Practical Sensor Network Management Technology for Healthcare Applications

Noriharu Miyaho, Tatsuro Nakamura, Takamasa Shimada, and Noriko Konno
Graduate School of Information Environment Technology
Tokyo Denki University (TDU)
2-1200, Muzai Gakuendai, Inzai, Chiba, Japan
e-mail: miyaho@sie.dendai.ac.jp, m7dec5c896sj8@t.vodafone.ne.jp, shimada@sie.dendai.ac.jp, konno@sie.dendai.ac.jp

***Abstract*—The implementation of telemedicine can make use of a sensor network that carries users' biometric information, as collected by tiny intelligent sensors attached to the human body. We propose a communication system that can be used for telemedicine to improve healthcare and quality of life by making use of bio-sensors, a sensor network and a database with mutual authentication to ensure security. This paper also describes the priority control mechanism in the sensor network, the experimental results, and clarifies the real-time performance of the proposed communication sensor network system.**

Keywords - healthcare, telemedicine, real-time processing, sensor, security, healing, ID-Based key sharing, EEG.

I. INTRODUCTION

Recently, the relaxing effects of visible light and aroma have been attracting attention. A network service in which aroma generators installed at users' locations are remotely controlled through the network has been proposed [1]-[3]. We expect that pain clinic doctors will be able to provide a health care service over the network using a combination of light and aroma. We have investigated a "healing" communication system in order to improve patients' quality of life (QoL). The system uses an aroma generator and a light wavelength controller, both of which are remotely controllable. We implemented a prototype system, and made both psychological and physiological measurements using an electroencephalogram (EEG).

First, the psychological effect of colour was examined in order to determine the actually comfortable healing environments. We examined the effect of different colors in lighting using a 7-point Likert scale from the viewpoint of mental health and the psychological effects that different visible light colors provide. The result is shown in Figure 1. The general evaluation for a healing effect was highest for the green light and the factor ratings were: Happiness factor (5.2625), Popularity factor (4.901), Healing factor (4.886), and Rest factor (4.781). The evaluation for restfulness was highest for blue light, with these factor ratings: Rest factor (4.946), Popularity factor (4.585), Healing factor (4.272), and Happiness factor (3.537), as shown in Figure 1 [4].

EEG is often used in a variety of fields to evaluate multiple cerebral states. It is well known that a specific EEG waveform is generated when the subject is in a specific state [5]. For example, in psychiatry, sleep stages and mental illnesses are diagnosed by their characteristic EEG waves [6].

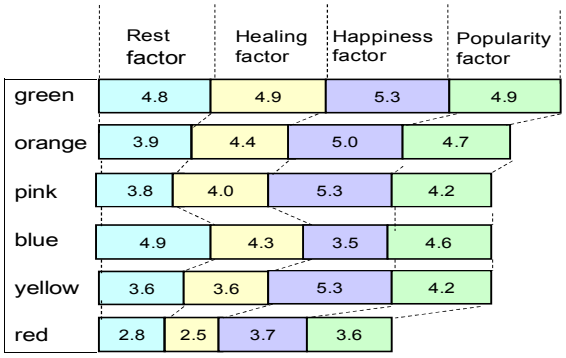

Figure 1. Mental Health factors of visible light color

For state conditions such as healing, it is well known that alpha and beta waves provide important evidence for medical diagnosis. The existence of alpha waves in an EEG has a strong correlation with the relaxation of a subject with eyes closed. Conversely, the existence of beta waves in an EEG has a strong correlation with a state of active concentration or excitement.

In our previous study, to estimate the healing effect of certain kinds of stimulation, we considered the presence of alpha waves in EEG records.

In our experiment, the international 10-20 system was used for EEG measurements and referential derivation was applied. The EEG data at electrode O1, where alpha waves are best observed, were used. The EEG data were sampled (at a rate of 200 Hz) with a 0.64 sec (128-point) Hamming window. Its logarithmic power spectrum coefficients were calculated by FFT and the spectral range of alpha waves (from 8 to 13 Hz) was used for analysis.

We found that the healing effect on subjects is larger when a specific combination of stimuli (lavender aroma, blue light, and music) is given to patients than when only a single stimulus is given. However, we found that green LED lighting also gives a significant human body healing effect when the brightness of the LED light was controlled to make the brightness vary inversely with frequency [7][8].

In this experiment, we compare the power of alpha waves recorded from subjects after irradiation for five

minutes by green LED light with a continuous spectrum and also with light having a 1/f fluctuation. The number of subjects was 4. The values of the power of alpha waves of all subjects were averaged. Figure 2 shows the results of this experiment. The power in the alpha wave band after irradiation by green LED light with 1/f fluctuation was higher than that after exposure to a continuous spectrum. In particular, the power for two subjects showed a significant difference ($p=0.05$). This result indicates that green light with a 1/f fluctuation has a healing effect.

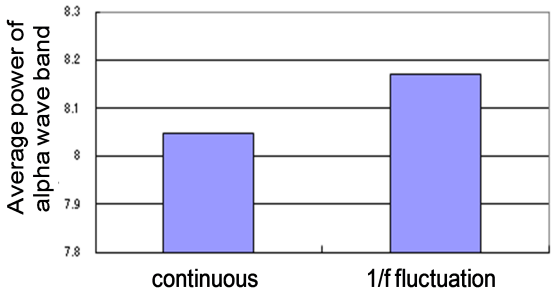

Figure 2. The average power in the alpha wave band versus the light exposure spectrum

We verified the corresponding effects using physiological and psychological techniques [2].

It will be possible to realize the above-mentioned healing environments inside a patient's premises via a network.

Currently, there is no objective method of evaluating the above-mentioned environments, although they will in the future be used to deliver "telemedicine". Therefore, healing communication systems that are reliable enough for use in commercial applications are yet to be developed. Our final goal is to realize healing environments and safe telemedicine services by making use of sensor networking technology and biomedical sensor node communication technology with a high level of security.

We proposed a mutual authentication method which relies on GPS (Global Positioning System) information [9][10]. Figure 3 shows the mechanism of this mutual authentication method. In conventional telemedicine, the hospital authenticates patients, to prevent leakage of personal information, but the patient does not authenticate the hospital.

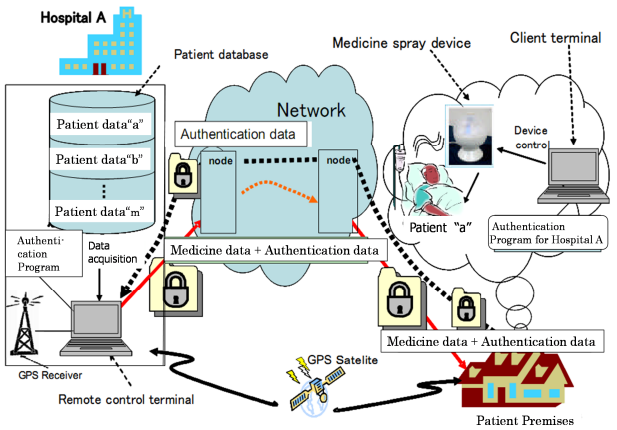

Figure 3. Proposed mutual authentication mechanism

Today, the patient should be able to authenticate the hospital because there is the potential of spoofing of the hospital and because authentication is necessary to ensure the security of network services. A reliable mutual authentication method can be realized by effectively combining GPS information, passwords, IDs, etc.

A secure remote diagnosis service can also be achieved by not only using a combination of GPS information and the user's and the hospital's passwords but also encrypting ID codes that are transmitted over the network. Today, the level of location precision determined by GPS is in the range of several centimeters, so GPS can be reliably used for authentication.

Examples of authentication data being exchanged by the patient and the hospital before any treatment commences are shown in Figure 3. Information sent by the hospital contains authentication information as well as the prescription. Information sent from the client contains authentication information and data about the patient's current physical condition, such as blood pressure and temperature.

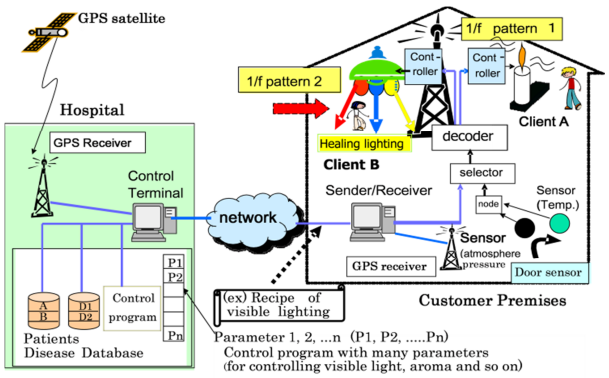

Figure 4. Telemedicine system for healing environment

Figure 4 shows the concept of the proposed telemedicine system for realizing a more comfortable and effective healing environment. The remote hospital has the individual patient's database and a disease-related database, which provide the appropriate recipe to control the visible

light brightness, aroma type, 1/f fluctuation type, and so on, in the remotely located patient's premises. These various kinds of stimulation need to be properly selected, to take account of the patient's current physical and mental condition. The control program has many different parameters for controlling the visible light. Environment sensor information such as the temperature, atmospheric pressure, and humidity will also be utilized to assess the patient's environmental conditions accurately. The patient's physical parameters such as brain waveforms, blood pressure, heart rate, and so on can be fed back by making use of a high speed network and the sensor network. By utilizing this network mechanism, the optimum combination of stimuli can be appropriately and dynamically provided in real time, improving the patient's physical and mental condition. The hospital, or other organizations related to various medical treatments, and the patient's premises can be mutually authenticated by the use of detailed information provided by a GPS information system to ensure security.

Even if the patient is being transported in an ambulance, the patient and the hospital can authenticate each other using a GPS database. Furthermore, mutual authentication can be applied between hospitals to establish a communication link and to prevent a situation in which two hospitals might both provide the same prescription to the same patient.

The remainder of this paper is structured as follows. In Section II, we describe the practical healing communication system which makes use of an ID-based key sharing scheme. Then, in Section III, we clarify the performance evaluation results obtained when using the proposed priority control mechanism and the sensor database efficiently using a stream cipher. Finally, we provide our conclusions from these studies in Section IV.

Encrypted data

AAuthentication Header			Prescription
Hospital Identification ID	Hospital password	Hospital GPS Information	Recipe data for prescription
ID 1	Pass1 s1	(X_1,Y_1,Z_1)	R_1
⋮	⋮	⋮	⋮
ID N	PassN	(X_N,Y_N,Z_N)	R_N

Encrypted data

Authentication Header			Patient biomedical data
Patient Identification ID	Patient password	Patient premises (GPS information)	Blood pressure, pulse wave, temperature
id 1	p 1	(x_1,y_1,z_1)	Data 1
⋮	⋮	⋮	⋮
id m	p m	(x_m, y_m, z_m)	Data m

Figure 5. Examples of authentication data formats

II. HEALING HEALTHCARE COMMUNICATION SYSTEM

If the proposed system is to be used for medical treatment, the following requirements must be met. First, the health care organization, for example a hospital, must prevent the leakage of personal information. Second, from the user's standpoint, reliable mutual authentication is necessary. The proposed system achieves reliable authentication using the position information from a GPS system in addition to a user ID and a password.

1) Configuration of the proposed system

The configuration of the proposed system is shown in Figure 6. The system is composed of a Monitoring Centre and a Remote Node. The former is equipped with a GPS device, a sensor database and a recipe database. The Remote Node is equipped with a sensor node, which includes a GPS device and a pulse wave sensor which measures the user's biometric data, and a Gateway Node, which controls actuators such as an aroma generator and a light wavelength controller according to a recipe received from the Monitoring Centre, after mutual authentication has been established with the Centre.

The operational procedure applied to the proposed system is as follows.

(1) A medical specialist in both aroma and lighting accesses the Recipe Database, and selects the appropriate healing recipe data for individual users. There may be individual patient and disease-related databases for providing the appropriate recipe to select the color of visible light, aroma type and 1/f fluctuation pattern type, and to control the visible light brightness in the remotely located patient's premises. These different kinds of stimulation need to be selected appropriately based on the patient's current physical and mental condition as indicated by the biometric sensors. In addition to environmental sensor information such as ambient temperature, atmospheric pressure, light level and humidity, data obtained from body sensors and relating to the patient's body, such as pulse rate, blood pressure, respiratory rate and so on, will be utilized to accurately determine the patient's current physical and mental state. Data relating to the patient's current physical condition, such as brain waveform, blood pressure, heart rate, etc., can be fed back via the high-speed network, and the optimum combination of stimulations can be appropriately and dynamically provided in real time, so that the patient's physical and mental condition will improve.

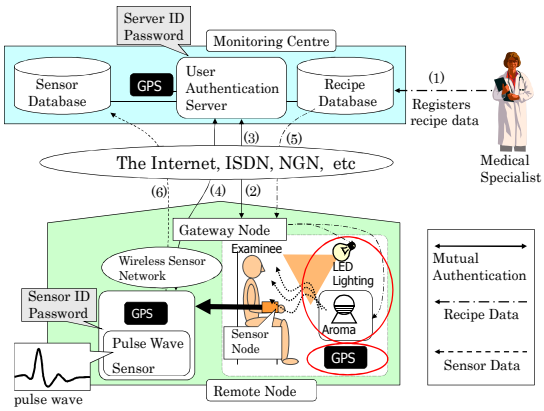

Figure 6. Configuration of the Proposed Healing Communication System

An example of the recipe data format is shown in TABLE I.

TABLE I. HEALING RECIPE DATA FORMAT

Aroma Recipe (1ch~6ch)	Brightness (Red color)	Brightness (Green color)	Brightness (Blue color)	1/f characteristics (pattern)

(2) A client (the Remote Node) accesses the Monitoring Centre via the Gateway Node, and sends his or her user ID, password, and geographical position as determined by GPS for mutual authentication.
(3) The Monitoring Centre sends the location information registered beforehand to the Remote Node for mutual authentication.
(4) The Monitoring Centre and the Sensor node execute mutual authentication as follows. The Monitoring Centre requests the Sensor node to send information about its geographical position, and determines whether the Sensor node's position coincides approximately with the position of the Remote Node.
(5) After mutual authentication has been established, the Monitoring Centre sends the appropriate healing recipe data via the Gateway Node.
(6) The Sensor node sends measured biometric sensor data to the Sensor Database via the Monitoring Centre. The sensor data acquired in real time are used to evaluate the patient's psychological and physiological status after the healing recipe has been applied. The results are fed back to the medical specialist to further improve the patient's condition.

2) Mutual Authentication and Key Sharing Scheme.

We propose the use of an ID-based key sharing mechanism [11] for mutual authentication. Several key sharing schemes have been developed for authentication over the Internet, such as Diffie-Hellman, and Kerberos [12].

These are not suitable for sensor network applications because the processing power of a sensor node is too limited. Another conceivable scheme for mutual authentication is a key pre-distribution scheme, in which each sensor node receives common keys in advance from other sensor nodes. Usually, we have been considering a sort of client-server type system, with each sensor connected to the hospital. However, when we make use of multiple sensors in a ubiquitous environment sensor network, the different sensors need to exchange information with each other. However, the number of keys that each node must manage increases in proportion to the number of sensor nodes, while the memory capacity of each node is limited. In addition, this scheme lacks extendibility. To avoid the problems of these schemes, we propose an ID-based key sharing scheme. This allows prompt mutual authentication because this key sharing scheme does not require interactive key information exchange operations. The configuration of the ID-based key sharing scheme is shown in Figure 7.

The key sharing procedure uses secret private keys. The key management server generates secret private keys based on users' ID information and transmits the keys to each node in advance over a predetermined secure communication path. The procedure for sharing keys between communication nodes is handled only by the nodes which have been authenticated by the key management server in advance.

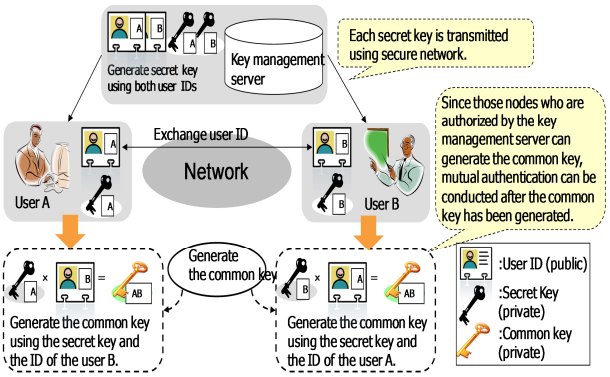

Figure 7. ID-based key sharing scheme configuration

This procedure is the basis of the proposed mutual authentication mechanism in which communication nodes share common keys. The common keys generated by one pair of communicating nodes differ from those generated by another pair of communicating nodes. This provides for network scalability. The mathematical background of the proposed common key generation method is as follows [13].

Let D be a private symmetrical matrix generated by the key management server.

The matrix I is a row vector, containing values which are equivalent to the ID information of each node. G is calculated based on matrix D and matrix I. The column vector G corresponds to the secret keys of the ID information. Matrix I is a row vector containing a set of values which are equivalent to the ID information of each node.

$$G = (D \cdot I)^T$$
$$G \cdot I = (D \cdot I)^T \cdot I = I^T \cdot D^T \cdot I = I^T \cdot D \cdot I$$
$$= (G \cdot I)^T$$

Therefore, a symmetrical matrix can be obtained. An example of the common key generation is provided below, based on this calculation.

Two nodes, say Node A and Node B, exchange their IDs, Ia and Ib, with each other and generate keys, Kab and Kba, using the exchanged IDs and their private keys.

$$K_{ab} = G_a \cdot I_b = (D \cdot I_a)^T \cdot I_b = I_a^T \cdot D^T \cdot I_b = I_a^T \cdot D \cdot I_b$$
$$= I_a^T \cdot (G_b)^T = (G_b \cdot I_a)^T = G_b \cdot I_a = K_{ba}$$

These expressions show that Kab is equal to Kba, and that the procedure for key sharing between two nodes can be executed. We can use this mutual authentication procedure to implement a sensor network that deploys the priority control mechanism on the proposed sensor network itself.

The security of the proposed scheme can be enhanced by increasing the length of the ID code in addition to adopting the elliptic curve method [14]. An appropriate level of security can be established to suit the required security policy and the sensor network environment.

3) Configuration of the Intelligent Sensor

We used a Sun SPOT from Sun Microsystems for the sensor node. Since its control program can be written in the Java language, it is easy to develop a prototype system. The secret key used by the user authentication server for mutual authentication is generated at each node. Using a pulse wave sensor and a GPS device, the Sensor Node can measure biometric data and acquire its geographical position information. The pulse wave sensor measures changes in the amount of hemoglobin in the blood. The pulse wave sensor circuit used is shown in Figure 8. The pulse wave sensor irradiates the tip of a finger with light, such as an infrared beam. The light falling on hemoglobin is absorbed, and the light falling on the sensor is light that has not fallen on hemoglobin, but is reflected from the blood-vessel/bone boundary. The light caught by the optical sensor is converted into an electrical current. After processing the corresponding electrical current through a differential amplifier it will be transmitted via wireless communication. The electrical current can be converted into blood pressure data using a current-voltage converter, a low-pass filter, and a differential amplifier. Changes in the amount of hemoglobin can thus be acquired.

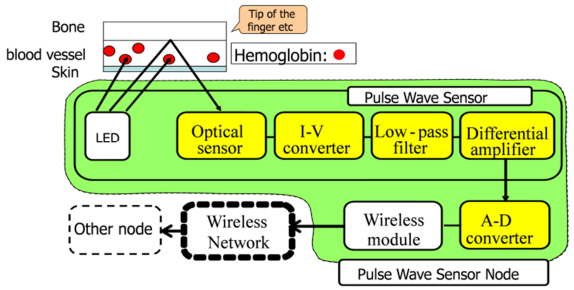

Figure 8. Pulse wave sensor circuit

4) Healing Recipes and the Evaluation of Physiological and Psychological Conditions

The proposed system uses pulse wave data to determine the specific healing recipe to be prescribed. Pulse wave data are useful for determining the condition of the autonomic nervous system. The autonomic nervous system is divided into the sympathetic nervous system, which represents the active state of a living body, and the parasympathetic nervous system, which represents the resting or relaxed state of the body. Since the autonomic nervous system directly affects the physiological and psychological conditions of a person, the psychological condition of a person can be determined objectively by measuring and analyzing his or her biometric data [15].

Some examples of the influence of the autonomic nervous system on the human body are shown in Table II.

TABLE II. PHYSIOLOGICAL TENDENCIES RELEVANT TO THE AUTONOMIC NERVOUS SYSTEM

		Sympathetic Nervous Activity	Parasympathetic Nervous Activity
Physiological Tendency	Heart	Increase of blood pressure, heart rate	Decrease of blood pressure, heart rate
	Blood Vessel	Contraction	Enlargement

The autonomic nervous system evaluation method is as follows. In the autonomic nervous system function, the sympathetic nerve is in a dominant state if the LF/HF value is high, and the parasympathetic nerve is in a dominant state if LF/HF value is low. Generally, for the analysis of frequency characteristics, the maximum entropy method (MEM) is used. MEM is a parametric technique and is used for estimating the power spectrum by making use of a linear prediction model. Even if only a few data points are measured, an adequate spectrum analysis with high resolution can be obtained by making use of MEM. That is the reason why MEM is suitable for analyzing the frequency spectrum just by using the minimum amount of data. In our experimental system, we used MEM to analyze the autonomic system function [16]. The autonomic nervous system function is measured by the acceleration pulse wave [17].

The acceleration pulse wave can be obtained using the second differential of the finger plethysmograms. The waveform pattern of the acceleration pulse is shown in Figure 10.

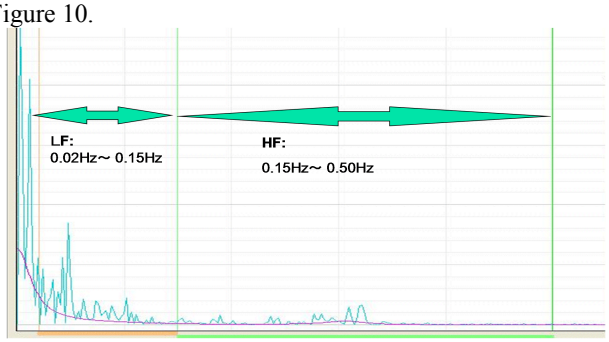

Figure 9. LF and HF bands of the autonomic nervous system

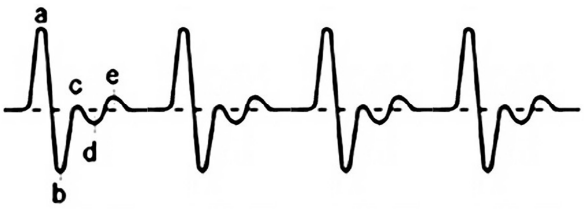

Figure 10. Waveform of acceleration pulse wave

The acceleration pulse wave form has the wave features a, b, c, d and e in Figure 10. Here, the value of b/a generally increases with the age of the subject, while d/a

decreases with age. The "waveform index" is the degree of aging of the blood vessel as measured by the change of the shape of the waves [18]. Generally, the b wave feature becomes shallow, and the d wave feature becomes deep with aging. Therefore, we can calculate the change of the waveform index due to aging by making use of the values d/a and b/a. Then, an arteriosclerosis degree (score) that describes the blood vessel can be obtained.

The calculated score expresses the degree of hardening of the artery wall and the degree of functional strain. A score of under 20 indicates that the degree of blood vessel aging is low, and the flexibility of the blood vessels is much higher than average. A score from 20 to 34 also indicates a low blood vessel aging rate, and the flexibility of the blood vessels is notably higher than average. A score of 35-39 indicates a low blood vessel aging rate, and the flexibility of the blood vessels is slightly higher than average. A score of 40-59 indicates that the flexibility of the blood vessels is average. A score of 60-64 indicates that the blood vessel aging rate is a little faster than average, and the flexibility of the blood vessels is slightly lower than average. A score of 65-69 indicates a rapid blood vessel aging rate, and the flexibility of the blood vessels is much lower than average. A score of over 70 indicates a very rapid blood vessel aging rate, and the flexibility of the blood vessels is much lower than the average [19]. The arteriosclerosis degree (score) evaluation formula is as follows.

Score = 50 + 10 (X1 mean - X1 peak value) / X1 standard deviation

*X1 (Waveform index) = d/a - b/a

For evaluating the stress value in a human being it is often effective to measure the alpha amylase activity in saliva.

With the alpha amylase activity in saliva, the degree of stress can be measured as a biomarker. The density of the alpha amylase, which is one of the digestive enzymes, changes with any active change in the sympathetic system. There are several biomarkers that measure the degree of stress, and cortisol is one of the typical ones. In the case of alpha amylase, the time interval from the stimulation to the secretion is shorter than in case of the cortisol [20].

Therefore, in a situation with significant mental stress (acute stress) a quantitative analysis of the degree of stress is possible by measuring the alpha amylase in the saliva.

There are several advantages to assessing the stress value by measuring the alpha amylase activity in saliva. The procedure is:

(1) Non-invasive
(2) Rapid measurement
(3) Rapid analysis
(4) Simple and portable measurement
(5) Low cost

It should be noted that the alpha amylase activity in saliva differs for each individual and also changes during the day, so measuring the degree of difference before and after the stimulation is essential [21].

A spectrum analysis of historical data of pulse cycles is known to be an effective method for determining the state of the autonomic nervous system [22]. Past studies indicate that the fluctuation of pulse cycles of low-frequency components (LF: 0.02 to 0.15 Hz) is related to the strength of the activities of both the sympathetic nervous system and the parasympathetic nervous system. On the other hand, high-frequency components (HF: 0.15 to 0.50 Hz) are related to the strength of the activity of only the parasympathetic nervous system.

5) Priority Control Mechanism used in the Sensor Network

There have been no in-depth studies on how to achieve real-time processing for the collection of sensor data, such as pulse data, as is required of a sensor network. To achieve real-time performance in addition to ensuring network security, we propose to use the above-described ID-based key sharing scheme for implementing priority control and for ensuring security in the sensor network. We have evaluated the network performance of the proposed priority control mechanism while taking various elements of the network environment into consideration.

6) Functional Requirements for the proposed system

The functions required for priority control in the sensor network are described below.

To protect the sensor data from eavesdropping and tampering, the data must be encrypted in an effective manner. For encrypting sensor data, it is necessary to ensure security of key sharing between the communication nodes using mutual authentication between the communication sensor nodes. The proposed encryption mechanism implemented on an experimental system is shown in Figure 11.

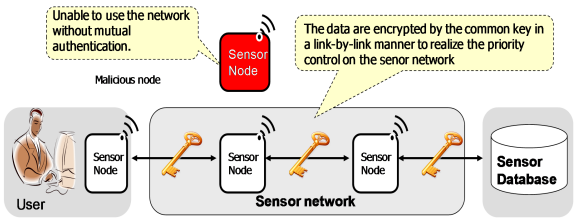

Figure 11. Encryption mechanism of the experimental system

Figure 12 shows an example of the format of the encrypted transmission data, which provides adequate confidentiality and security. To achieve mutual authentication between the sensor node and the sensor database, the sensor data must first be promptly encrypted over the end-to-end path using common keys. In addition, the corresponding data can also be encrypted in a link by a link procedure using different common keys. Figure 13 shows an example of the format of encrypted transmission data between sensor node 3 and the sensor database, which is the final destination. The encrypted data can finally be decrypted in the sensor database using both the key which is the common key with sensor node 3 for link-by-link communication and the different common key used between sensor node 1 and the sensor database.

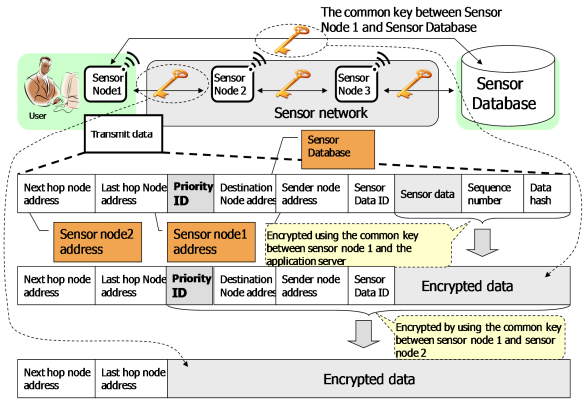

Figure 12. Composition of the transmitted sensor data

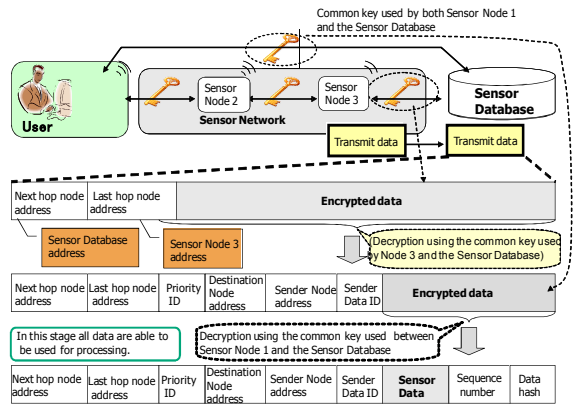

Figure 13. Decryption of the encrypted transmitted sensor data

III. EVALUATION OF SYSTEM PERFORMANCE

A. Evaluation of the proposed priority control mechanism

1) Conditions of the experiment

Traditionally, sensor network applications for environmental monitoring, precision agriculture, and so on, do not require a prompt response, and do not have to handle operations with different QoS. However, real-time communication services that make use of wireless sensor networks are becoming indispensable, in particular for healthcare monitoring [23]. Against this background, the priority queue monitoring mechanism and the corresponding communication protocols have been investigated [24].

However, most of the results obtained are based on simulations, and the substantial tradeoffs between the different QoS requirements have not yet been established. Consequently, we first examined the ability of the commercially available and economical Sun SPOT sensor nodes to send data while making use of the priority control mechanism, and ascertained the feasibility of realizing a queuing control system easily. Communications in sensor networks can be broadly divided into two categories: local coordination and sensor-based communication. Before sending information to the transit sensor node, sensors within a local area should cooperate in order to aggregate data and ensure reliable data transmission. However, in this paper, we disregarded these extra conditions in order to analyze the transmission effectiveness of a sensor node that employs the priority control mechanism. Based on these considerations, we evaluated the delay time performance under the following conditions.

The basic configuration of the experimental system in which the proposed priority control mechanism was implemented is shown in Figure 14. A Sun SPOT node from Sun Microsystems was used in the experiment.

In the experimental system, sensor data were transmitted from two sensor nodes to the sensor database, which collected sensor data via two intermediate hop nodes in order to ascertain the performance of the priority control mechanism. We set two levels of priority in all relay sensor nodes: high and low priority levels. For example, a high priority level was assigned to pulse wave data to reduce both delay and delay fluctuation. A low priority level was assigned to temperature data because neither its transmission delay nor its delay fluctuation needs to be small. A different data buffer was used for each priority level.

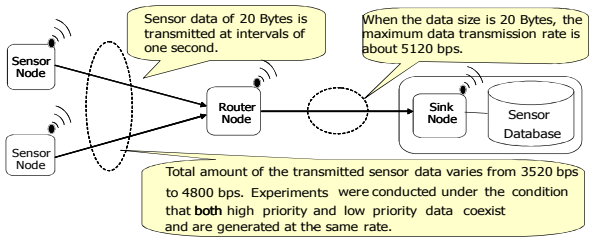

Figure 14. Configuration of the Experimental System

A photo of the actual sensor network is shown in Figure 15. Here several Sun SPOT nodes are used for a Sensor Node, a Router Node (Transit node), and a Sink Node. According to the specifications of the Sun SPOT it adopts the IEEE802.15.4 wireless standard (2.4-2.4835 GHz), and can transmit packet data using QPSK modulation technology.

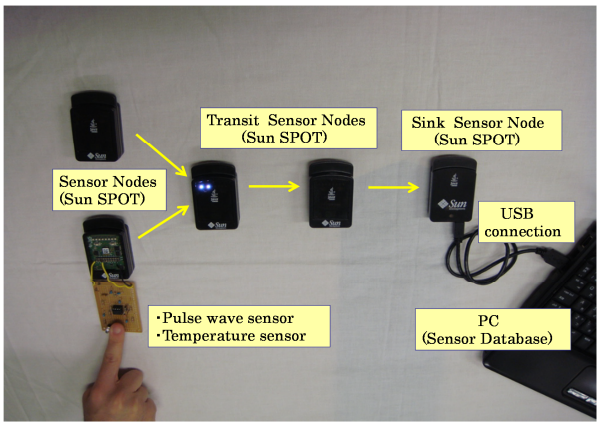

Figure 15. Photo of the experimental sensor network system

The size of each packet of sensor data was 20 bytes (8 bit quantization and sampled at 20 Hz). The sensor data were transmitted once every second. The maximum transmission speed of data transmitted over two hops was about 5120 bps as dictated by the specification of Sun SPOT. Two nodes can communicate by transmitting sensor data at speeds ranging from 3520 bps to 4800 bps.

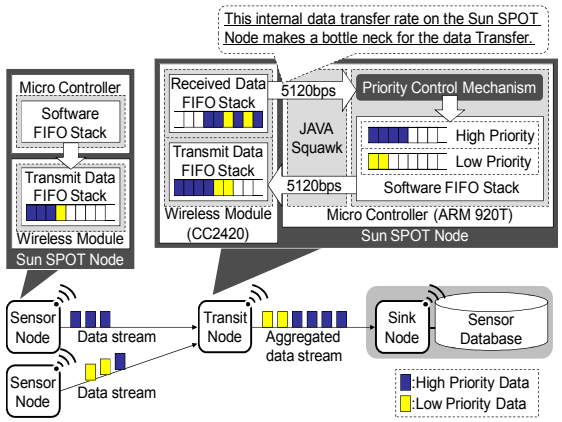

Figure 16. The mechanism providing priority control

In the sink nodes and transit nodes, we adopted a simple priority control mechanism in which the operation of switching to the lower priority output buffer can be done only after the higher priority output buffer has become empty, although the input data are stored continuously inside the buffer in a FIFO manner. Operation will be switched back again to the higher priority output buffer if higher priority data are stored in the FIFO buffer, even when the low priority data are being output, in order to ensure real-time performance of the higher priority data, as shown in Figure 16.

In this case, we found that the communication bottleneck among the Sun SPOT nodes was due to a restriction in the internal data transfer rate between the wireless module (C2420) and microcontroller (ARM920T), which are controlled by Java squawk in the Sun SPOT node. When the data size is 20 bytes, the maximum data transmission speed is measured as 5120 bps. However, even if the data transmission rate exceeds the specified limit for a short time, the data can be transmitted provided that the excess amount of transmitted data does not exceed the Sun SPOT FIFO buffer size.

The entire queuing control was implemented in the software. The Sun SPOT adopts the 180 MHz 32 bit micro-processor (ARM 920T) and can make use of 512 Kbyte RAM for programs and the FIFO control buffer.

The processing mechanism of the proposed priority control system is mainly composed of two independent processes, as shown in Figure 16.

Figure 17 (a) shows the process that registers the received sensor data in the appropriate priority control stack by identifying the priority of each data item by checking the Priority ID of the data frame, which was previously described in Figure 12.

Fig.17 (b) shows the process flow that transmits the data stored in each control stack according to its inherent priority level. The high priority control stack is identified first, and all high priority data are transmitted until no high priority data are left in the stack. In the next step, the process checks the low priority control stack and sends the low priority data if any exist. After finishing this procedure, the data transmission process reverts to the first operation and these operations are repeated continuously.

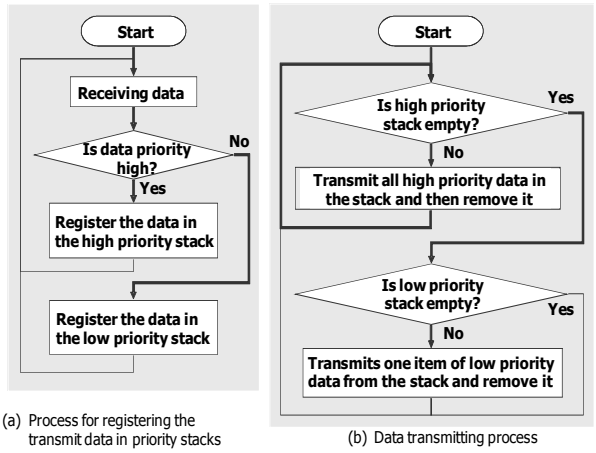

Figure 17. Processing flow of the proposed priority control mechanism

We carried out two experiments, one using priority control and the other without it. The transmission rates of both the high priority and the low priority data were the same. We measured the average data-receiving interval at the sink node, the average delay time and the average delay fluctuation of the transmitted sensor data. Sensor data were transmitted continuously for 12 seconds. Considering that about 1 second is required for call set up, we used data measured between 2 seconds and 12 seconds.

2) Experiment Results

We classified the experimental results into two parts: first where the total transmitted data rate was less than 5120 bps, and second where it was more than 5120 bps. As shown in Figure 18, the transmitted data rate of 5120 bps corresponds to the Sun SPOT internal transfer rate, so the maximum transmission throughput cannot exceed this limit. However, if the period of continuous data transmission is sufficiently small, then the use of the internal buffer may allow the transmission to be successful in some circumstances. Figure 19 shows the experimental results of the interval between receiving one packet and the next, the average delay time and the average delay fluctuation.

The average receiving interval was approximately one second, irrespective of whether priority control was used or not. We confirmed that no errors were observed at the destination sink node. The average delay and the average delay fluctuation increased in proportion to the total amount of sensor data transmitted from all nodes. In

addition, the difference in the average delay and the average delay fluctuation between high priority data and low priority data became greater as the total amount of sensor data increased. The reason is due to the simple priority queuing control mechanism, implemented by the software as mentioned above. From these experiments, we obtained the following conclusions when we made use of Sun SPOTs as ad hoc sensor nodes.

(1) Restriction of the total volume of sensor data and aggregation of this data are very important in ensuring adequate real-time performance.
(2) The software control priority queuing scheme is very efficient in minimizing both the delay time and the delay variation simultaneously.
(3) When the total rate of sensor data transmitted is less than the pre-assigned maximum transmission speed of 5120 bps, the priority control mechanism is effective.

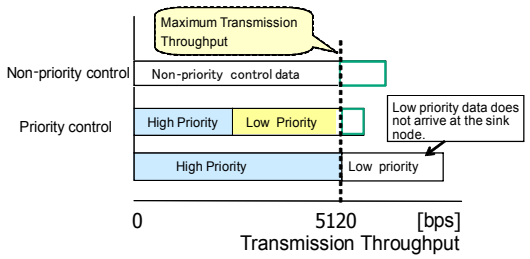

Figure 18. Priority and non-priority control concepts

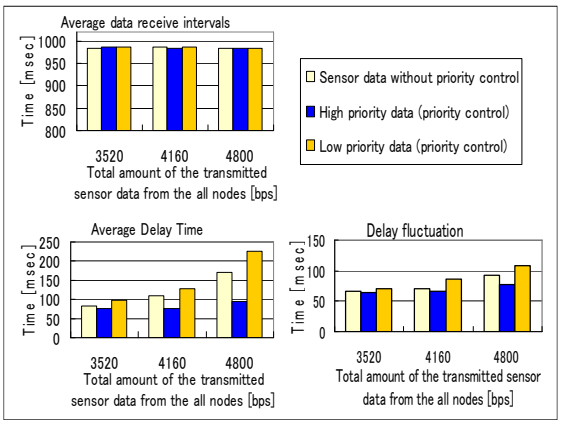

Figure 19. The average delay and the average delay fluctuation

B. Evaluation of sensor database performance

To ensure the confidentiality of personal information, such as measured sensor data, the sensor data were encrypted, and a secure method was used for accessing the sensor database. We evaluated quantitatively the real-time performance of the Sensor Database [25][26].

1) Configuration of the Database

The proposed database consisted of a Sensor Database, which stored encrypted data, and a Monitoring Centre, which stored encryption keys. A stream encryption method that requires low processing power was employed for data encryption, as shown in Figure.20.

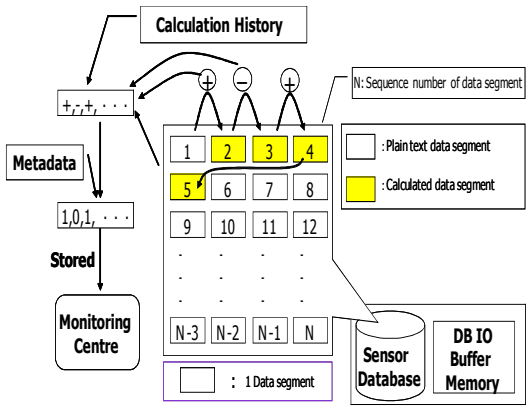

Figure 20. Proposed Encryption Method

In the proposed encryption method, sensor data, which consist of a series of plain text characters, is divided into segments of a certain number of bits. The simplest case is using a string of multiple bits as one word. One of the possible reversible logical operations, such as addition, subtraction or exclusive-OR operation, is applied to combine the binary values (the string of bits of value 0 or 1) of one word with those of the following word. The result of the calculation is then stored in the location of the second of these words and the sequence then repeated moving on to the next word. A different reversible operation may be selected for each word in the sequence, depending on the encryption key information stored in the authentication server.

The result of successive execution of a reversible operation on the original binary data can be replaced by the original data in each word. Although the above example uses a "word" as the minimum unit of encryption, any size can be selected as the minimum size of the bit length. Efficient encryption and decryption can be achieved by selecting an appropriate bit length execution. The information history associated with the sequence of selected reversible operations mentioned above is provided as metadata managed by the monitoring center, and the actual operations were executed on the test data for the evaluation.

For example, in encrypting an item of data consisting of three consecutive words, suppose that "1" corresponds to a binary addition, and "0" to a binary subtraction. If the metadata is "101" for example, a binary addition is executed for the first and second words, and the result is stored in the second word. After that, a binary subtraction is executed on the second and third words, and the result is stored in the third word. After that, a binary addition is executed on the third and fourth words, and the result is stored in the fourth word. In this way, metadata is used until an operation is executed on the last word in the sequence. To extract plain text from data encrypted as above, in the absence of the metadata, the number of random attempts required could be as high as 2 to the power of the number of words in the worst case. It is therefore difficult for a malicious third party to

decrypt the data. In addition, since the size of data segment can be changed regularly, it can be made even more difficult to decrypt the data.

2) Experimental Methodology

In accordance with the proposed method, the processing power (including encryption) of the sensor database in the monitoring center was evaluated in line with the following principle. The parameters used in the experiments were the number of simultaneous connections to the sensor database (users), and the capacity of the I/O buffer used for direct access to the sensor database via a network interface. The rate at which data was stored in the sensor database was used as the measurement criterion. We assumed quasi-client terminals that contained sensor nodes.

We further assumed that 100 to 300 such terminals accessed the database simultaneously. When a sensor node accessed the monitoring center, it conducted mutual authentication using the user authentication server.

After the sensor node had received the healing recipe data, it transmitted a series of items of sensor data composed of pulse wave data (1kB, 8-bit data with a sampling rate of 1 kHz, for example) to the Sensor Database at intervals of one second for several seconds. In order to examine the real-time performance of the Sensor Database, we conducted evaluation experiments to determine the conditions under which all sensor data from 300 terminals were successfully stored, the operation being completed as quickly as possible. The criterion used was the rate at which the data transmitted continuously from each sensor node was stored. Normally, a continuous measurement of 5 minutes is sufficient to infer whether a person is in a relaxed state or not, so experiments were conducted for 5 minutes.

3) Results of the Experiment

Figure 21 shows the evaluation results. Parameter A used in this experiment is the total number of sensor nodes that accessed the database. This number is equal to the number of users. Parameter B is the capacity of the I/O buffer in the database. Experiments were conducted using these as the parameters. The results are shown below.

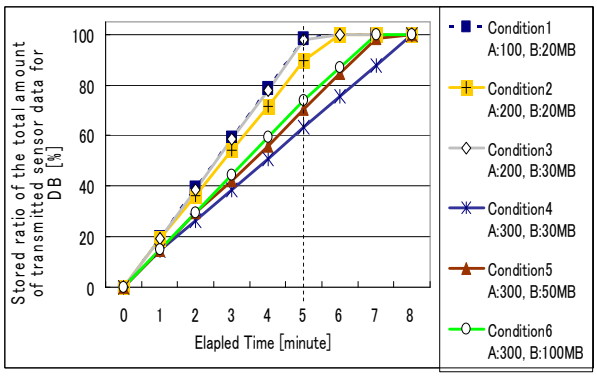

Figure 21. Results of the System Performance Evaluation

(1) Only for Conditions 1 and 3 did the amount of sensor data stored reach 100% of the total transmitted within 5 minutes of the start of the experiment. However, if the number of users is greater than that applied in the above conditions, it will be necessary to adjust the capacity of the I/O buffer in the database.

(2) The experiments using Conditions 4 to 6 revealed that for a fixed number of users, the effect of increasing the I/O buffer capacity for collecting data beyond 30 MB is relatively small.

(3) The results of these experiments identified the size of the DB I/O memory required to implement the system. It was found that if the number of users is in the range of 100 to 200, a 20 MB I/O buffer in the database was sufficient, even when sensor data collecting services were provided simultaneously to all sensors.

This result can be used to build a sensor network that has real-time performance sufficient for applications for future telemedicine.

IV. CONCLUSION

We have proposed a health care communication system that uses GPS technology and ensures confidentiality of personal information. The system can be used for telemedicine to improve a user's QoL.

In addition, we have proposed a priority control mechanism that uses an ID-based key sharing scheme in the proposed sensor network both to achieve adequate real-time performance and to ensure security of sensor data. Evaluation using an experimental system confirmed that the average delay time and the delay fluctuation of delay-sensitive data were reduced effectively when such data were transmitted with high priority compared with the method of non-priority control. We have also confirmed that a sensor database that uses an efficient encryption mechanism for ensuring security and maintaining the confidentiality of users' sensor data shows excellent real-time performance.

In the future, we will collaborate with medical hospitals and social welfare centers to realize practical healthcare applications.

ACKNOWLEDGMENT

This study was supported in part by Tokyo Denki University Research Center for Advanced Technologies (Q07J-13) and a grant of Strategic Research Foundation Grant-aided Project for Private Universities from Ministry of Education, Culture, Support, Science, and Technology, Japan (MEXT) (2007-2011)

REFERENCES

[1] N. Miyaho, T. Nakamura, N. Konno, and T. Shimada, "Sensor Network Management for Healthcare Applications", ICSNC2010, ICSNC1 SENET I, pp.14-20 Aug., 2010.

[2] N. Miyaho, N. Konno, and T. Shimada, "Study on Healing Environment using Green, Blue and Red LED and Aroma", J. Light & Vis. Env. Vol. 32, No. 2, pp. 47-52, May, 2008.

[3] N. Miyaho, N. Konno, and T. Shimada, "Study on Healing Environment using green, blue, red LED and aroma" (Invited), First International Conference on White LEDs and Solid State Lighting (White LEDs-07), Nov., pp. 307-310, 2007

[4] N. Konno, "The psychological effect of color lighting with regard to mental health", Bulletin of Tokyo Denki University, Arts and Sciences, No.6, pp. 55-62, 2008. (In Japanese).

[5] Mary A. Carskadon and Allan Rechtschaffen, "Monitoring and Staging Human Sleep", Principles and Practice of Sleep Medicine (Fourth Edition), pp. 1359-1377, 2005.

[6] Alex L. van Bemmel, "The link between sleep and depression: The effects of antidepressants on EEG sleep", Journal of Psychosomatic Research, vol.42, Issue 6, pp.555-564, June, 1997.

[7] T. Nakamura, T. Shimada, N. Konno, and N. Miyaho, "Study on Healing Environment Conditions by making use of 1/f Fluctuation", IEICE National Convention, BS-12-6, 2007.

[8] N.Shinzawa, M. Komazaki, and N. Miyaho, "Study on Applications of Using Visible Light Communications", IEICE National Convention 2008 A05_004, 2008. (In Japanese)

[9] S. Kurokawa, Y. Iwaki, and N. Miyaho, "Study on the distributed data sharing mechanism by making use of the mutual authentication and meta database", IEEE APCC2007, pp. 215-218, 2007.

[10] S. Kurokawa and N. Miyaho, "Study on a distributed data sharing mechanism with mutual authentication", IEICE IN Technical Paper IN 2006, No.214, pp 203-206, 2006. (In Japanese)

[11] S. Tsujii, K. Araki, and T. Sekine, "A New Scheme of Non-Interactive ID-based Key Sharing with Explosively High Degree of Separability (Second Version)", Tokyo Institute of Technology Technical Report, Dept. of CS, TR-0020, 1993. *(In* Japanese)

[12] http://www.rfc-editor.org/rfc/rfc1510.txt (Sep.1993), <2011.7.10>.

[13] R. Blom, "Non-public key distribution," Proceeding of Crypto'82, pp. 231-236, 1982.

[14] O. Kiyoshi, R. Ryuichi, and M. Kasahara, "Notes on ID-based Key Sharing System over Elliptic Curve", ISEC99-57. pp.37-42, 1999. *(In* Japanese)

[15] J. W. Severinghaus, and J. F. Kelleher, "Recent developments in pulse oximetry", Anesthesiology 76 1018-1038, 1992.

[16] N. Konno, "Influence that Irradiation of color Lighting exerts on Autonomic Nervous system Function", Bulletin of Tokyo Denki University, Arts and Sciences, No.5, pp. 67-74, 2007.(In Japanese)

[17] H. Takada, K. Okino, and Y. Kiwa, "An Evaluation Method for Heart Rate Variability, by using Acceleration Plethysmography", Health & Prom., 31(4), pp. 547-551, 2004.

[18] H. Takada, K. Washino, and H. Iwata, "Accelaration plethysmography to evaluate aging effect in cardiovascular system.Using new criteria of four wave patterns", Medical progress through technology 21(4), pp. 205-210, 1996-1997.

[19] H. Takada, "Proposal of Aging Score Method by Acceleration Plethysmography", Health Evaluation and Promotion, 29(5), pp. 855-861, 2002.

[20] Weibel L, "Methodological guidelines for the use of salivary cortisol as biological marker of stress", Presse Med 32., pp. 845-851, 2003.

[21] M. Yamaguchi, M. Deguchi, J. Wakasugi, S. Ono, N. Takai, T. Hihashi, and Y. Mizuno, "Hand–held monitor of sympathetic nervous system using salivary amylase activity and its validation by driver fatique assesment", Biosens Bioelectron, 21, pp. 1007-1014, 2006.

[22] Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology: "Heart rate variability: standards of measurement, physiological interpretation and clinical use", Circulation, Vol. 93, pp. 1043-1065, 1996.

[23] T.Bratan and M.Clarke, "Optimum design of Remote Patient Monitoring System", 28th International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS'06, pp.6465-6468, 2006.

[24] M. Basta, R.Severino and M. Alves, "Supporting different QoS levels in Multiple-Cluster WSNs", Proceedings of 10th Portugeuse Thematic Network on Mobile Communications Workshhop (RTCM), Porto, Portugal, June, 2009.

[25] T. Kobayashi, S. Kurokawa, N. Konno, and N. Miyaho, "Study on Database Server Performance Evaluation for Realizing Aroma Information Delivery", IEICE Student National Convention, p.86, 2007. (In Japanese)

[26] T. Nakamura, T. Shimada, N. Konno, and N. Miyaho, "Study on the sensor database for realizing Healing Communication System", IEICE Society Convention, BS10-25, pp.S113-114, 2009.