

Load Control Scheme to Preserve Processing Capacity for Emergency Biometric Data

Sehrish Malik, Boo-Hyung Lee, and Jong-Hyouk Lee

Protocol Engineering Lab., Sangmyung University
Cheonan, Republic of Korea

Email: {serry, boohyung, jonghyouk}@pel.smuc.ac.kr

Abstract—A significant increase in ageing population is seen in past ten years. Recent advances in wireless sensor networks and wireless body area networks have paved the way for remote health monitoring. With remote health monitoring devices, patients and caretakers are enabled to keep track of patient's health status each second and provide immediate treatment to the patient in case of any emergency. Reliability of such devices is a big concern as any delay or drop of biometric data transmission can put patient's life at risk. In this paper, we propose a load control scheme to provide reliable communications for emergency data. Thanks to reserved capacities for emergency data in the proposal, the packet dropping probability for emergency data is much lower than the no load control scheme.

I. INTRODUCTION

Nearly all the countries of the world are about to face the ageing population issue. A decrease in rate of mortality and a decrease in rate of birth are the factors, which result in ageing population. On the other hand, the number of seniors in the world is rapidly increasing. According to [1], people aged 60 or over had 9.2 percent stake in total population in 1990 that rose to 11.7 percent in 2013. It will grow to 21.2 percent by 2050. Population ageing requires proper measures to be taken so that old aged people could be provided with the best healthcare systems. Since a focus has been shifted from young to old aged people, the pressing need of the hour is to put the best efforts in preparing healthcare systems, which can take care of seniors in every situation.

The health issues associated with old aged people are very critical most of the time. Chronic medical conditions put many seniors' lives at stake. Constant care is needed for old aged people with such diseases. Every second is very precious for them as their health condition can go worse at any second. Hence, such patients (e.g., old aged people) need to be provided with the facilities of sufficient healthcare monitoring devices.

When a patient uses a healthcare monitoring device, the device collects vital signals from a patient's body via sensors and sends them to a remote healthcare monitoring server usually located at a hospital. Signals indicate the health status of the patient. At any given time, a patient could be going through a critical stage. Therefore, it is important to make sure that a patient's critical healthcare information is transferred in the shortest possible time and in a reliable fashion to avoid any delay in the patient's treatment.

In this paper, we present a load control scheme designed to provide reliable communications for emergency biometric

data. In the proposed scheme, a predefined value is used to preserve processing capacity for emergency biometric data at a healthcare monitoring device. This reserved capacity will decrease the dropping probability of the emergency packets and make the service of the health monitoring devices more reliable for the patient in emergency cases.

The rest of this paper is as follows. Section II presents the related work and the proposed load control scheme is introduced in Section III. In Section IV, the proposed scheme is analysed and compared with the no load control scheme (i.e., default scheme). Analysis results are presented in Section V. Section VI concludes this paper.

II. RELATED WORK

The concept of remote healthcare monitoring has been introduced more than a decade ago which suggests the method of monitoring a patient's health condition by providing bidirectional communication between patients and caretakers [2]. Recent advances in a wireless sensor network have made it feasible to implement functionalities of remote healthcare monitoring for patients. A wireless sensor network provides ease and efficiency in communication along with advance monitoring, automation, and control [3].

A typical remote healthcare monitoring consists of three tiers. The first tier is a body area domain, the second tier is a communication and network domain, and the third is a service domain. The body area domain can be implemented with a number of wireless body area networks. It is composed of sensors measuring biometric data from the body and a personal server (e.g., smartphone). The communication and networking domain acts as an intermediary between the body area network and the service domain. It passes the data signals received from the body area domain to the service domain via Wi-Fi or LTE. The service domain is a trusted authority maintaining a remote health monitoring server responsible for receiving, recording, and analysing patients' healthcare information [4].

An extensive assessment regarding the needs and requirements of ubiquitous healthcare has been presented in [5]. It reviews and compares the hardware, communication, and computing of remote healthcare monitoring so that better improvements can be offered for the future.

Not much research has been conducted specifically for preserving processing capacity for emergency biometric data. For instance, it has been discussed in combination with other main focuses, such as a deployment of wireless body network in different possible environments, scenarios, or integration

with other environments. In [4], ViiCare was proposed to provide high quality healthcare services to patients. ViiCare has been made taking in consideration the factors of low delivery rate and reduced costs. A low delivery rate will increase its reliability while a reduced cost will make it affordable to more number of users. In [6], studies have been done for the deployment of cloud-enabled architecture by checking the feasibility of its applications in pervasive healthcare through various mechanisms.

III. PROPOSED LOAD CONTROL SCHEME

A. Considered Scenario

We consider a heart rate monitoring device that enables one to record his/her heart rate in real time, or record the heart rate for later study. It consists of two elements: a chest strap transmitter and a personal server (e.g., smartphone or wrist receiver). The chest strap transmitter is a wearable monitoring device, which users wear, to send data to a personal server. Biometric data from the device is sent to a personal server, which can be loaded with different data packets at any given time. Thus, a proper load control is desirable at the personal server to avoid any unwanted delay in processing emergency biometric data to be sent to a remote healthcare monitoring server located at a hospital. Note that the personal server is assumed to be equipped with LTE and WiFi.

The upper and lower thresholds for the heart rate of a patient are used to determine whether the patient is in emergency cases or not. According to the American Heart Association, the target heart rate zone of a person is in between 50 percent and 85 percent of his/her maximum heart rate [7]. Commonly, the maximum heart rate is calculated by subtracting a patient's age by 220. The upper and lower thresholds are thus given in Eqs. (1) and (2) respectively:

$$\alpha = (220 - age) \times 0.50 \quad (1)$$

$$\beta = (220 - age) \times 0.85 \quad (2)$$

where age is the patient's age. The given formulas work fine for the age of people under 40 but to find out the maximum heart rate for old aged people, it is recommended to multiply the age by 0.75 and then subtract from 208 as follows:

$$\beta' = (220 - (0.75 \times age)) \times 0.85. \quad (3)$$

B. Load Control Procedure

The heart rate monitoring device collects biometric data through a sensor and then categorizes the collected biometric data as an emergency data packet P_E if the data does not fall into the range $[\alpha, \beta]$ or as a normal data packet P_N if the data falls in the range. Fig. 1 shows the load control procedure in which categorized data packets come from the heart rate monitoring device into the personal server to be processed.

As shown in Fig. 1, the load control procedure is designed to preserve processing capacity for P_E by defining a predefined value K . Let C_{used} be the number of data packets being processed in the personal server. Let C_{total} be the total capacity in terms of data packets at the personal server. Then, $(C_{total} - K)$ is the processing capacity reserved only for P_E . For P_E , LTE is used as a means of transmission media, whereas WiFi is used to transmit P_N to the remote healthcare

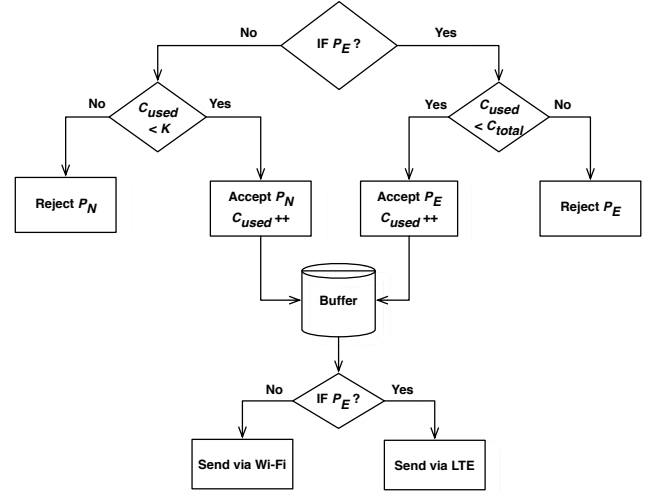


Fig. 1: Load control procedure at the personal server.

monitoring server. Note that we assume that LTE is a reliable transmission media compared with WiFi.

IV. PERFORMANCE ANALYSIS

In this section we analyze the performance of the proposed load control scheme. The emergency packet dropping probability P_{EPD} and the normal packet blocking probability P_{NPB} are considered.

A. Assumption

The following assumptions are made regarding the arrival and processing rates for P_E and P_N with offered loads:

- The arrivals of P_E and P_N to the personal server follow Poisson distributions with rates of λ_E and λ_N , respectively.
- The processing times of P_E and P_N (i.e., the residence time of a packet at the personal server) are exponentially distributed with means of $1/\mu_E$ and $1/\mu_N$, respectively.
- The total offered load at the personal server ρ_T is the sum of the emergency packets' load $\rho_E = \lambda_E/\mu_E$ and the normal packets' load $\rho_N = \lambda_N/\mu_N$.

B. Markov Chain Model

Similar to [8], a one-dimensional Markov chain is used to analyze the proposed load control scheme compared with the no load control scheme (i.e., default scheme).

State i in the Markov chain model denotes the total number of packets in a personal server, including P_E and P_N . Suppose $q(i, j)$ represents the transition rate from state i to state j .

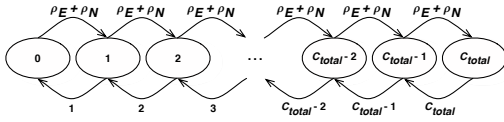


Fig. 2: No load control.

1) *No Load Control Scheme*: With the no load control scheme, packets are dealt without differentiating between P_E and P_N . No threshold is maintained for P_E . All packets are accepted to process regardless of the number of packets until C_{total} . It can thus cause dropping of packets when the arrival rate of packets is high. It can also increase the packet processing time, causing unwanted delay. Fig. 2 shows the one-dimensional Markov chain for the no load control scheme.

The transition rates for the no load control scheme are as follows:

$$q(i, i+1) = \rho_E + \rho_N, \quad (0 \leq i < C_{total}) \quad (4)$$

$$q(i+1, i) = i+1, \quad (0 \leq i < C_{total}) \quad (5)$$

where $q(i, i+1)$ and $q(i+1, i)$ are the transition rate from state i to state $i+1$ and the transition rate from state $i+1$ to state i , respectively. The no load control scheme considers both ρ_E and ρ_N in every state transitions until C_{total} is full. The steady state probability for the no load control scheme p_k is obtained as follows:

$$p_k = \frac{(\rho_E + \rho_N)^k / k!}{\sum_{n=0}^{C_{total}} (\rho_E + \rho_N)^n / n!}, \quad (0 \leq k < C_{total}). \quad (6)$$

For the no load control scheme, P_{EPD} and P_{NPB} are thus obtained as:

$$P_{EPD} = P_{NPB} = \frac{(\rho_E + \rho_N)^{C_{total}} / C_{total}!}{\sum_{n=0}^{C_{total}} (\rho_E + \rho_N)^n / n!}. \quad (7)$$

2) *Proposed Load Control Scheme*: When C_{used} (i.e., used capacity at the personal server) crosses K , only P_E is accepted at the personal server and P_N is rejected. P_E is rejected only when C_{used} is equal to C_{total} . In other words, for P_N , it is blocked when C_{used} is equal to K , whereas P_E is only dropped when C_{used} is equal to C_{total} . Figure 3 depicts the Markov chain model for the proposed load control scheme.

The transition rates for the proposed load control scheme are as follows:

$$q(i, i+1) = \rho_E + \rho_N, \quad (0 \leq i < K) \quad (8)$$

$$q(i+1, i) = i+1, \quad (0 \leq i < K) \quad (9)$$

$$q(i, i+1) = \rho_E, \quad (K \leq i < C_{total}) \quad (10)$$

$$q(i+1, i) = i+1, \quad (K \leq i < C_{total}) \quad (11)$$

where ρ_E and ρ_N are considered when $0 \leq i < K$ (i.e., K is not reached), but when $K \leq i < C_{total}$, only ρ_E is considered.

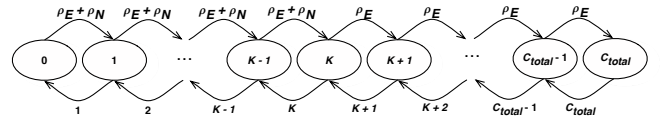


Fig. 3: Proposed load control.

Now, the steady state probability for the load control scheme p_k can be expressed as follows:

$$p_k = \frac{(\rho_E + \rho_N)^k / k!}{\sum_{n=0}^K (\rho_E + \rho_N)^n / n! + \sum_{n=K+1}^{C_{total}} (\rho_E)^{n-K} (\rho_E + \rho_N)^K / n!}, \quad (0 \leq k < K). \quad (12)$$

$$p_k = \frac{(\rho_E)^{k-K} (\rho_E + \rho_N)^K / k!}{\sum_{n=0}^K (\rho_E + \rho_N)^n / n! + \sum_{n=K+1}^{C_{total}} (\rho_E)^{n-K} (\rho_E + \rho_N)^K / n!}, \quad (K \leq k < C_{total}). \quad (13)$$

Then P_{EPD} and P_{NPB} of the proposed load control scheme can be determined by Eqs. (14) and (15), respectively.

$$P_{EPD} = \rho_{C_{total}}, \quad (14)$$

$$P_{NPB} = \sum_{k=K}^{C_{total}} \rho_k. \quad (15)$$

V. ANALYSIS RESULTS

In this section, numerical analysis results are presented. C_{total} at the personal server is assumed to be 50. λ_N is set as 0.06, whereas λ_E is set as 0.03. μ_N and μ_E are varied from 20 ms to 700 ms.

A. Effect of Normal Packets' Load

First we analyze how ρ_N affects the overall performance of the proposed load control scheme in comparison to the no load control scheme.

Variations of P_{NPB} are shown in Figure 4. We can see that the no load control scheme has a lower P_{NPB} than the load control scheme because the proposed load control scheme reserves some capacities for P_E . So, in the proposal, P_{NPB} is higher as P_N is not accepted once K is reached. As such, P_{NPB} in the proposal is also increased as K decreases.

Figure 5 depicts variations of P_{EPD} as ρ_N increases. Compared with the no load control scheme, the proposed load control scheme provides much lower of P_{EPD} because of reserved capacities for P_E . In addition, the proposal increases P_{EPD} at a low rate and is almost consistent unlike the no load control scheme.

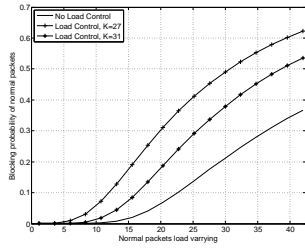


Fig. 4: P_{NPB} vs. ρ_N

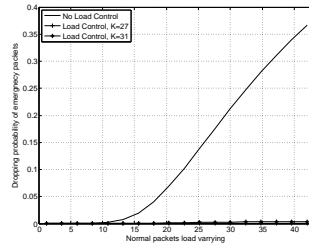


Fig. 5: P_{EPD} vs. ρ_N

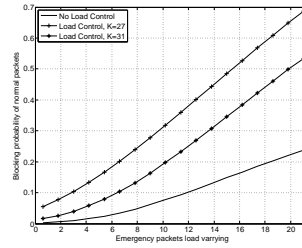


Fig. 6: P_{NPB} vs. ρ_E

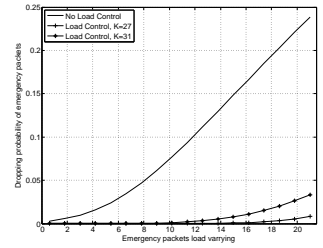


Fig. 7: P_{EPD} vs. ρ_E

B. Effect of Emergency Packets' Load

We observe the performance of the proactive load control scheme in comparison to no load control scheme when ρ_E is varied between the defined ranges, while keeping ρ_N at average, i.e., $720/2 = 360$.

Figure 6 shows that P_{NPB} increases as ρ_E increases for the both schemes. Similar to the results shown in Figure 4, the proposed load control scheme causes higher of P_{NPB} due to the reserved capacities for P_E . Though P_{NPB} in this case is higher than no load control scheme but it is still a better approach to block more P_N in order to save more P_E from dropping.

Figure 7 depicts variations of P_{EPD} as ρ_E increases. Similar to the results shown in Figure 5, the proposed load control scheme provides better performance compared with the no load control scheme as the proposed one reserves some capacities for P_E . With the increase of K , P_{EPD} also increases as the increased value of K means less capacity being reserved for P_E .

VI. CONCLUSION

Recent advances in wireless sensor networks and wireless body area networks have made previously considered impossible options for e-healthcare come true. It is necessary to provide reliable and cost effective methods to patients so that everyone can avail e-healthcare services without delay when reporting a patient's health condition to his/her caretaker. In this paper, we introduced a load control scheme designed to provide reliable communications for emergency biometric data. In the proposal, biometric data is categorized into normal and emergency data, and some capacities are reserved only for emergency data. Thanks to the reserved capacities, the packet dropping probability for emergency biometric data is much lower than the no load control scheme (i.e., default scheme). The upcoming e-healthcare structure will require not only reliable data transfer, but also data to be authenticated between devices. We are planning to apply the load control scheme in authentication systems for e-healthcare.

ACKNOWLEDGMENT

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea

(NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2014R1A1A1006770).

REFERENCES

- [1] United Nations, "World Population Ageing Report," 2013.
- [2] S. J. Brown, "Remote health monitoring and maintenance system," *U.S. Patent*, No. 6168563, Jan. 2001.
- [3] A. Dunkels and J. Vasseur, "IP for smart objects," *Internet protocol for smart objects (IPSO) alliance: White paper*, 2008.
- [4] X. Liang, X. Li, M. Barua, L. Chen, R. Lu, X. Shen, and H. Y. Luo, "Enable pervasive healthcare through continuous remote health monitoring," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 10–18, 2012.
- [5] F. Touati and R. Tabish, "U-healthcare system: State-of-the-art review and challenges," *Journal of medical systems*, vol. 37, no. 3, 2013.
- [6] J. Wan, C. Zou, S. Ullah, C.-F. Lai, M. Zhou, and X. Wang, "Cloud-enabled wireless body area networks for pervasive healthcare," *IEEE Network*, vol. 27, no. 5, pp. 56–61, 2013.
- [7] <http://www.livescience.com/42081-normal-heart-rate.html>
- [8] S. Pack, B. Lee, and Y. Choi, "Proactive load control scheme at mobility anchor point in hierarchical Mobile IPv6 networks," *IEICE TRANSACTIONS on Information and Systems*, vol. 87-D, no. 12, pp. 2578–2585, December 2004.