by the expansion of sleep recording systems and the availability of high mobile bandwidth, sleep monitoring systems are now offering a wider range of new services. This revolution makes the idea of in-home sleep monitoring practical. For insomnia assessment and diagnosis, subjective and objective measures of sleep structure need to be collected from patients. These measures should be incorporated into clinical studies to assist the diagnosis of sleep disorders [2]. Subjective measures are necessary for an accurate evaluation of sleep quality. These measures are currently collected during a face-to-face clinical consultation, where questionnaires are conducted by a psychologist or medical practitioner. With an increasingly mobile society and the worldwide deployment of mobile applications, this information can be collected using an application on a smart device. Objective measures are obtained from polysomnographic (PSG) signals collected from on-body specific electrodes, to quantify the patient behavior during sleep. The PSG signals recorded as a minimum include electroencephalogram (EEG), electromyogram (EMG), electrocardiogram (ECG) and electrooculogram (EOG). The frequency and amplitude of these measures depend on the state of the brain and the body activity among the wakefulness and sleep states. However, long-term PSG monitoring generates huge amount of data, hence requiring efficient communications approaches for the transmission of collected health data to the remote clinical back-end system. Moreover, such in-home sleep monitoring systems pose unprecedented threats to a patient's privacy. It is thus important to provide an efficient and secure end-to-end connectivity between in-home patients and the remote clinical part.

In this paper, we focus on the challenging issue related to the efficient and secure transmission of PSG signals, from the in-home patients to their remote clinical servers. A new communication and security framework is proposed and evaluated using real experiments and sleep PSG signals. The reminder of this paper is organized as follow. Section II, describes the system architecture and presents the different design constraints and challenges. Section III, reviews existing communication and security protocols, and proposes an integrated communication and security mHealth framework. Section IV, evaluates experimentally the proposed framework, and provides a thorough comparative study on selected communication and security protocols. Finally, Section V, derives design guidelines for the deployment of practical in-home sleep monitoring systems, and draws future research directions.

II. System description

The effective and accurate diagnosis of insomnia requires different PSG measures and questionnaires collected from patients in their homes overnight. The collected health information then needs to be transferred to a remote clinician's back-end server for further data analysis to enable

Manuscript received July 30, 2013. * This work was partly supported by NPRP grant #[5-1327-2-568] from the Qatar National Research Fund which is a member of Qatar Foundation. The statements made herein are solely the responsibility of the authors.

[+] Sana Tmar- Ben Hamida and Beena Ahmed are with Electrical and Computer Engineering Department, Texas A & M University, Doha, Qatar (email: {sana.tmar, beena.ahmed}@qatar.tamu.edu)

[++] Elyes Ben Hamida and Adnan Abu-Dayya are with Qatar Mobility Innovations Center (QMIC), Qatar Science and Technology Park, Doha, Qatar. (email: {elyesb, adnan}@qmic.com)

978-1-4799-3163-7/13/$31.00 ©2013 IEEE

an assessment of the subject's sleep quality and assist in diagnosis. During the data analysis process, the PSG signals are usually divided into epochs of 20s or 30s. These epochs are then classified into sleep stages according to one of the sleep standards: the Rechtschaffen and Kales (R&K) [3] or the new sleep clinical standard proposed by the American Academy of Sleep Medicine (AASM) [4]. Our study is based on the AASM requirements which categorized a normal healthy sleep cycle into four states: NREM (non-Rapid Eye Movements) sleep which is classified into three stages (referred to N1 through N3) and REM (Rapid Eye Movements) sleep. A sleep cycle for adults lasts between 60 and 90 minutes on average and is repeated four to five times for a normal night of sleep. The AASM requires at least 2 EEG channels, 2 EOG channels and 1 EMG channel. The collected data is then segmented into 30s epochs.

A. Functionalities

An efficient in-home sleep monitoring system must provide the following functions: i) Recording of physiological signals: the subject is equipped with different sensors and electrodes that constantly measure different vital signals (e.g. EEG, ECG, etc.); ii) Electronic diary: consists of collecting subjective measures (i.e. questionnaires) from patients to provide extra information about the sleep quality (daytime activities, pre-sleep rituals, etc.); iii) Monitoring & Communication: PSG signals and questionnaires are transported to the clinical back-end system using secure and efficient protocols; iv) Sleep analysis: this step is automated and consists mainly of three stages: preprocessing, features extraction and classification. The aim of the first stage is to detect artifacts, eliminate noise and segment the whole signal into epochs. During the second step, features are extracted from individual epochs of recorded PSG signals. These are then used to classify each epoch into one of the sleep stages [5]; and finally v) Reporting: it aims to provide the clinician with the required information to make a diagnosis about the patient's sleep patterns.

B. System Architecture

The architecture of an in-home sleep monitoring system is illustrated in figure1, and comprises three main components:

The Sensing devices: the patient is equipped with different electrodes for data acquisition. Our system consists of: 2 EEG channels (frontal and central), 2 EOG channels (right and left), 1 ECG channel and 1 EMG channel. Each of these signals provides the activity of the autonomous nervous system during sleep. As shown in figure 1, the ECG electrode is incorporated into adjustable chest band and the EEG and EOG electrodes are fitted into adjustable head cap. These electrodes are recorded to a central device that transmits the collected data to a smart equipment.

The Device Coordinator: the PSG signals are collected on the coordinator (or smart phone) which is equipped with various wireless technologies. The collected measures are stored and then transmitted to the clinical back-end system.

The Clinical back-end system: this system consists of a database to store the received data and a server to analyze and process these health data. It provides the clinical data used in the diagnosis of primary insomnia. It includes the sleep stage classifier which will provide information on the sleep structure for use in determining whether or not the patient is having good sleep for their age.

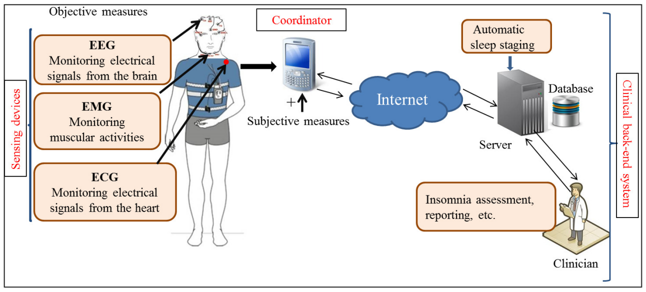
Objective measures
Coordinator
Automatic sleep staging
EEG
Monitoring electrical signals from the brain
EMG
Monitoring muscular activities
ECG
Monitoring electrical signals from the heart
Sensing devices
+
Subjective measures
Internet
Database
Server
Insomnia assessment, reporting, etc.
Clinician
Clinical back-end system

Fig.1. In-Home Wearable Insomnia Monitoring and Diagnosis System.

C. Design Challenges

The design of such autonomous in-home remote sleep monitoring systems poses several intrinsic design challenges and constraints. More specifically, the following design challenges should be carefully addressed to enable the emergence of such mobile health (mHealth) solutions:

- The *real-time availability* of *accurate sleep data* (*i.e.* collected patients physiological signals) is a major requirement to enable timely sleep quality assessment and proper decision making;
- The *scalability* of the in-home monitoring systems and communication architecture is a strong requirement to effectively enable the remote monitoring of a large number of in-home patients, and to accommodate the collection of a large amount of real-time sleep recordings.
- The *security* of the collected measures is a crucial challenge, and should be carefully treated. In fact, the collected patients health information are highly confidential, and the following basic security concepts should be addressed: *authentication*, *availability*, *authorization*, *confidentiality*, *non-repudiation and integrity*.
- The *reliability*, *resilience* and *quality of service* (QoS) of *communications* are of great importance to provide an *end-to-end connectivity* between in-home patients and their medical centers. Moreover, given the large amount of data to be transferred, *low overhead communications* are required to better accommodate available network bandwidths and data plans (*e.g.* GPRS, 3G, 4G, *etc.*).
- Finally, the *usability* of the autonomous sleep monitoring system is also an important challenge. Indeed, the mHealth solution should seamlessly exploit available networks (e.g. WiFi, GPRS, 3G, etc.) and automatically recover from communications errors, without disturbing patients or insomnia monitoring operations.

D. Contributions

In this paper we focus on the challenging issue of providing efficient and secure end-to-end connectivity between the in-home patients' coordinators (i.e. smart phones) and the remote clinical back-end system, as shown in figure 1. Our contributions are many-fold and summarized as follows. First, we review and identify existing communications and security solutions for the context of the in-home monitoring and diagnosis of insomnia, and we propose an integrated communication and security framework. Second, we experimentally evaluate the performance of the selected solutions in terms of communication delays, costs and overheads. Finally, we derive design guidelines for the deployment of effective in-home patients monitoring systems.

III. Proposed communication & security framework

In this section, we review and identify specific communications and security solutions for the context of the in-home monitoring and diagnosis of patients insomnia. As shown in figure 2, the proposed communication and security framework, which is built on top of the TCP/IP Internet protocol, is composed of three main components: i) the Health Data Payload to be transmitted to the remote clinical backend server for further analysis and decision making; ii) the Machine-to-Machine (M2M) communication protocol which is in charge of providing reliable end-to-end connectivity between the deployed in-home mHealth systems and the remote clinical backend sever; and finally iii) the security layer which is in charge of securing all the communications and the transmission of highly confidential health data. These different components are described in more details in the following sub-sections.

A. *Data Serialization Formats for Encoding Health Data*

The main objective of data serializations formats is to convert a set of complex objects and structured data to sequences of bits. Indeed, in such mHealth applications, the collected PSG signals to be sent to the remote backend server can be very complex and huge. It is thus necessary to encode these data before their actual transmission. In the following sub-sections we review potential health data serialization formats for encoding the collected PSG signals.

1) *European Data Format (EDF):* EDF [6] is a standard, non-proprietary and flexible file format which was initially published in 1992 for the exchange and storage of biological or medical time-series. Each EDF file includes a header and one or multiple data records. The header is ASCII based and contains general information regarding the patient, the medical time-series (e.g. start time/date, end time/date, etc.) and the technical characteristics of the signals (e.g. sampling rate, calibration, etc.). The data records contain the actual time-series encoded using little-endian 16-bit integers. More recently, the specification of this file format was enhanced, and the resulting EDF+ file format was published in 2003 [6]. The advantages of EDF+ in comparison to EDF are mainly the possibility to encode discontinuous signals, and the inclusion of time-stamped annotations, events and stimuli.

Health Data Payload	***Collected Sleep Signals & Measurements (EDF [6], CSV [7], BIN)***	
M2M Protocols	***HTTP [8]***	***MQTT [9]***
Security Layer	***SSL/TLS [10]***	
Transport Layer	***TCP***	
Network Layer	***IP v4 / IPv6***	
Data Link Layer	***Ethernet, PPP, etc.***	

Fig.2. The proposed communication and security framework

1) *Comma-Separated Values (CSV) Format*: CSV is an IETF Standard [7], common and simple data format which is currently widely deployed and in use by business and consumer applications. In CSV, data are represented in plain text as a set of records, separated by line breaks (e.g. Line Feed: '\n', Carriage Return: '\r', etc.), and where each record consists in a set of fields separated by a special character or delimiter, most commonly a coma (',') or tab ('\t'). This data format is optimized for plain text (e.g. Unicode, ASCII, etc.) and tabular based data, and due to its simplicity, can be very easily implemented and integrated in any embedded device or platform. More specifically, biological or medical time-series can be very easily encoded using this format.

2) *Proprietary Binary Encoding (BIN) Forma:* An alternative solution to the open or standardized data encoding formats is to use proprietary binary formats. The basic idea is to encode the biological or medical time-series using proprietary binary representations where, for example, the time-series timestamps and values might be encoded as 4-bytes and/or 8 bytes data records. This solution allows an exclusive control over the system (e.g. prevent reverse engineering, optimized storage, etc.), at the cost, however, of limited extensibility and interoperability.

B. *M2M Communication Protocols*

It is expected that Machine-to-Machine (M2M) communications will be the main enabler of future Internet of Things, especially for mHealth applications. As shown in figure 2, the M2M communication protocol represents the second main component of the proposed framework. This protocol will be responsible for establishing a reliable end-to-end communication link between the deployed in-home coordinators (i.e. smart phones or gateways) and the remote clinical back-end server. Moreover, the M2M protocol transfers all the patient health information and collected PSG time-series to the remote medical centers for further data analysis and decision making. All these communications are generally established through a Wide Area Network (WAN), such as GPRS (General packet radio service), 3G (3rd generation of mobile telecommunications technology) or through 4G LTE (long-term evolution), or a Wireless Local Area Network (WLAN), such as WiFi. Existing M2M protocols can be classified according to two main categories: *i) Representational State Transfer (REST) protocols*, such as HTTP [8]; and *ii) Publish–Subscribe protocols*, such as MQTT [9]. The remainder of this section provides a brief overview of the two main M2M protocols, i.e. HTTP and MQTT.

1) Hypertext Transfer Protocol (HTTP): HTTP is a standardized (IETF) application protocol [8], built on top of the TCP, UDP and SSDP layers, for distributed and collaborative systems, such as the World Wide Web, aka. the Web. HTTP is based on a REST-style architecture where clients send requests to servers, which process the requests and return responses. These requests and responses are built around the exchange of HTTP resources, aka. Uniform Resource Locators (URLs). HTTP specifications provides several HTTP methods (e.g. GET, POST, PUT, DELETE, HEAD. etc.) to specify the desired action to be performed on the corresponding HTTP resource. For example, the GET method could be used to retrieve a representation of a given URL; whereas the PUT method could be used to store the attached entity under the provided URL. Though HTTP cannot be considered as a lightweight M2M communication protocol, due to its verbose nature and text based format, some existing commercial and open-source M2M Platforms are based on this protocol. For example, the commercial XIVELY Internet of Things Cloud Platform (cf. https://xively.com/, June 2013) is entirely based on HTTP-based and REST-style APIs, where data types are represented hierarchically in the URLs, and M2M devices can push, retrieve, create or delete data streams using HTTP requests. Another typical example is the open-source MANGO M2M Platform (http://mango.serotoninsoftware.com/, June 2013) which, similarly to XIVELY, provides a HTTP-based and REST-style connectivity protocol and APIs.

2) MQ Telemetry Transport (MQTT): MQTT [9] is the de facto upcoming standard for M2M communications. MQTT is a lightweight application protocol, built on top of the TCP layer, to enable efficient communications over unreliable, intermittent or expensive networks. Moreover, MQTT was specifically designed to operate in constrained environments, such as embedded M2M devices with limited processor, memory and network bandwidth resources (e.g. sensor devices, smart phone, etc.). MQTT is a publish/subscribe messaging protocol and its architecture is based on three main components: The MQTT Broker (i.e. server), and a set of MQTT Publishers and Subscribers (i.e. clients). The MQTT broker is responsible for delivering messages, received from a set of MQTT Publishers, to a set of MQTT Subscribers. Three main quality of services (QoS) for message delivery are supported: i) At most once (QoS 0) where messages are delivered according to the Best effort of the underlying TCP/IP layers; ii) At least once (Qos 1) where messages are assured to be delivered but with possible duplicates; and iii) Exactly once (QoS 2) where messages are assured to be delivered exactly once. This protocol is agnostic to the data payload and is based on the concept of topics or hierarchical logical channels (e.g. /Patient1/ECG/Data.edf). Using this topic-based system, MQTT Subscribers can receive all messages published to topics to which they subscribed to, whereas MQTT Publishers are responsible to publish the right messages or content in the right topics. Though MQTT is not yet a standard, it is currently attracting lots of interests from the embedded research and industrial communities, and several open-source and commercial implementations of this protocol have already been released, and are currently running in several M2M and IoT production environments. More recently, a new OASIS technical committee has been formed to propose MQTT as an OASIS standard.

C. Security Protocols

The security of the in-home patients' health information as well as the collected physiological data is a major challenge. Nowadays, the Transport Layer Security (TLS) [10], and its previous ancestor Socket Secure Layer 3.0 (SSL), is the de facto Internet security protocol standard. TLS is an IETF standard which provides secure communications for applications over TCP/IP, user authentication, data confidentiality and integrity, generation and distribution of secret keys for symmetric and asymmetric encryptions. In particular, TLS provides three main security components: i) Asymmetric encryptions for the exchange of keys between the clients and server, as well as for the authentication; ii) Symmetric encryptions to ensure the privacy of the exchanged data; and finally iii) Message Authentication Code (MAC) to ensure the data integrity and authenticity.

Once a TCP connection is established between the client (e.g. device coordinator) and the server (e.g. the remote clinical back-end server), SSL/TLS [10] starts by a handshake sequence in order to exchange session ID, compression method, client/server certificates, ranfdom values and supported cipher suites. The main objective of this first step is to authenticate the client and to exchange secret keys between the client and the server. Then, all subsequent communications and data exchanges are secured and encrypted using these exchanged keys.

IV. Experimental performance Evaluation

In this section we experimentally evaluate the performance of the proposed communication and security framework, and we provide a thorough comparative study between all the identified protocols, in terms of communication delays, performance, costs and overheads.

A. Experimental Test-Bed Setup

For the purpose of this study, an overnight PSG recording from one healthy adult subject was utilized. Six PSG signals were obtained in this recording, *i.e.* EOG-L, EOG-R, ECG, EMG, EEG Central and EEG Frontal signals. Each of these physiological signals was sampled at 200Hz during a period of 8 hours, 14 minutes and 35 seconds.

In order to evaluate the performance of the proposed communication and security framework, an experimental test-bed comprising two main components was setup: *i)* a *device coordinator* which holds all the collected physiological signals and implements the different communication and security solutions identified in Section

III; and *ii)* a *clinical back-end server* which is connected to the coordinator through a local area network. Prior to the transmission of the collected PSG signals to the remote back-end server, the coordinator firstly encodes these health signals using a *data serialization format* (cf. Section III.A). Then, the encoded data are transmitted to the back-end server using a *M2M protocol* (cf. Section III.B). In the following sub-sections, two communication modes are evaluated: *i)* an *offline communication mode* where all the collected data are sent in one-shot to the server; and *ii)* an *online communication mode* where the encoded data are fragmented into small data segments of 30 seconds, and which are sent gradually to the server. It should be noted that this later mode enables the real-time availability of the sleep data at the back-end server for timely decision making and proper incident detection. Finally, the whole communication process is secured using SSL/TLS, and the resulting communication overhead is evaluated.

B. Experimental Evaluation of Data Serialization Formats

The amount of the collected health data per subject is quite huge, with around 6 million data points (*i.e.* pairs of timestamps and values) per signal. The data thus needs to be properly encoded prior to transmission to the remote clinical back-end server, to improve the scalability and efficiency of the in-Home Wearable Insomnia Monitoring and Diagnosis System. As shown in figure 3, six main health data serialization formats were experimentally evaluated, *i.e.* EDF [6], EDF + ZIP (*i.e.* the de facto compression data method), CSV [7], CSV + ZIP, Proprietary Binary Encoding (cf. Section III.A.3) and BIN+ZIP. The obtained results show that the CSV serialization format is the worst among the evaluated approaches, with a total health data payload size of 466.2492MB. Moreover, the results clearly indicate that the EDF+ZIP is the best method, with an achieved compression rate of around 90% in comparison to CSV, thus making it an interesting data serialization candidate for our mHealth solution. In the remainder of this experimental study, we will adopt the EDF+ZIP format for the encoding of all the collected PSG signals. As shown in figure 3, the total size of the resulting encoded health data payload is 50.3MB (*i.e.* for the whole period of 8h 14mn 35s), whereas the size of each health data segment (*i.e.* 30s length) is 48.4KB.

C. Evaluation of the Estimated Data Transmission Delays

We also evaluated the expected health data transmission delay in the system. Depending on the available networks, the collected health data could be sent from the coordinator to the remote clinical back-end server via various communication channels, such as GPRS, 3G/4G, WiFi or Bluetooth. As shown in Table 1, the expected theoretical transmission delays can vary from a few seconds to a few hours, depending on the considered networks. It should be noted that these theoretical delays are purely indicative and assume a best-case scenario of zero packet loss. Obviously, the use of GPRS for the transmission of such high amount of health data is neither recommended nor practical. In order to enable the remote monitoring of in-home patients, the only viable solutions is to use WiFi networks or high bandwidth cellular networks, such as 3G or 4G. Most current smart phones and tablets already integrate all these modern communication technologies, thus making them the natural choice to setup device coordinators for mHealth applications.

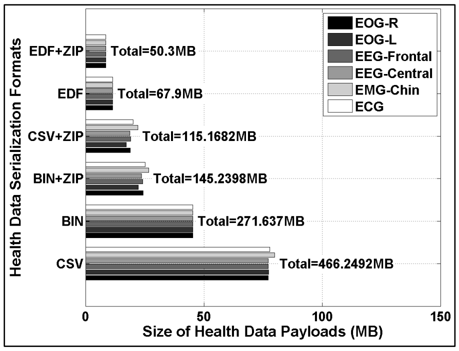

Fig. 3. Total Size of Obtained Health Data Payloads (MB) versus Data Serialization Formats.

TABLE I. EXPECTED HEALTH DATA TRANSMISSION DELAYS VERSUS COMMUNICATION NETWORKS (***EDF+ZIP* FORMAT**)

	GPRS[a]	3G[b]	4G[c]	WiFi[d]	Bluetooth[e]
Peak down-link speed (bps)	85.6K	12.17 M	67.65 M	54M	24M
Peak up-link speed (bps)	42.8K	1.18M	29.37 M		
Expected TX Delays	≈ 2.73h	≈ 6mn	≈ 15s	≈ 8s	≈ 18s

a) GSM GPRS Class 10; b) Typical ooredoo (formerly QTEL) 3G Speeds; c) Typical ooredoo 4G Speeds; d) WiFi 802.11g; e) Bluetooth v3.0 + HS

D. Experimental Evaluation of M2M Protocols Overhead

Once the collected health data are properly encoded, the data is transmitted from the device coordinator to the remote clinical back-end server. In this section, we evaluate the performance of the two selected M2M communication standards, *i.e.* HTTP [8] and MQTT [9]. As already discussed in Section IV.A, two communication modes are evaluated: *i)* an *offline mode* where all encoded data (*i.e.* 50.3MB) are sent in one-shot (*i.e.* in the morning); and *ii)* an *online mode* where the encoded data are fragmented in segments of 30 seconds (*i.e.* 48.4KB per segment), and which are periodically/gradually sent to the remote server (*i.e.* during the whole night). It should be noted that MQTT is evaluated using the three available QoS levels (cf. Section III.B.2).

As shown in figure 4, the online communication mode induces a higher communication overhead in comparison to the offline mode. This is mainly due to the inherent protocols handshakes overheads, as well as due to the fact that the EDF format headers are replicated in all transmitted data segments. Moreover, as expected, the MQTT protocol achieves lower bandwidth and communication overhead in comparison to HTTP, even when using the highest QoS level. The detailed communications costs and overheads are shown in Tables II and III for the online and offline modes, respectively. Similar to the results presented in figure 4, the online communication mode induces a higher number of exchanged packets between the coordinator and the back-end server, with around 24k packets for HTTP and 3k to 8k packets for MQTT. However, quite surprisingly, the total amount of generated network traffic is lower when using the online communication mode (≈46-48MB) instead of the offline mode (≈50MB). The reason is related to the ZIP technique which was found to provide best compression ratios on single data segments (*i.e.* 975 data segments of 48.4KB/30s each) than on full data (i.e. one 50.3MB data record). Finally, we observe that the impact of the MQTT QoS levels is much more significant in the online communication mode, since the transmission of each single data segment requires specific MQTT handshakes (for QoS 1 and 2). This is not the case in the offline communication mode since all the data are sent once and only one QoS handshake is required.

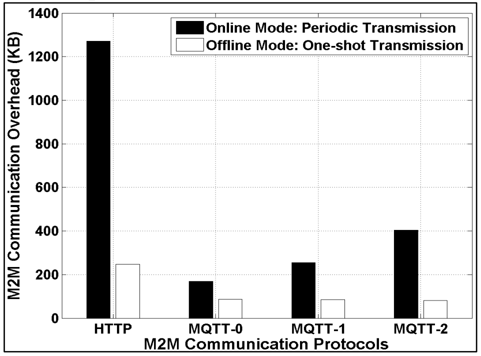

Fig. 4. M2M Communication Overhead (KB) versus M2M Protocols.Experimental Evaluation of Security Protocols Overhead

TABLE II. M2M COMMUNICATION PROTOCOLS OVERHEAD AND PERFORMANCE (**ONLINE MODE**: PERIODIC TRANSMISSION OF SEGMENTS)

	IP Packets Counts			IP Packets	TCP Payload
Protocols	**Total**	**TX**	**RX**	**Size (MB)**	**Size (MB)**
HTTP	24725	15824	9045	48.048	46.806
MQTT-0	3322	2019	1303	46.534	46.369
MQTT-1	5006	3010	1996	46.623	46.375
MQTT-2	7969	4987	2982	46.777	46.382

Finally, we evaluate in this section the impact of the SSL/TLS security protocol in terms of communication overhead. To that end, we consider the MQTT protocol with a QoS of 1 (*i.e. At least once*), an offline communication mode and the SSL/TLS Public Key Certificate approach [10]. All the communications are secured through the exchange of SSL/TLS Certificates between the Client (i.e. coordinator) and the Server (i.e. clinical back-end server). The considered SSL/TLS cipher-suite is DHE-RSA-AES256-SHA, with TLS version 1.0 and self-signed CA certificate. The experimental results show that the amount of generated network traffic is equal to 50.895MB (versus 50.383MB without SSL/TLS). This is mainly due to the specific overhead related to the SSL/TLS protocol headers and handshakes [10]. On average the total overhead of SSL/TLS was found to be between 1% to 2% across all evaluated protocols, communication modes and QoS levels.

TABLE III. M2M COMMUNICATION PROTOCOLS OVERHEAD AND PERFORMANCE (**OFFLINE MODE**: ONE-SHOT TRANSMISSION OF ALL DATA)

	IP Packets Counts			IP Packets	TCP Payload
Protocols	**Total**	**TX**	**RX**	**Size (MB)**	**Size (MB)**
HTTP	4854	3233	1621	50.541	50.3
MQTT-0	1720	1179	541	50.385	50.3
MQTT-1	1682	1168	514	50.383	50.3
MQTT-2	1592	1200	392	50.379	50.3

V. CONCLUSIONS AND FUTURE WORKS

It is now possible to monitor sleep disorders, such as insomnia, in the comfort of the subject's home. In this paper, a new communication and security framework for the remote monitoring of in-home insomnia patients was proposed and thoroughly evaluated through experiments. Our outcomes have several implications for mHealth solutions designers. First, the encoding of the collected PSG signals is of prime importance to improve the scalability and efficiency of the mHealth solution. In this regard, the EDF and EDF+ZIP were found to be the best health data encoding techniques. Second, the M2M communication modes and protocols should be also carefully designed. Our results suggest that the Publish–Subscribe MQTT protocol can be an interesting solution to enable the real-time availability of the collected health data, and to ensure reliable and scalable communications with the remote clinical back-end server. Finally, this work emphasized the importance of implementing effective low-overhead security mechanisms, such as SSL/TLS, to ensure the privacy and security of the exchanged health information and PSG signals.

REFERENCES

[1] N. Murali, A. Svatikova and V. K. Somers, "Cardiovascular physiology and sleep," Frontiers in bioscience: a journal and virtual library, vol. 8, p. 636–652, 2003.

[2] L. Zhang and Z. Zhao , "Objective and subjective measures for sleep disorders.," Neuroscience Bulletin, vol. 23, no. 4, pp. 236-240, 2007

[3] A. Rechtschaffen and A. Kales, A manual of standardized terminology, techniques and scoring system for sleep stages of human subjects, Washington DC, 1968.

[4] H. Danker-Hopfe, P. Anderer, J. Zeitlhofer, M. Boeck, H. Dorn, G. Gruber, E. Heller, E. Loretz, D. Moser, S. Parapatics, B. Saletu, A. Schmidt, and G. Dorffner, "Interrater reliability for sleep scoring according to the Rechtschaffen & Kales and the new AASM standard." Journal of sleep research, vol. 18, no. 1, pp. 74–84, 2009.

[5] J. Hasan, "Past and future of computer-assisted sleep analysis and drowsiness assessment." Journal of clinical neurophysiology, vol. 13, no. 4, pp. 295–313, 1996.

[6] B. Kemp and J. Olivan, "European data format 'plus' (EDF+), an EDF alike standard format for the exchange of physiological data.", Journal of Clinical Neurophysiology, vol. 114, no. 9, pp. 1755-1761, 2003.

[7] Y. Shafranovich, "Common Format and MIME Type for Comma-Separated Values (CSV) Files", IETF Standard, RFC 4180, 2005.

[8] R. Fielding, and Al., "Hypertext Transfer Protocol - HTTP/1.1", IETF Standard, RFC 2616, 1999.

[9] D. Locke, "MQ Telemetry Transport (MQTT) V3.1 Protocol Specification", IBM, 2010.

[10] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", IETF Standard, RFC 5246, 2008.