# Security Considerations for Wireless Carrier Agonistic Bio-Monitoring Systems

Ben Townsend and Jemal Abawajy(✉)

Faculty of Science, Engineering and Built Environment, School of Information Technology, Deakin University, Waurn Ponds Campus, Locked Bag 20000, Geelong, VIC 3220, Australia
jemal.abawajy@deakin.edu.au

**Abstract.** Advances in information and communications technology has led to a significant advances in noncontact portable devices capable of monitoring vital signals of patients. These wearable and implantable bio-monitoring systems allow collections of wearable sensors to be constructed as a Body Area Network (BAN) to record biological data for a subject. Such systems can be used to improve the quality of life and treatment outcomes for patients. One of the main uses for a bio-monitoring system is to record biological data values from a subject and provide them to a doctor or other medical professional. However, wearable bio-monitoring systems raise unique security considerations. In this paper, we discuss some of the security considerations that have arisen in our work around communications agnostic bio-monitoring, and how we have addressed these concerns. Furthermore, the issues related to the identifying and trusting sender and receiver entities are discussed.

**Keywords:** Bio-monitoring systems · Medical monitoring · Mobile communications · Information security · Information privacy · Telemetry · Medical telemetry

## 1 Introduction

It is a modern reality that portable medical monitoring systems are already with us, with such devices currently being used in hospitals using short range transmission infrastructure to allow patient sensors to communicate with ward-based central base-stations. Indeed, in both the academic and commercial worlds, there is much ongoing research into wearable bio-monitoring systems, looking at how we can build wearable networks of sensors and transmitters to monitor and care for patients while not physically confining them to a hospital ward. Such systems are intended to be used by patients in a hospital or in a remote location such as the home. They can provide monitoring for non-critical care patients or for those who require ongoing. Such systems are intended to be used by patients in a hospital or in a remote location such as the home. They can provide monitoring for non-critical care patients or for those who require ongoing monitoring during recovery from illness or operation. They can also be used for extended diagnosis-related data collection.

© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015
B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 725–737, 2015.
DOI: 10.1007/978-3-319-28865-9_48

Bio-monitoring systems have been the subject of a significant amount of research over the past several years. These researches have produced wearable monitoring systems suitable for many applications such as:

- Athletes attempting to reach peak physical performance where monitoring determines biological and physiological status to define where they can focus training.
- Hospital patients who are mobile yet require ongoing monitoring can be allowed to wear a monitoring system and thus not be restricted to the hospital ward.
- Outpatients may require the collection of diagnostic data over a possibly extended period of time.
- The elderly or infirm who are not in a continuous care scenario but may need to be monitored in their homes, to preserve quality of life but ensure ongoing wellbeing.

The potential of wireless sensor networks for telemedicine and biometric monitoring, where sensors with communications capabilities interact to form a body area network for use in medical monitoring is well known. However, one of the concerns of the research into such systems is that the security of data is sometimes implied or assumed, but not explicitly considered as a requirement of the overall solution [3]. Because of the potential sensitivity and ethical concerns around the ability to access biological data measurements for a specific patient, any system transmitting and storing this data should enforce privacy and/or security mechanisms to prevent unauthorised access to the data. In this paper, we address this problem through the application of obfuscation of data and the ability to directly apply encryption to patient readings independently of the carrier that is used to transmit the data.

Our work relates to a communications carrier-agnostic bio-monitoring solution, where we allow the wearable monitoring system to seamlessly select and use the best available carrier to transmit bio-monitoring data and provide the best opportunity for the system to successfully send its data back to the doctor, As part of this research, we have had to consider the impacts that an agnostic approach has on the transmission of data, including how data is secured and how much data can be transmitted over each of the different carriers. Carrier agnosticism means that we cannot rely on the specific capabilities of any one carrier if such capability is not available across our suite of carriers. This includes assuming the presence of native carrier data encoding, identifying and trusting the senderand encrypting sensitive medical data. In developing the protocol, we have had to consider how to address limitations caused by our inability to rely on the capabilities of a specific carrier. In this paper, we discuss security considerations that have arisen in our work, and how we have addressed these concerns in the context of remaining carrier agnostic.

The rest of the paper is organized as follows. In Section 2, the background and related work are presented. In Section 3, security concerns for bio-monitoring data is presented. In Section 4, the issues related to the identifying and trusting sender and receiver entities are discussed. The conclusion is given in Section 5.

## 2 Background and Related Work

A bio-monitoring system is a system that converts information such as respiration, heart rate, temperature, brain activity, heart activity, or blood glucose levels into data that can be processed and recorded. These systems usually consists of set of sensors that collect data from the subject and communicate it to the gateway (e.g., smartphone) that transmits the collected data to a server or directly to the hospital [11].

Figure 1 is a general schematic of a wearable bio-monitoring system that uses mobile technologies with devices such as smartphones being used to co-ordinate the medical sensors and transmit sensor data to the medical professional. The systems are typically wholly body-portable – powered by batteries, worn or carried on the person, and disconnected from physical cables or power infrastructure. Measured data is sent through the wireless network to an acquisition point, which collects the data and transfers it to a database server. Using such a portable system, a patient in a non-critical-care situation can be monitored from the comfort of their own homes or at other remote locations, while on the move, at the shops or out for a walk.

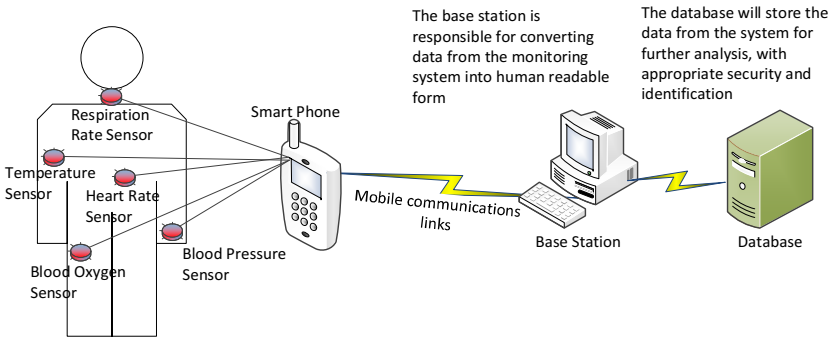


**Fig. 1.** A general wearable bio-monitoring system

There are a number of data types that we might conceivably record in a wearable bio-monitoring system. Budinger [2] discusses some of the data types we might want to encode as the output of a bio-monitoring system. Table 1 summarises the types, sizes, # Octets required to encode the data and min/max values for the sorts of medical data that we might have to record and transmit through the system. Data such as the above may be sampled, digitised and encoded quite readily. However, while these values are discrete and readily encoded, other values may be used in bio-monitoring. The recording of more extensive digitised data may require significant data capacity. As an example, the American Heart Association has stated that a single ECG (electrocardiogram) record showing heart activity could require up to 1.36 gigabytes of storage to allow it to be stored at a meaningful resolution [6].

Throughout the past ten years or so there has been a significant amount of research into wearable monitoring systems. Although many novel and unique systems have been suggested or developed to remotely monitor subjects, much research focus exists

for the specific elements of the bio-monitoring system – the hardware, the sensors, the infrastructure and networking between the hardware which are used to make up a cohesive and wearable bio-monitoring system. However, security is not the main issue in the design of such systems.

**Table 1.** Medical data types

| Type | Min | Max | Unit | Type | # Octets | Example |
|---|---|---|---|---|---|---|
| Temperature | 0 | ~50 | Degrees C | Binary | 1 | 00100101 |
| Heart Rate | 0 | ~200 | Beats per minute | Binary | 1 | 00111100 |
| Blood Pressure | 0 | ~200 | mmHg (x 2 measurements) | Binary | 2 | 01111000 01010000 |
| Respiration rate | 0 | ~50 | Breaths per minute | Binary | 1 | 00001110 |
| Blood oxygen concentration | 0 | 100 | Percentage Oxygen Saturation ($SpO_2$) | Binary | 1 | 01100100 |
| Blood glucose concentration | 0.0 | ~50.0 | Mmol/L – a decimal value (to 1 decimal place) | Binary coded ASCII | 3 | 8.2 |

Varshney [10] identifies several potential issues with existing and proposed wireless health monitoring systems, including the following requirements which, it is asserted, would need to be met by any viable solution for application to the real-world: (i) A high level of security; (ii) A high level of privacy for patient data; and (iii) Highly reliable and usable wireless infrastructure. However, the research focus of many proposed systems in the field concentrates on specific implementations of a BAN and its sensors. There is often an assumption that communications are ubiquitously available and that a pervasive Internet connection is always available. As communications are considered ubiquitous, little consideration is given to the communications backbone as a significant component of the proposed bio-monitoring solution, and issues such as security of data during transmission from the patient to the doctor seem to be assumed and/or implied.

Kwak et al [7] assert that there are three main areas of concern around healthcare monitoring systems. Of specific relevance to our work, they state that the areas of privacy and security are paramount in the implementation of any bio-monitoring system. We assert that a bio-monitoring system must consider the privacy and security of data as part of the fundamental system requirements. Kwak el al [7] state that most papers they reviewed take security against attack into account and that is highly relevant to medical systems. However, while the authors also identify privacy and obfuscation of data and the encryption of transmissions as requirements for bio-monitoring, these issues do not seem to be given the same levels of concern in the research we have reviewed. The presence of these capabilities seems to be assumed and not specifically implemented as part of the proposed systems. As our proposed communications protocol is carrier agnostic, these issues are concerns for us. We cannot rely on an assumption that our carrier will encrypt and/or ensure our data is private. To remain truly carrier agnostic, we must implement security and privacy ourselves.

Borec-Lubecke et al [12] discuss the looming use of the Internet of Things to assist in the monitoring of patients for healthcare purposes [12]. They identify the issues of data privacy and communication security as fundamental to the implementation of a functional eHealthcare solution. However, while identifying the issues, their paper does not propose any solutions to widespread transmission of patient data and/or records. Hanson et al [8] identify a number of the traits that a medical bio-monitoring system must possess or incorporate into its design, including security of access and configuration, privacy of information and encryption of data. Once again, privacy and encryption are key facts. Hanson also mentions configurability as a requirement of a solution and on this point we wholly agree. Our proposed communications protocol considers the need to reconfigure a monitoring system "over the air" while it is deployed in the field. In evaluating how this might be achieved, this has identified additional security and identification concerns that must be addressed in an operational real world solution.

**Table 2.** Fields in the message protocol

| Field Nbr. | Field Name | Abbrev. |
|---|---|---|
| 1 | Start of Message Frame | SOMF |
| 2 | Message Protocol Format | MFMT |
| 3 | Message Type | MTYP |
| 4 | Application ID | APID |
| 5 | Sender Device ID | SDID |
| 6 | Recipient Device ID | RDID |
| 7 | Message ID | MSID |
| 8 | Message Structure | MSTR |
| 9 | Generation Timestamp | GENT |
| 10 | Validity Period | VAPD |
| 11 | User Data Segment Length | UDSL |
| 12 | User Data Segment Encryption ID | UDSE |
| 13 | Header Checksum | HCHK |
| 14 | User Data Segment Checksum | UCHK |
| 15 | Combined Message Checksum | MCHK |
| 16 | User Data Segment | UDSG |

## 3 Security Concerns for Bio-monitoring Data

While a large binary data set such as an ECG may not be readily human readable, the data types shown in table 1 are quite easily interpretable. As with other transmissions, messages transmitted from a bio-monitoring system to a doctor may be intercepted by a third party during the transmission process. Where message data is not obfuscated and/or encrypted in such a way as to render the data incoherent to an external unauthorised attacker, patient data could be compromised. We would assert that the developers of bio-monitoring systems must consider the protection of information during

transmission as a fundamental system requirement. The protection of data is especially important if we facilitate transmission of the data via an open network such as the Internet, where many devices may "see" a message between source and destination. To this end, both obfuscation and encryption of data should be considered an essential part of the overall capabilities of a bio-monitoring system.

### 3.1 Communications Protocol

In our research, we are creating a robust communications protocol to facilitate bio-monitoring communications via a carrier agnostic approach. Being carrier agnostic allows us to use carriers such as Internet, Packet Radio, Mobile Data, MMS and SMS. We have chosen a carrier agnostic approach due to the nature of medical monitoring and potential ramifications if the system cannot deliver a monitoring message for a critical medical situation. A remote wearable monitoring system must have every opportunity to "get the message through" to its base station. By supporting multiple carriers in the same monitoring system, our solution can select the best available communications method at the point of transmission and fail over between carriers as required. We have developed a simple communications protocol which consists of a header block and a user data segment,that can be transmitted via any of a number of possible carriers, including Internet, Mobile or Fixed Line Data call, SMS, Multimedia Message and Packet Radio. In being carrier agnostic however, we have had to facilitate a number of key features, including obfuscation of data, identification of sender and recipient, and encryption of the user data. The structure of our packet is shown In Table 2.

### 3.2 Obfuscation

In the context of a bio-monitoring system, the obfuscation of data removes the ability to associate data with the subject without the provision of a key to the data. As part of our research, we have created a communications protocol (see table 2 above) that can be used to transmit bio-monitoring data and associated header information. The communications packet header identifies the sender device, receiver device and the monitoring "application" in which a message is intended to be used. By remaining carrier agnostic, we cannot assume identification elements such as IP address or telephone number will exist in our message. However, we only identify devices in the header. No personally identifying details (such as patient ID, patient name etc) are incorporated into the message.

While the user data segment of our message may contain biological readings from a specific subject (amongst other possible uses for the data segment), the message itself contains no information that can associate a specific subject with their readings. To make the association between subject and biological readings transmitted in a message, the reader of the message needs to correlate the sender device ID (i.e. the ID of a specific bio-monitor) to a subject ID. This correlating data is stored at the base station used by the doctor, and is never transmitted over the network. As such, to

perform this correlation implies access to data that is only available via direct access on the base station itself.

Because we divorce the data in the transmission from the identity of the subject, it is difficult for an attacker who intercepts a transmission to re-associate the data to a specific subject unless the attacker also gains access to the base station. To this end, we propose that the first security tool that any bio-monitoring system should implement is the effective obfuscation of the subject's data from its identification details. This can be further supplemented by the implementation of a rule that states that no personally identifying data is ever transmitted within a bio-monitoring application such that it could be intercepted and used to establish the link between the subject and their monitoring data.

### 3.3 Encryption of Data

Our communications protocol facilitates the control, management and transmission of data within a bio-monitoring system consisting of wearable bio-monitors and a central doctor's base station (for example at the hospital). In this system, the user data segment of our messages is used to transmit system data such as the biological readings of patients. Consider, for example, a hypothetical encoding scheme where user data segment is encoded with biological readings via a number of type/value pairs. In this instance the first octet defines the type and the next X octets define the data for that data type, repeated in each message as shown in Fig. 2.

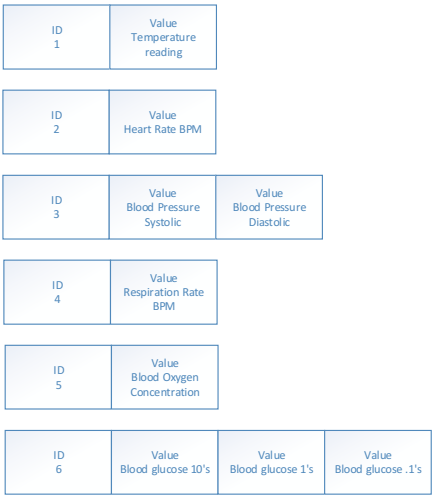


**Fig. 2.** Hypothetical Values and Octets of data in the User Data Segment

This data is obfuscated and cannot be related back to a specific subject without the index that shows which sender device ID relates to which patient. However, despite the obfuscation, if such data were encoded into a message without any form of encryption, in would in most cases be clearly readable by taking the data octets and

decoding their binary values. The type/value pair encoding mechanism does provide a level of obfuscation to the data. To correctly interpret the data requires the attacker to "understand" what each type value means and what size the data for that type is. However, it could be argued that simple obfuscation of this nature is not enough to protect the data against a determined attempt to compromise the system and interpret the values.

Consider also an alternative scenario, where our user definable data segment may carry biological data encoded in a standards compliant packet of medical telemetry – for example using the IEEE 11073-20601 standard that has been defined specifically for this purpose. Where a standard's based format is used to transmit data, it is possible that the attacker could, through analysis, determine the standard in use and therefore have a ready "map" of the methods of encoding data within a message. It is as a result of these sorts of scenarios that we must consider whether the data we are transmitting requires encryption, over and above the obfuscation discussed previously. Our research makes use of a number of communications carriers, including public carriers such as the packet radio network and the Internet. This means that, in some cases, our transmissions may be broadcast and could be intercepted by anyone who is listening. For certain types of transmission, we may determine that our data should be protected over and above the capabilities of an obfuscated data set, and thus we must consider how we protect the data appropriately.

Where the need for encryption rather than obfuscation is identified, one might argue that many carriers provide encryption capabilities as a native part of their feature set. For example, GSM mobile communications including both mobile data and SMS have typically been encrypted using the A5 family of algorithms [1]. However, in recent years, A5 and other encryptions have been broken and there are a number of published solutions that allow decryption of GSM based mobile transmissions potentially in real time [1][5]. As noted earlier, the nature of our research is carrier agnostic, and this requires that we allow our system to utilise multiple communications mechanisms and thus maintain an ability to fail over to an alternate carrier when the preferred carrier is unavailable. As a result of the need to support multiple carriers, we cannot rely on encryption provided natively by a specific carrier unless the same capability exists across all of our potential carriers. Our research has identified that, where our data is to be transmittable via the best available carrier from a pool that might include Internet, Packet Radio, Mobile Data, MMS or SMS, we must accept that encryption does not exist natively in each of these carriers. As such, in taking the lowest common denominator of features from our carrier pool, we must not expect the carrier to provide the encryption.

Our solution therefore requires the bio-monitoring system implement the ability to apply encryption to the data as part of the system's capabilities and not rely on the carrier. While this is something we considered in our work through the necessity of our agnostic approach, we would strongly recommend the encryption of data transmissions be implemented as a native capability of any monitoring system over and above any capabilities offered by the carrier.

### 3.4 Appropriate Encryption

While encryption is a requirement of the bio-monitoring systems' transmissions, we must also consider that for some of our potential carriers the data capacity of a message may be limited. For example, in an ideal world we would use an unlimited Internet data stream, but in our system we may have to fall back to slow packet radio transmission at 9600 baud [4] (TAPR 1995) (TAPR 1995), or even use an SMS message with a mere 140 octets of data capacity [6]. Because we do not always have the luxury of an unlimited data stream, we must not only consider that encryption is essential. We must also consider whether the encryption to be applied is appropriate for the full gamut of prospective carriers in our system. In defining an appropriate encryption algorithm for use with our protocol, we believe that a number of factors must be considered:

- The encryption algorithm should require a (relatively) low overhead to store encrypted data. The number of additional octets of data required to encrypt the data should low when compared to the data content to be encrypted. Where we have length limited carriers, we do not want the encryption overhead to outweigh the volume of data in the message.
- The encryption algorithm should provide a level of data security that is commensurate with the requirements for data protection imposed by the application. For example, obfuscation of the data and the removal of personally identifying detail in all messages may reduce the need for complex, high overhead encryption. While monitoring data is personal and should be confidential, if it has no contextualisation to a specific subject in the case of interception of a specific message, do we need to make use of 1024 bit encryption that would take longer than the lifetime of the universe to break?
- Any encryption algorithm should ideally have a low processing overhead to encrypt or decrypt data. The remote monitoring system is likely to be battery operated may not have significant processing power.
- The time to encrypt or decrypt a message must allow us to treat messages urgently, so it is not acceptable to allow encryption to cause significant delays before the transmission can occur.

From the above set of constraints, it is apparent that the appropriate encryption needs to have a low processing overhead and a low data overhead (in terms of the additional octets that are required to encrypt the data). If we are using 1024 bit RSA encryption, for example, the overhead is such that we could not use SMS as one of our potential carriers (as the RSA encrypted data would exceed the 140 octets of the SMS payload). To facilitate the ability to encrypt user data, we have allowed our communications protocol to implement application specific encryption through the use of an application-defined encryption ID that is transmitted as part of the communications packet header. This single octet value allows the application using the protocol to select one of 255 possible encryption mechanisms that can be applied to the user data segment data. In this way, the application can define the types of encryption to be used based on the capabilities of the potential carriers in the system. For exam-

ple, the ID may be used to identify different key sets for public key encryption, further securing the data by the use of multiple possible rolling keysets. Thus an encryption ID value of 1 may signify key set 1 is in use. An ID of 2 signifies keyset 2 in use etc. Alternatively, the encryption mode may change based on the carriers that are currently active. For example, where SMS is a potential carrier, only low overhead encryption may be used identified by a specific set of encryption ID's. Alternatively, if the carriers in use all have large possible data payloads (such as Internet, Packet Radio and Mobile Data Call), then higher overhead encryption may be defined on an application specific basis.

## 4 Identifying and Trusting Sender and Receiver

In a bio-monitoring system, it is highly likely that the component transceivers within the system will be known as part of the system configuration. This includes both the base station and any wearable monitors in use within a particular application. Because the component devices are known, this allows us to utilise device identification to assist us in trusting messages sent or received on the network. Because our communications are carrier agnostic, we cannot depend on any of the identification details that may be included in a carrier specific message (for example, IP address, telephone number etc). We must be cognizant of the fact that some of our potential carriers (such as packet radio) may not include a system level station ID as part of their message transmission. Therefore, as part of our protocol, we have implemented a number of identification fields to specifically identify one of the transceiver stations in the system. Four identification fields are part of our standard message header block, namely an Application ID, Sender Device ID, Recipient Device ID and Message ID.

The application ID is a single octet used to identify one of 255 possible applications that may use the same communications infrastructure. This is specifically relevant where one or more of our carriers are part of a broadcast infrastructure, for example over radio or Internet. In these cases, many participating (and non-participating) devices may "listen" to the same transmission, even if it is not addressed to them. The application ID allows segmented use of the communications infrastructure by defining different logical applications on the same infrastructure. Applications using our protocol must check the application ID matches their own application prior to actioning a message.

The sender device ID and receiver device ID are 24 bit numbers that identify a specific device within the application. While this may identify up to 16 million unique devices per application, it is unlikely that a single monitoring application would require this number of devices for an application. As there is no requirement that we sequentially allocate ID's to devices on an incremental basis, we are able to use the ID to establish a trust relationship. To do this, device ID's are allocated according to an algorithm. The algorithm can be application defined based on the requirements of the system using the agnostic-communications protocol. By using algorithmic allocation of ID's, only certain device ID's will be valid within the network. This will allow the application to implement checks to ensure that a device ID fits the allocation algo-

rithm and may thus make it more difficult for a rogue device to easily obtain a valid ID and masquerade on the network to "listen" to the transmissions going back and forth.

The sender and receiver ID identify the source and destination of a message as part of the message header's addressing. This allows us to build an application where a message is only "read" by the device it is intended for. The receiver should check that its own ID value matches the receiver ID in the message. The sender ID allows us to define specific message types that will only be actioned when they come from a specific sender. For example, a message to change the configuration of a remote monitor may only be accepted if the sender ID is the same as that of the base station at the hospital.

Finally each message has its own internal identification, encoded in the message ID field. For our protocol, the message ID is a 24 bit number, and thus 16 million unique messages per sender and receiver pair can be identified using the message ID alone. The message ID is allocated by the sender of the message, using the next available ID from its pool of message ID's. Message ID's are used in conjunction with the application, sender and receiver ID's to provide a highly unique message identifier within the system. With 16 million (approx.) ID's available, we would assert that this is sufficient for a bio-monitoring application, as even sending 1 message per second, 24 hours per day, this would give us a monitoring period of 194.18 days before the pool was exhausted and had to cycle back to 1. If we reduce messages to 5 second intervals, we have over 900 days before the pool is exhausted.

To manage message addressing, we combine all of the identification fields together. The application, receiver, sender and message ID's provide a total of 10 octets or 80 bits of identification. To set the message ID, the sequence of messages between a sender and receiver pair is tracked by the sender. Thus, in application 1, for a combination of sender ID 1 and receiver ID 2, the message ID relates to the sequence of messages sent between this sender and receiver and is incremented for each message sent in that direction. When sending between sender ID 2 and receiver ID 1, the message ID relates to the sequence between sender 2 and receiver 1 and so tracks that series of communications in that direction. This will thus provide 16 million messages per sender/receiver pair. For example, see Table 3.

**Table 3.** The use of message ID between specific sender and receiver pairs

| Transmission number | Sender ID | Receiver ID | Message ID |
|---|---|---|---|
| 1 | 1 | 2 | 1 |
| 2 | 1 | 2 | 2 |
| 3 | 2 | 1 | 1 |
| 4 | 1 | 2 | 3 |
| 5 | 2 | 1 | 2 |

By combining the application, sender and receiver ID's, and the message ID in a sender/receiver directional pairing, we can ensure that messages come from a known and accepted source, that the message is being actioned by the correct device, and that the message was sent by a sender we will accept. By maintaining an application specific set of sender authorisations, we can also ensure we do not action specific types of message (for example, configuration messages) unless they come from a station that is authorized to make configuration changes (for example, the base station). By using the message ID in conjunction with the sender and receiver, we can also track the sequence of messages, and ensure we do not miss messages (for example, if the message ID between sender 1 and destination 2 suddenly jumps from message ID 10 to message 12, we can infer message ID 11 may have been lost).

## 5 Conclusion

Security of data, the need to obfuscate data and the ability to identify and trust a sender and receiver within a transmission can all be beneficial attributes to the successful implementation of a bio-monitoring system. Obfuscation prevents the transmitted data from being associated with a specific subject without additional data that is never transmitted over the network. In any system that transmits data over a public network, we should assume that the data may be intercepted and this, obfuscation should be the first line of defence for any biological monitoring data transmission. Encryption provides the ability to protect data from unauthorised access, even if that data has already been obfuscated. However, when using carriers with limited payload capacity it must be considered that encryption can have an additional bandwidth and encoding overhead, so we assert that the encryption used for the transmission of bio-monitoring data must be appropriate to the application. We identify a number of factors to inform the decision of what constitutes an appropriate data encryption mechanism. The use of message fields to uniquely identify the members of a bio-monitoring system facilitates a number of capabilities in the system. The use of algorithmic allocation of device ID's can make it more difficult for a rogue device to generate an ID masquerade as part of the network as any ID needs to match the allocation algorithm, which is not published by the network. The ability to specifically identify sender and receiver provides an ability to action messages only when they are received at the correct station, and allows us to restrict the use of certain message types (i.e. configuration messages) unless they are sent from an appropriate sender. We have found that all three elements are required to properly implement a carrier agnostic approach to bio-monitoring communications and must be considered as fundamental requirements of our system. However, given their benefits, we would assert that all of these features should be considered as security requirements of any medical bio-monitoring system.

## References


1. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext Only Cryptanalysis of GSM Encrypted Communication. Technion Technical Report, vol. CS-2006-2007 (2006)
2. Budinger, T.F.: Biomonitoring With Wireless Communications. Annual Review of Biomedical Engineering **5**(1), 383–412 (2003)
3. Townsend, B., Abawajy, J., Kim, T.-h.: SMS-based Medical Diagnostic Telemetry Data Transmission Protocol for Medical Sensors. Sensors **11**(4), 4231–4243 (2011)
4. ETSI: Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (GSM 03.40), European Teleommuniations Standards Institute, Valbonne, France (1996a)
5. Guneysu, T., Kasper, T., Novotny, M., Paar, C., Rupp, A.: Cryptanalysis with Copacobana. IEEE Transactions on Computers **57**(11), 16 (2008)
6. Iskandar, R., Simri W, I.W.: Compression of ECG Signal Using Neural Network Predictor and Huffman Coding. Proceeding Seminar Ilmiah Nasional KOMMIT 2010 **30**, 3 (2010)
7. Kwak, K.S.: Social Issues in Wireless Sensor Networks with Healthcare Perspective. The International Arab Journal of Information Technology **8**(1), 7 (2011)
8. Hanson, M.A., Powell Jr, H.C., Barth, A.T., Ringgenberg, K., Calhoun, B.H., Aylor, J.H., Lach, J.: Body Area Sensor Networks: Challenges and Opportunities. Computer **0018–9162**(9), 8 (2009)
9. TAPR 1995: Packet Radio: What? Why? How?, Tucson Amateur Packet Radio Corporation (2013). http://www.tapr.org/pr_intro.html (retrieved October 3, 2013)
10. Varshney, U.: Pervasive Healthcare and Wireless Health Monitoring. Mobile Network Applications **2007**(12), 15 (2007)
11. Fang, X., et al.: An extensible embedded terminal platform for wireless telemonitoring. In: 2012 International Conference on Information and Automation (ICIA), pp. 668–673 (2012)
12. Boric-Lubecke, O., Gao, X., Yavari, E., Baboli, M., Singh, A., Lubecke, V,M.: E-healthcare: remote monitoring, privacy, and security. In: 2014 IEEE MTT-S International Conference on Microwave Symposium (IMS), pp. 1–3 (2014)