

NETWORK-AWARE BIOMEDICAL SIGNAL PROCESSING

Loss Concealment or Loss Awareness

Beatriz Barros¹, Ana Aguiar² and Daniel E. Lucani²

¹*Instituto de Telecomunicações, Departamento de Engenharia e Gestão Industrial, Faculdade de Engenharia da Universidade do Porto, Rua Dr. Roberto Frias s/n, Porto, Portugal*

²*Instituto de Telecomunicações, Departamento de Engenharia Electrotécnica e de Computadores, Faculdade de Engenharia da Universidade do Porto, Rua Dr. Roberto Frias s/n, Porto, Portugal*

Keywords: Biomedical signal processing, Networking, Loss concealment.

Abstract: The development of biomedical signal processing algorithms typically assumes that the data can be sampled at an uniform rate and without loss of samples. Although this is a valid assumption for Holter applications or clinical testing, these assumptions become questionable in the presence of remote monitoring of patients through inherently lossy communication networks. The task for the networking engineers has been to create better, more reliable protocols to avoid packet losses from affecting the signal processing algorithms. However, inherent constraints from resource-constrained devices and lossy networks used for remote monitoring make this objective infeasible in many situations. Given irreparable losses due to data transmission, this paper poses the following questions: (i) how would the current algorithms react to losses, and (ii) what alternatives are available to still guarantee reliable monitoring and detection of emergency events. For the latter, we consider two options: the use of current algorithms after a loss concealment stage, and the design of loss aware algorithms. We argue that a joint design of network protocols and signal processing algorithms is instrumental for providing reliable biomedical monitoring. We propose a simple, yet powerful model of the network under a variety of packet loss channels as well as data packetization mechanisms. Extensive numerical results are provided for addressing question (i), focusing on the sensitivity and positive predictivity of standard ECG algorithms under a variety of network scenarios. We use the MIT-BIH arrhythmia database and simple loss concealment mechanisms and show that even small percentages of packet losses can have a significant impact on a algorithm's performance.

1 INTRODUCTION

Conventional wisdom for biomedical signal processing algorithms says that the data, although noisy, is received without losses and typically at an uniform sampling rate. Although a valid assumption for the case of Holter devices and clinical observation, a stronger challenge is faced when considering transmission of the data through inherently lossy networks. The demands on the networking community have been to provide protocols and mechanisms that support a lossless transmission of the data. For example, Ref. (Alessanco and Garca, 2010) provides analysis and simulation results using the real-time ECG protocol (RETP), an alternative to TCP/IP for reliable transmission of all data samples, studying networks with losses and its effects upon delay and mean opinion score (MOS) value for clinical assessment. In this sense, the development of signal processing algorithms for feature ex-

traction and communication protocols for data gathering are typically considered as separate tasks.

Although valid in Holter devices and during clinical observation, remote and online monitoring of patients introduces new challenges and constraints to the system. A closer inspection reveals that biomedical devices for remote data gathering rely on resource-constrained, bandwidth-limited, wireless devices and unreliable connectivity, e.g., (Hu et al., 2009) (Pandian et al., 2008). These limitations may prevent the system from providing perfect reliability on the data transmission process, which translates in samples being lost irreparably.

Although remote and automatic monitoring of patients is usually seen as a clear option to reducing medical costs, if packet losses produce an increase of false positives in emergency scenarios i) the economical benefits may vanish as personnel and equipment may be mobilized unnecessarily, or ii) the system may

not be deployed in practice due to lack of reliability.

Our take is that a design of signal processing algorithms that are aware of lossy transmissions is fundamental for guaranteeing *reliable monitoring* and become pivotal towards a joint design of network protocols and processing algorithms. We propose two different approaches to the problem from the signal processing viewpoint: loss concealment and loss awareness. The former relies on using loss concealment mechanisms, e.g., prediction algorithms to determine missing samples, as well as appropriate interleaving and packetization of the samples in order to hide the losses from current algorithms. The benefit of this approach is that current algorithms may be kept without change. The main drawback of this approach is that the signal processing algorithms do not differentiate between actual samples and predicted samples, i.e., they are not able to exploit this knowledge.

Although previous work has considered loss concealment as an option, e.g., (Theera-Umpon et al., 2008), (Prieto-Guerrero et al., 2007), it has done so without exploiting additional dimensions provided by the communication architecture. For example, (Theera-Umpon et al., 2008) considers that losses happen during a given interval, which could be a valid assumption considering that a data packet is likely to carry several samples. However, interleaving the samples prior to generating the data packets, i.e., rearranging the samples across several packets so that they are non-contiguous, provides a powerful option to spread the lost samples. This can allow the concealment mechanisms to operate more efficiently as the number of contiguous samples missing may decrease dramatically.

Loss awareness calls for a re-design of biomedical signal processing algorithms to consider one or several of the following: i) variable (and random) sampling, ii) confidence values for samples providing full confidence for actual samples and lower confidence for predicted/estimated samples, iii) incorporate network statistics as key parameters for the algorithms, iv) control of the data source to request specific lost samples (but possibly not all) or reduce sampling rate.

To attain optimal performance of the two approaches, a joint design of network protocols and signal processing algorithm is required. In other words, a joint design of network protocols that can adapt to requirements of the algorithms and algorithms that can adapt to network characteristics and effectively control the protocols. This new paradigm for network-aware biomedical algorithm design shall be instrumental to making effective, remote, and low cost biomedical monitoring a reality.

Aiming at a deeper understanding of how packet

losses affect vital signs processing algorithms as well as how concealing packet losses can improve this behavior, we make the following contributions:

- *Requirement and Challenges:* We provide a discussion of requirements and challenges of remote, online biomedical monitoring emphasizing different possible sources of sample losses, which may not only be limited to network congestion or losses in wireless channels but that can be generated due to active security attacks.
- *Evaluation Framework:* Based on key communications, network, and loss concealment parameters and building blocks, we propose a simple yet detailed model to characterize algorithm performance. This evaluation model is adaptive, in the sense that different versions of the proposed building blocks can be incorporated seamlessly.
- *Numerical Analysis:* We evaluate ECG algorithms in terms of sensitivity and positive predictivity under a variety of network and loss concealment scenarios. The MIT-BIH data base and the ecgpuwave algorithm are used as an interesting example. The results clearly illustrate that advanced loss concealment mechanisms or, alternatively, loss-aware vital signs algorithms are a must in networks that cannot guarantee delivery of every sample. This case is extremely relevant for remote monitoring of patients using simple wireless devices, e.g., wireless sensor networks, wireless body-area networks. Our preliminary results confirm that concealment of lost samples is possible in a limited number of scenarios (low packet loss rates, low number of samples per packet) even with simple loss concealment algorithms, which implies that no modification of current algorithms is needed after an initial loss concealment stage. However, loss concealment becomes insufficient in more typical wireless network scenarios.
- *Alternative Algorithms:* We provide a discussion of alternative approaches to joint network protocol-signal processing algorithm design as well as loss concealment mechanisms that may be promising in our applications.

2 REQUIREMENTS AND CHALLENGES

Remote and automatic monitoring of patients sets a series of design requirements and inherent challenges driven from them.

- *Data Rates.* Depend considerably on the vital signs that are being collected and linked to the

sampling rates. For example, a 3-lead ECG monitor sending 2 channels sampled at 250 Hz with 8-bit samples has a raw data rate of 4 kbps. However, a 12-lead ECG monitor sending 8 channels sampled at 1000 Hz with 12-bit samples, generates a raw data rate of 96 kbps. Although, the former is a much more common case for remote monitoring, we emphasize that this is the source data rate. The actual requested data rate to the network shall depend on a variety of factors, of which packetization (i.e., how many and which samples are sent in each packet) plays the key role. Communication protocols at different layers add headers to each packet traversing the network for control and identification purposes. Depending on the protocols used, this header's size could be significant. In many scenarios, it is in the order of tens of bytes. Clearly, if only one 8-bit sample is sent per packet in the 3-lead case and if overall header is 20 bytes per packet, the rate from the perspective of the network is actually 84kbps. Sending several samples per packet reduces the overhead, but at the cost of i) additional delay in the transmission of the samples, ii) higher impact to the system due to a single packet loss.

- *Time Criticality.* Remote monitoring of patients is time critical in the sense that the samples should be received within a certain time frame to be able to predict, prepare, and/or react to critical situations. However, a delay of several seconds is still acceptable from this perspective (Alesanco and Garca, 2010).
- *Light-weight, Cost-effective Solutions.* One of the key arguments for remote, online monitoring is to reduce the economical and qualified human resources cost of monitoring patients. Devices and services provided require a cost-effective design, which may limit the storage and processing capabilities of these devices. These limitations constitute one of the key motivations for considering network-aware algorithms which can leverage resources in an effective fashion and where more computationally intensive algorithms are not implemented in the end devices. This requirement also motivates the use of off-the-shelf network devices with standard protocols, e.g., Bluetooth or ZigBee, which introduce limitations of their own in terms of maximum data rate per user, reliability, transmission range, protocol overhead, or transmission band.
- *Reliable Monitoring.* Although the objective of reliable monitoring of patients has been translated thus far into providing reliable, lossless transmission of data, this need not be the case. The ulti-

mate objective of the system is to deliver a reliable monitoring service to patients and medical personnel. In fact, this ultimate objective may be compromised if the system is unable to adapt to varying network conditions, which may render present sampling settings unserviceable, or if the loss of samples compromises the accuracy of event detection algorithms and/or triggers unnecessary alerts.

- *Security and Privacy.* Vital signs monitoring deal with sensitive and private information, which impose stringent requirements in terms of cybersecurity and consumer privacy. However, current network architectures consider devices with limited processing capabilities close to the individual (data source), which calls for light-weight security solutions (Stuart et al., 2008). The architecture must ensure that unauthorized agents are unable to access the data collected and that active attacks capable of disrupting data collection are mitigated. From the perspective of design of network-aware signal processing algorithms, active attacks can become a source of packet losses in the system and one that could be relevant even if the architecture has enough resources to guarantee delivery of data packets in normal operation.

3 SYSTEM MODEL

We model the transmission of a vital signs data stream across a network as depicted in Figure 1. The raw data stream received from the vital signs monitor is fed into a transmitter, which in its simplest form prepares the data for sending across the network by splitting it into packets, containing one or more samples each. These packets are passed through the network, which causes some packets to be lost. At the receiver, the stream is re-built from the data in the received packets, whereby the samples corresponding to lost packets are replaced. The re-built stream is then fed into a signal processing algorithm that extracts useful information from the data. For our evaluation, we use the well-established heart beat detection algorithm *ecgpuwave* (Pan and Tompkins, 1985). This model enables us to assess the impact of the most relevant parameters of the transmission of a signal across a packet data network on the performance of a widely known signal processing algorithm that assumes by design that no data losses occur.

The packetization step plays a relevant role, since for a same packet loss rate in the network more samples are lost when each packet carries a larger number of samples. The drawback of transmitting a single

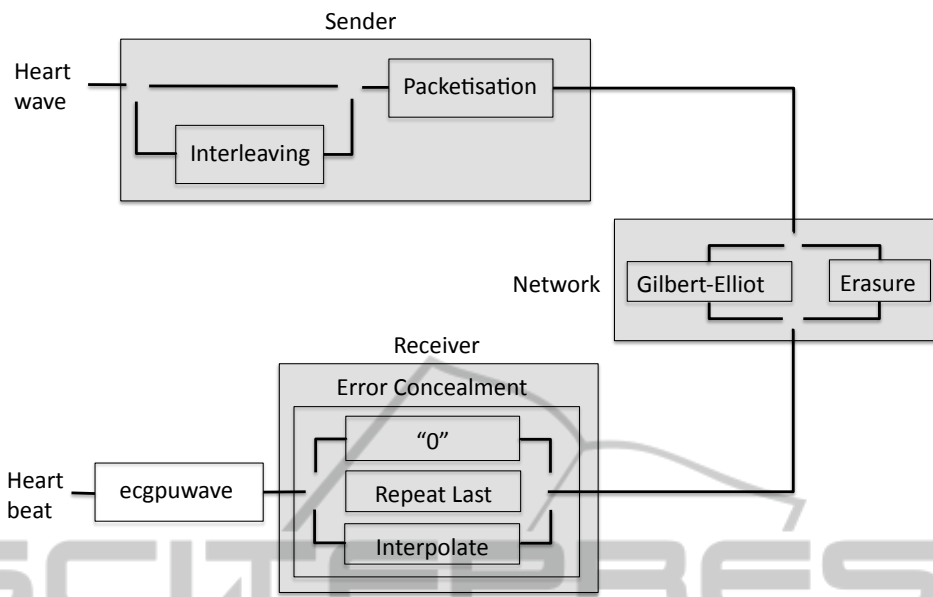


Figure 1: System Model.

sample per packet is efficiency, since each data packet sent on the network carries overhead due to several layers of in-band signaling. Additionally, some network may require some overhead per packet for accessing the resources. Hence, there is a trade-off between efficient network utilization and the effects of eventual packet losses.

The pattern of network error occurrence can also significantly influence the impact of network losses. The packet losses may occur randomly, as in Bluetooth links, or correlated in time, as in WiFi or cellular links. The effects of correlated packet losses can be more damaging than the effects of random losses, because correlated losses can cause the deletion of a significant part of the signal that is to be processed. In the specific case of heart wave and heart beat detection, the loss of various packets containing eventually more than one sample can cause a QRS complex to disappear. While this may not be very serious for heart beat detection, it may have significant impact in subsequent algorithms, like arrhythmia detection.

Finally, the receiver must decide how to replace the samples of the missing packets when rebuilding the data stream, since periodic samples are expected. The simplest approach is replacing the missing samples with zero. The research field of audio streaming offers a good starting point to look for more intelligent ways to deal with packet losses (Perkins et al., 1998). Several loss concealment techniques have been studied over the years, of which we address one sender-based technique, interleaving, and two receiver-based techniques, sample repetition and

interpolation of transmitted state, described in detail below.

4 PACKETIZATION OVERHEAD

The trade-off for risking the loss of multiple samples per packet is that it is more efficient to transmit multiple samples in a packet in terms of network resource usage, with side effects on the energy required for transmission. We define as overhead the ratio of application data, in this case bits of ECG samples, to the total transmitted data, i.e. including all the in-band signaling of the various protocol layers involved in the communication. To gain a better perception of the values involved, Table 1 shows the overhead for several packetizations used for transmission of MIT-BIH 11 bit samples using UDP (8 Byte header) over IPv4 over WiFi, or Bluetooth, both commonly used technologies for the wireless transmission of ECG data. For the Bluetooth calculations, we consider SCO packet types and HV1 profile for 1 sample per packet, and multiple HV2 packets for all other packetizations. The values in the table clearly show the advantage of transmitting multiple samples in each network packet, and only for more than 20 samples in each network packet does the overhead decrease below 50%.

Table 1: Network overhead for the chosen packetizations and commonly used network technologies.

	IP over WiFi	Bluetooth
1	92.6	88.8
2	86.3	87.6
5	71.5	68.9
10	55.6	67.5
20	38.5	34.9
50	20.1	16.4

5 NETWORK LOSS MODELS

The packet loss models of a network are characterized by the average packet loss rate and the time correlation between those losses. These models depend on a variety of parameters, ranging from the medium used (wireless vs. wired) to the topology and size of the network. Hence different types of networks show different packet loss behaviours.

Two models are commonly used for the generic characterization of network packet losses, namely the random independent loss model and the Gilbert-Elliott model. The first models packet losses as independent events, and is characterized by the average packet loss rate. The latter models packet losses as a two-state markov chain, assuming a dependency between loss events of consecutive packets. It is characterized by the loss probabilities in each state and the transition probabilities between the states.

6 LOSS REPAIR AND CONCEALMENT TECHNIQUES

At the receiver, the arriving packets are buffered to remove variations in the transmission latency across the network (jitter in networking jargon). Then, the data in the packets is used to rebuild a stream of periodic heart wave samples. When packets are lost, the corresponding missing samples must be replaced, so that the timing of the rebuilt stream is not disrupted and it contains periodic samples as expected by the subsequent algorithms. The approach taken to deal with missing samples at this step is called error concealment, a name that we borrow from the vocabulary of voice streaming. Some of these mechanisms rely on actions on the part of the sender to better empower the receiver at this step, and some others are purely receiver-based.

In sender-based techniques, the sender processes the information to be sent such that the transmission becomes resilient to some amount of errors. An alternative is that the sender re-transmits missing data trig-

gered by a request from the receiver, although this involves at least one full round-trip delay and additional buffering at the sender. The sender-based technique that we will focus on is called interleaving, although additional techniques can be tested in our framework. Interleaving consists in sending non-adjacent samples (in time) in each data packet and separating time-adjacent samples across several data packets. On the loss of a packet that carries more than one sample, the missing samples are not successive, thus transforming the loss of a large chunk of data (a packet) into the loss of the same amount of samples but spread across the number of packets involved in the interleaving process. The drawback of this technique is the delay that it introduces and the corresponding buffering requirements both at the sender and the receiver: enough data must be stored at the sender before generating a batch of packets.

As receiver-based error concealment techniques we illustrate two insertion techniques, substitution with "0" and with the previous sample, and one interpolation technique. In the first case, any missing sample is replaced with a value equivalent to 0 or with the last correctly received sample, respectively ("0" or "Repeat Last" in Figure 1). In the case of interpolation, each sample is replaced with the linear interpolation between the previous and following correctly received samples. Linear interpolation is more costly in terms of computation than simple insertion techniques.

7 METHODOLOGY AND PARAMETERS

We carried out extensive simulations to assess the impact of network transmission losses on the accuracy of the well-known heart beat detection algorithm, *ecg-puwave* (Pan and Tompkins, 1985). We used various packetizations and varied the quality of network transmission, i.e., the average packet loss rate. For each case, we used one of the three error concealment techniques described above. Additionally, we used interleaving with the basic error concealment case ("0"). We set off simulating the case of uncorrelated transmission losses, which is the best case scenario. That is, correlated losses will cause more damage to the rebuilt data stream, so that the results shown here represent the best expected performance in case of a specific amount of network losses. The parameters used in the study are summarized in the Table 2.

We evaluated the impact on the performance of the heart beat detection algorithm by comparing the sensitivity and the positive predictive value (PPV)

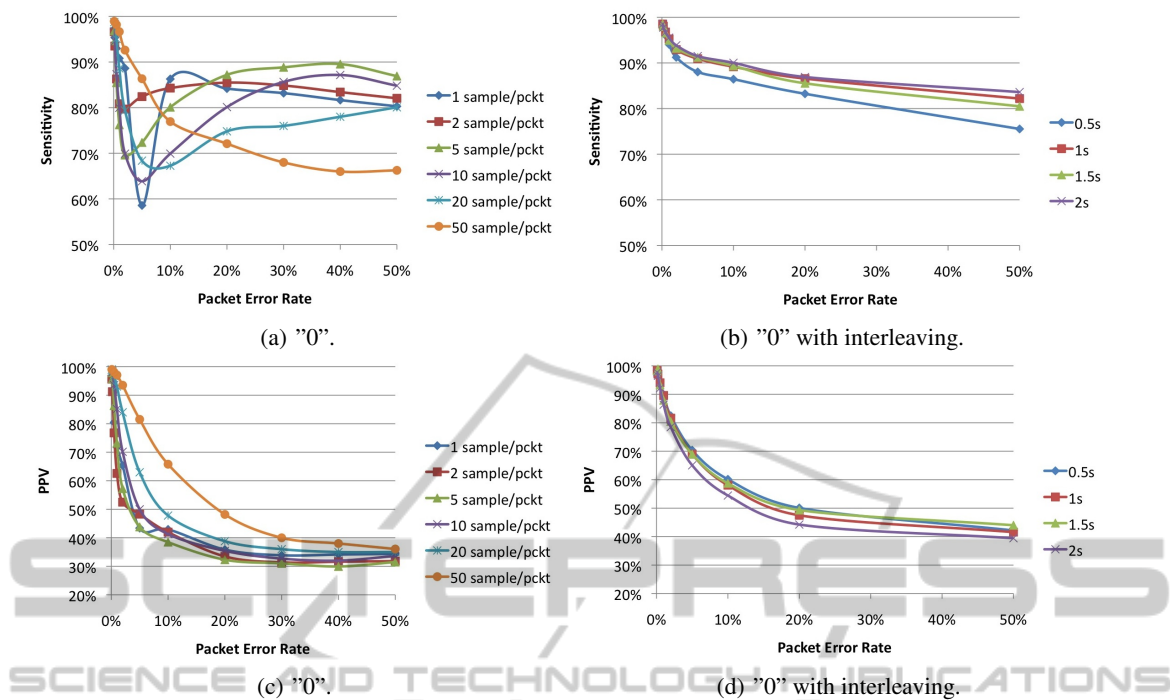


Figure 2: Sensitivity and PPV with interleaving for random transmission losses.

Table 2: Parameter space explored for the results.

Packetization [# samples]	{1, 2, 5, 10, 20, 50}
Interleaving	On/Off
Packet loss rate	$\in [0.1; 50]\%$
Error concealment	"0", "Last", "Interpolation"

obtained for an ECG stream rebuilt after suffering packet losses with the values obtained for the same ECG stream that did not suffer losses. The sensitivity expresses the rate of all existing QRS complexes that are detected, whereas the PPV expresses the rate of detected QRS complexes that do not exist in the original ECG stream. We use the MIT-BIH arrhythmia database (Moody and Mark, 1990) and the ecg-wave implementation in the PhisioToolkit (Moody et al., 2000).

8 RESULTS

The reference values for comparing the impact of samples losses are the specificity and PPV of the heart beat detection algorithm without any losses, which are 99.1% and 99.33%, respectively. Figure 2 shows the specificity and PPV for simple replacement of missing samples with "0", without and with interleaving, in the presence of uncorrelated network errors. Simply substituting the missing samples causes an er-

atic behavior of the heart beat detector in terms of sensitivity and the PPV degrades to values below 90% even for low amount of losses. This large amount of falsely detected beats is caused by the large amount of steep slopes introduced when replacing missing samples with values close to 0. Spreading the missing samples in time, achieved by interleaving samples before packetization at the sender, maintains the sensitivity and PPV above 90% for random network losses up to 1%, demonstrating the potential of this technique.

Figure 3 shows the results for insertion with previous correct sample and linear interpolation without interleaving. Oppositely to replacing missing samples with "0", replacing each sample with the last correctly received value shows negligible performance degradation (sensitivity and PPV larger than 99%) of the heart beat detection algorithm for up to 1 sample per packet and up to 50% network packet losses. On the other hand, as expected, larger packetizations tolerate less network losses, namely 2% for 10 sample packetization and only 0.5% for 20 samples per packet. Finally, replacing missing samples with a value resulting from interpolation using the nearby correctly received samples provides only 0.5% better sensitivity and PPV than insertion with "Last" for more than 5% losses, despite the additional computational complexity involved in the latter concealment technique.

Table 3 shows the maximum usable packetization

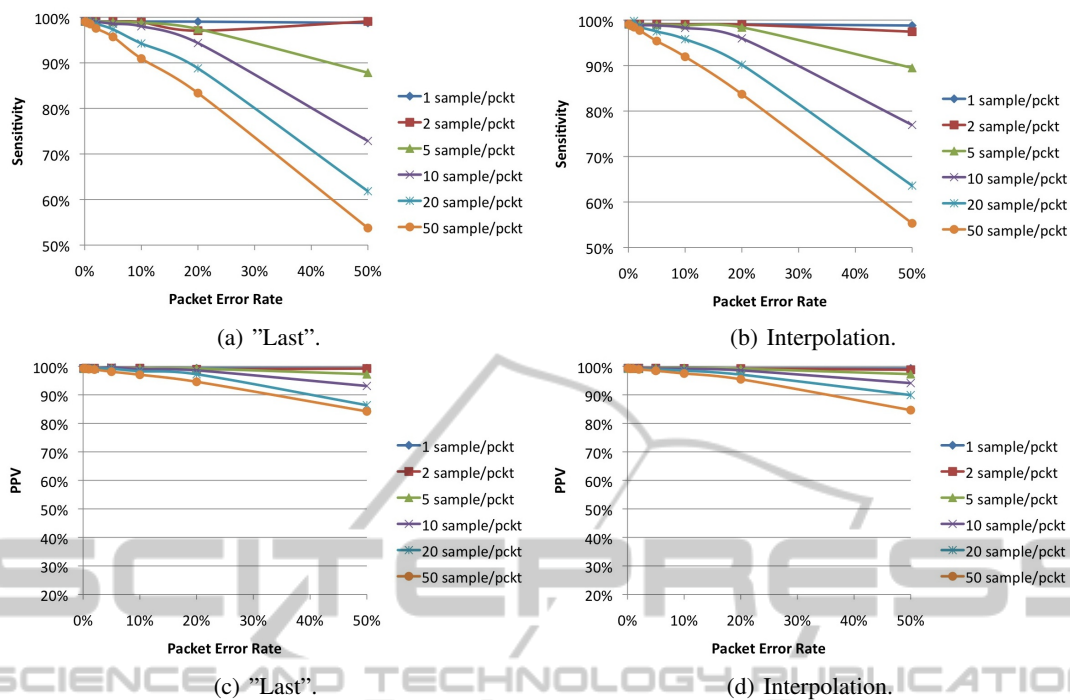


Figure 3: Sensitivity and PPV for random transmission losses.

Table 3: Maximum packetization to guarantee sensitivity and PPV above 99%.

Packet Loss Rate [%]	"0"	"Last"	Interpolation
0.1	-	50	50
0.2	-	20	20
0.5	-	20	10
1	-	10	10
2	-	10	5
5	-	2	5
10	-	1	2
20	-	1	2
50	-	1	1

to guarantee sensitivity and PPV above 99% for each error concealment technique used, showing that none of the studied techniques performs better than the other in all situations. Specifically, using "Last" for error concealment is more efficient for networks with low packet losses whereas the additional complexity of linear interpolation pays off for less reliable networks. From the perspective of network efficiency, however, the combinations of packetizations and error concealment techniques for which the well-known ecgwave algorithm would perform acceptably imply transmission overheads of more than 50% (see table 1), and are extremely inefficient and energy costly.

9 DISCUSSION

Although our results show that it is feasible to transmit ECG data across wireless links with currently available technologies for post-processing by signal processing algorithms, e.g., heart beat or arrhythmia detection, they do not provide efficient and reliable operation. Due to practical considerations, like patient comfort and usability, ECG monitoring devices are usually resource constrained both in terms of processing and available energy. An efficient use of these resources is then critical in ECG monitoring system design. Our evaluation clearly shows that this is not possible today with state-of-the-art technologies. Next, we describe three fields that we believe should be explored targeting specifically the transmission of ECG data for automatic post-processing solutions.

Firstly, the framework that we present and the associated parameter space needs to be further evaluated, and the fundamental trade-offs involved in the choice of transmission technologies, packetizations, loss concealment techniques, etc. must be studied for varied network scenarios. Emphasis shall be put in a joint optimization of the parameters involved in the transmission of ECG data to achieve highest network and energy efficiency, conditioned on guaranteeing minimum performance levels of the signal processing algorithms.

Another line of research that will produce relevant insights is the development of loss concealment techniques to efficiently repair the ECG stream at the receiver, with or without the cooperation of the sender. We specifically envision the use of linear prediction, Kalman filters or other adaptive filters to reconstruct the ECG signal. Although this may not provide a strong improvement over simpler techniques for the purpose of heart beat detection, it shall play a significant role in the performance of subsequent, more elaborate algorithms, like arrhythmia detection.

Taking a holistic view of the problem, we further propose the development of network-aware signal processing algorithms that are either resilient or can adapt to certain levels of sample loss. We envision the application of non-uniform sampling mechanisms and results from the field of compressed sensing.

10 CONCLUSIONS

We address the often ignored problem of transmission of biomedical signal data across networks for remote processing, proposing a framework that models the relevant building blocks of such a system. We use the framework to perform an initial numerical evaluation of the impact of uncorrelated random network packet losses in the performance of the well-known heart beat detection algorithm ecgpuwave using the MIT-BIH database. Our results show that 1) packet losses cause significant degradation of the heart beat detection algorithms; 2) simple loss concealment techniques, like insertion of last known sample and linear interpolation, significantly reduce the impact of network losses, but their performance depends on the packetization used; 3) packetization constitutes an important parameter to choose the trade-off amongst network and energy efficiency and impact of packet losses; 5) there is not one combination of packetization and loss concealment technique that performs best for all network scenarios studied.

As a consequence of these findings, we identify the need to further research the transmission of data from biomedical signals across networks and propose to deepen the understanding of the applicability of three fields of research to biomedical signal transmission and processing. Namely, 1) the joint optimization of transmission parameters, 2) the development of advanced loss concealment techniques, like Kalman filters and linear prediction, and 3) the development of loss-resilient signal processing algorithms, leveraging results from compressed sensing or non-uniform sampling theory.

ACKNOWLEDGEMENTS

The authors thank Miguel Coimbra and Can Ye for fruitful discussions.

This work was supported by FCT (Fundação para a Ciência e a Tecnologia) through the VR (Vital Responder) project (within the CarnegieMellon—Portugal program. ref. CMU-P/CPS/0046/2008).

REFERENCES

- Alesanco, A. and Garca, J. (2010). Clinical assessment of wireless ecg transmission in real-time cardiac telemonitoring. *IEEE Transactions on Information Technology in Biomedicine*, 14(5):1144–1152.
- Hu, X., Wang, J., Yu, Q., Liu, W., and Qin, J. (2009). A wireless sensor network based on zigbee for telemedicine monitoring system. In *The 2nd International Conference on Bioinformatics and Biomedical Engineering*, pages 1367–1370.
- Moody, G. and Mark, R. (1990). The mit-bih arrhythmia database on cd-rom and software for use with it. In *Computers in Cardiology*, pages 185–188.
- Moody, G., Mark, R., and Goldberger, A. (2000). Physionet: a research resource for studies of complex physiologic and biomedical signals. In *Computers in Cardiology*, pages 179–182.
- Pan, J. and Tompkins, W. (1985). A real-time qrs detection algorithm. *IEEE Transactions on Biomedical Engineering*, 32(3):230–236.
- Pandian, P. S., Safeer, K. P., Gupta, P., Shakunthala, D. T., Sundersheshu, B. S., and Padaki, V. C. (2008). Wireless sensor network for wearable physiological monitoring. *Journal of Networks*, 3(5).
- Perkins, C., Hodson, O., and Hardman, V. (1998). A survey of packet loss recovery techniques for streaming audio. *IEEE Network*, 12(5):40–48.
- Prieto-Guerrero, A., Mailhes, C., and Castanié, F. (2007). Lost sample recovering of ecg signals in e-health applications. In *The 29-th Annual International Conference of the IEEE EMBS*, pages 31–34.
- Stuart, E., Moh, M., and Moh, T. S. (2008). Privacy and security in biomedical applications of wireless sensor networks. In *First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, pages 1–5.
- Theera-Umpon, N., Phiphatkhunarnon, P., and Auephanwiriyaikul, S. (2008). Data reconstruction for missing electrocardiogram using linear predictive coding. *IEEE International Conference on Mechatronics and Automation (ICMA)*, pages 638–643.