European Research in Telemedicine/La Recherche Européenne en Télémédecine (2016) 5, 137—144

Available online at ScienceDirect www.sciencedirect.com

Elsevier Masson France EM|consulte www.em-consulte.com/en

ORIGINAL ARTICLE /*Remote Monitoring*

Development of key generation algorithm using ECG biometrics for node security in wireless body area sensor network

Le développement de l'algorithme de génération de clé en utilisant la biométrie ECG pour la sécurité du nœud dans le réseau de capteurs de surface corporelle sans fil

J. Chukwunonyerem[a,*], A.M. Aibinu[b], A.J. Onumanyi[b], O.C. Ugweje[b], E.N. Onwuka[b], C. Alenogbena[b], N. Ezechi[a]

[a] *NASRDA centre for basic space science, bookshop building, university of Nigeria, PMB 2022, Nsukka Enugu State, Nigeria*
[b] *Department of telecommunication engineering, Federal university of technology Minna, PMB 65, Gidan-Kwanu, Minna-Bida Road, Niger State, Nigeria*

Received 14 June 2016; accepted 24 September 2016
Available online 23 November 2016

KEYWORDS
Biosensor;
Security;
Energy;
Algorithm;
WBASN

Summary This paper investigates security and inter-node transmission energy for biosensors in a wireless body area sensor network (WBASN) system. Existing security solutions in WBASN have been observed to employ the pre-deployment of static authentication keys, which are unsecured and energy intensive. Electrocardiogram (ECG) biometric-based security scheme was developed using the peak location index (PLI) and inter-pulse-interval (IPI) of the heart beat. The fast Fourier transform method was used to process individually selected ECG datasets of diabetic patients and the differential equation method was used to extract the ECG biometric features (PLI and IPI). Energy model of Chipcon CC2420 specification was used to evaluate inter-node energy consumption performance. The research results showed that different PLI and IPI features were extracted from the ECG datasets and unpredictable authentication keys were generated. Node energy consumption performance evaluation showed a 25% reduction in

* Corresponding author.
E-mail address: chuksjustusy2k2@yahoo.co.uk (J. Chukwunonyerem).

http://dx.doi.org/10.1016/j.eurtel.2016.09.002

energy consumption for successful inter-node transmission. The ECG feature keys generated were different and unpredictable at every instant, providing for inter-node communication security. Non-additional node energy for processing the authentication acknowledgment packets provided for inter-node energy consumption reduction. The developed algorithm has provided for secured inter-node communication with a 25% energy efficiency in node transmission energy consumption for a WBASN system.

MOTS CLÉS
Biocapteur ;
Sécurité ;
Énergie ;
Algorithme ;
WBASN

Résumé Cet article examine la sécurité et l'énergie de la transmission inter-nœuds pour biocapteurs dans un système réseau de capteurs de surface corporelle sans fil (WBASN). Les solutions de sécurité existantes dans un système WBASN ont été observées pour recourir à un pré-déploiement de clés d'authentification statiques qui sont non sécurisées et à forte intensité énergétique. Un régime de sécurité à base biométrique pour électrocardiogramme (ECG) a été développé en utilisant l'indice de position de pic (PLI) et l'intervalle entre les impulsions (IPI) des battements du cœur. La méthode transformée de Fourier rapide a été utilisée pour traiter des ensembles de données ECG de patients diabétiques choisis individuellement et la méthode d'équation différentielle a été utilisée pour extraire les caractéristiques biométriques ECG (PLI et IPI). Le modèle énergétique de spécification Chipcon CC2420 a été utilisé pour évaluer la performance de consommation énergétique inter-nœuds. Les résultats de la recherche ont montré que différentes caractéristiques PLI et IPI ont été extraites des ensembles de données ECG et que la production de clés d'authentification était imprévisible. L'évaluation de la performance de la consommation énergétique des nœuds a montré une réduction de 25 % de la consommation énergétique pour la réussite de la transmission inter-nœuds. Les touches de fonction ECG générées étaient différentes et imprévisibles à chaque instant en fournissant la sécurité de la communication inter-nœuds. L'énergie non supplémentaire des nœuds pour le traitement des paquets d'authentification d'accusés de réception a fourni une réduction de la consommation énergétique inter-nœuds. L'algorithme développé a fourni une communication inter-nœuds sécurisée avec une efficacité énergétique de 25 % dans la consommation énergétique de la transmission des nœuds pour un système WBASN.

Introduction

Wireless Body Area Sensor Network (WBASN) is an evolving technology in the field of bio-medical engineering. Miniature wireless biosensors are strategically implanted on/inside the human body to create a wireless network of biosensors within the human body [1]. This network allows for monitoring of different essential biological signals within the host [2]. The measured body parameters include: the heart rate, body temperature, blood glucose level, and a prolonged electrocardiogram (ECG) recording. These can be done over a long period [2] to improve the quality of the measured data, which may not be properly ascertained within few physical visitations. Security is a major challenge in the development of a WBASN system. Sensitive medical data and node communication require reliable energy efficient security [3].

Any security breach (e.g. improper/unauthorized change of drug dosage, treatment procedures or emergency response) could be of adverse effect or result in the death of the host.

Notable application areas of WBASN are in the field of remote and mobile health care delivery. These include: measuring essential body parameters/signals; diagnosis of illness; transfer of medical data and records; monitoring patient rehabilitation or treatment procedures. These allow for sharing of medical records and provision of remote medical monitoring and support [4].

This research is focused on security and node energy conservation. An efficient biometric security scheme based on the human ECG features has been developed. This scheme is self-protective, explores the unique nature of peak location index (PLI) and inter-pulse-interval (IPI) of ECG waveform to generate authentication keys that can be used to secure node communication within the WBASN system. Performance evaluation of the systems shows a 25% reduction in energy for successful inter-node transmission.

Fig. 1 shows the architecture for a mobile health care system for telemedicine. Medical information from the biosensor implants on humans could be accessed as a cloud hosted service by health care professionals though any third-party network provider (external networks).

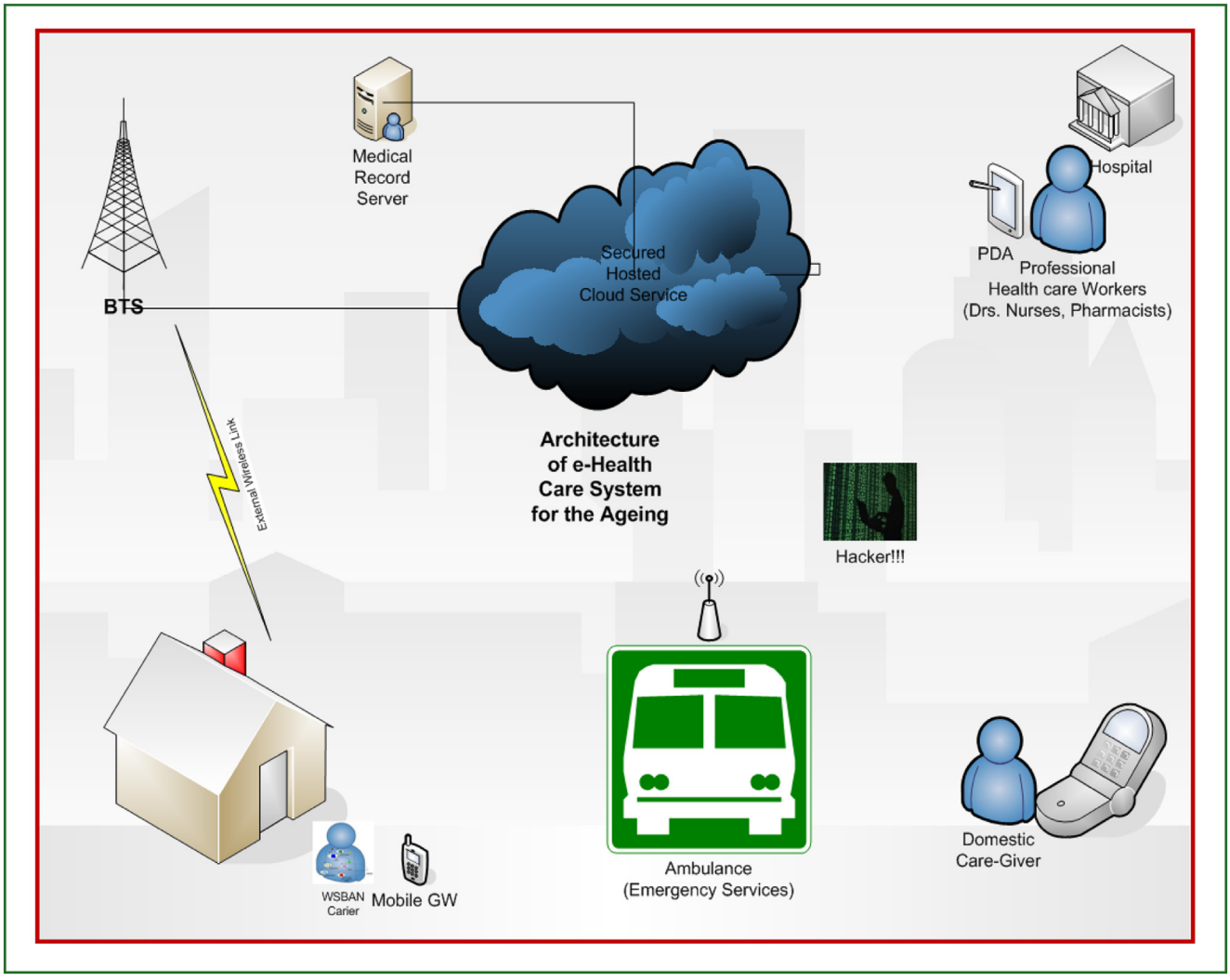

Figure 1. System Architecture of WBASN for mobile health care.
Architecture du système du WBASN pour soins de santé mobiles.

Literature survey

In this work, a literature survey was carried out within the context of security and energy conservation. Some of the literatures reviewed presented diverse security and energy conservation methods from different researches.

Latré et al. [4] presented a security review at sensor detection level using the message authentication code (MAC). Prior to node deployment, all sensors were identified and their distinct MAC addresses stored in the gateway device (GW). MAC authentication is done at this level to permit communication between the biosensors and the GW device. Although MAC is distinct for every node, it can be copied and compromised, and as such, does not offer reliable security in this regard.

The methodology presented in Surfi et al. [5] employed the use of a multi-scroll chaos application on the GW device to encrypt ECG packets at the sensor nodes. Although the technique achieved end-to-end security, it was observed that the chaos-based encryption is software-based installed on a hardware device that is vulnerable to security breach.

The work presented by Poon et al. [6], studied the use of IPI and photoplethysmography (PPG) as biometric features in generating unique keys. The key generation algorithm used in the methodology accounted for accurate inter-node synchronization and authentication. Although security was achieved, computational complexity was a major drawback as more energy and power were needed to implement the technique in WBASN.

Ramli et al. [7] designed a biometric security scheme using Message Authentication Protocol (MAP). Detection of R-Peak and Heart Rate Variability (HRV) estimation for each ECG measured was established and used for authentication between the nodes. Although security was achieved with less complexity in key generation and authentication between the nodes, it was observed that the methodology used did not account for the energy consumption level at the nodes.

Wang et al. [8] used non-fiducial-based features to remove key distribution problems and overhead as a result of time synchronization for ECG features used in WBASN. The result showed that the changing nature of human body resulted to reduced chances of physiological features being

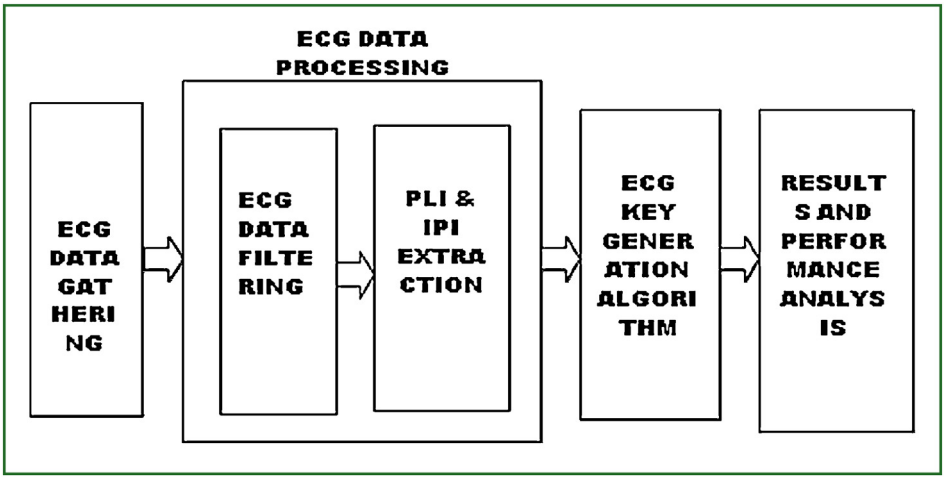

Figure 2. Methodology block diagram.
Schéma fonctionnel de la méthodologie.

alike. The research work did not account for the energy consumption.

In the aforementioned research works, the use of security methods that employ pre-deployment of static keys on the nodes making inter-node transmission vulnerable to attacks has been observed. In the case where human physiological traits and biometric features (PPG, ECG, IPI, HRV) were used to achieve security, it has been observed that complex key generation schemes were used that resulted in high node energy consumption.

This research has developed an energy efficient security scheme for inter-node transmission using the dynamic changes in IPI and PLI of the human heart beat through the following objectives:

- to extract unique ECG features (PLI and IPI) for diabetic subject using the differential equation method;
- to develop an ECG feature-based key generation algorithm;
- to evaluate the algorithm performance in terms of inter-node transmission energy conservation.

Materials and methods

The block diagram of the research methodology is presented in Fig. 2.

ECG data gathering

Five diabetic patients' ECG data was downloaded from the Physionet database as the selected input dataset.

ECG data processing

Using the fast Fourier Transform tool in MatLab, the ECG waveform was processed in frequency domain to filter out noisy signals; the Inverse Fourier Frequency Transform tool was used to revert the ECG signal back to time domain. Using first order linear difference equation method, ECG biometric features (PLI and IPI) were identified and extracted.

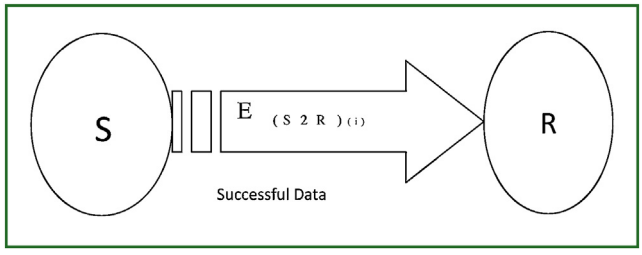

Figure 3. Successful inter-node transmission.
Succès de la transmission inter-nœuds.

Using Matlab, the ECG feature key generation algorithm was developed. The algorithm identifies and extracts PLI and IPI features from the ECG dataset. The features are used to generate unpredictable authentication keys for secure inter-node transmission.

Methodology for energy consumption evaluation

Energy conservation was evaluated using the energy model of Chipcon CC2420 specification [9] as mostly used in low rate wireless personal network (LR-WPAN). The work in Gutierrez [10] on LR-WPAN was reviewed and likened to WBASN. Chipcon CC2420 energy consumption model as derived and used in Howitt et al. [11] and Zhang et al. [12] were adopted.

Fig. 3 illustrates a successful packet transmission between nodes S and R. Energy evaluation was based on inter-node transmission scenario where data packets and authentication acknowledgment packets were successfully transmitted from node S to node R.

Using the CC2420 specification as presented in [9], Zhang et al. [12] and as can be seen in Table 1, Chipcon CC2420 specification supports eight different transmit power levels ranging from 0 dBm to −25 dBm and eight different transmit current levels ranging from 8.5 mA to 17.4 mA.

Table 1 Chipcon CC2420 Specification.
Spécification Chipcon CC2420.

Index (*i*)	Transmission power P*t(i)* [dBm]	Transmission current I*t(i)* [mA]
1	−25	8.5
2	−15	9.9
3	−10	11.2
4	−7	12.5
5	−5	13.9
6	−3	15.2
7	−1	16.5
8	0	17.4

It has a transmission rate-R*b* of 250 kbps. A supply current-I*r* of 19.7 mA is needed to receive packets. It also makes use of supply voltage-V*s* of 1.8 V.

For any given transmit power level index $P_{t(i)}$, the transmitter is needed to be supplied with an electrical power given by:

$$P_{(elect)(i)} = I_{(i)} \times V_{(s)} \tag{1}$$

$$P_{(rec)} = I_{(r)} \times V_{(s)} \tag{2}$$

Inter-node transmission of a unit packet in a LR-WPAN takes a transmission period given by:

$$T_{(p2p)} = \frac{L}{R_{(b)}} \tag{3}$$

where L is the packet length and $R_{(b)}$ is the transmission rate.

The LR-WAN is characterized by variable length data packet: L-Ack and L-Pack [11]. These are used to represent the number of bits in the authentication acknowledgment packet and data packets respectively.

L-Ack and L-Pack are respectively made up of three major components:

- L_oh: length of the header field = 11 bytes;
- L_add: length of the address field = 4—20 bytes;
- L_data: variable length data payload = 15—133 bytes;
- L-Ack = 8X11(bits) = 88 (bits);
- L-Pack = 8 X (L_oh + L-add + L_data) = 8 X (11 + 4 + 15) = 240(bits).

For successful transmission of variable length data and acknowledgment packets, the peer-to-peer LR-WPAN energy model at any given transmit power level index *i*, is given by:

$$\begin{aligned}\left[E_{(S2R)_{(i)}}(L_{pack(i)}|success)\right] &= \left[E_{(Tx\_D)_{(i)}}(L_{pack(i)})\right] + \left[E_{(Rx\_D)_{(i)}}(L_{pack(i)})\right] \\ &+ \left[E_{(Tx\_A)_{(i)}}(L_{ack(i)})\right] + \left[E_{(Rx\_A)_{(i)}}(L_{ack(i)})\right]\end{aligned} \tag{4}$$

where $L_{pack(i)}$ is the packet length, $E_{Tx\_D(i)}$ is the energy used to transmit packet by the transmitter. $E_{Rx\_D(i)}$ is the energy used by the receiver to receive the packet. $L_{Ack(i)}$, length of acknowledgement packet, $E_{Tx\_A(i)}$ is the energy used by the receiver to transmit the acknowledgment packet. $E_{Rx\_A(i)}$ is the energy used by the transmitter to receive the acknowledgment packet.

From Eq. (1), (2) and (3), Energy used to transmit packet length L_{pack} from node S to node R is.

$$E_{(TX)_{(S2R)}} = p_{(t)_{(i)}} \times \frac{L_{(pack)}}{R_{(b)}} \tag{4a}$$

Energy used by node R to receive packet length L_{pack} from node S is.

$$E_{(Rx)_{(R)}} = p_{(rec)_{(i)}} \times \frac{L_{(pack)}}{R_{(b)}} \tag{4b}$$

Energy used by node R to transmit acknowledgment packet of length $L_{(Ack)}$ from node R to S is.

$$E_{(Tx)_{(Ack)_{(R)}}} = p_{(rec)_{(i)}} \times \frac{L_{(Ack)}}{R_{(b)}} \tag{4c}$$

Energy used by node S to receive acknowledgment packet of length $L_{(Ack)}$ from node R is.

$$E_{(Rx)_{(Ack)_{(S)}}} = p_{(i)} \times \frac{L_{(Ack)}}{R_{(b)}} \tag{4d}$$

Taking into consideration that the nodes are on the same body generating the same authentication keys, for every inter-node transmission, energy that would have been used in transmitting and receiving authentication acknowledgment packet is conserved. Eq. (4) can be reduced to:

$$\left[E_{(s2r)_{(i)}}(L_{pack(i)}|success)\right] = \left[\frac{(I_{(t)}V_{(s)})(L_{(ack)} + L_{(pack)}) + (I_{(r)}V_{(s)})}{R_{(b)}}\right] \tag{5}$$

For a zero authentication acknowledgment packet, Eq. (5) reduces to:

$$\left[E_{(s2r)_{(i)}}(L_{pack(i)}|success)\right] = \left[\frac{V_{(s)}(I_{(t)}L_{(pack)} + I_{(r)})}{R_{(b)}}\right] \tag{6}$$

Eq. (5) has been used to calculate the inter-node transmission energy consumption at different transmitting power level index for:

- n2n LR-WPAN;
- S2R-WBASN (the research work).

Results

Using the developed algorithm, the research results obtained are presented. Figs. 4 and 5 are the results of the generated ECG waveform for diabetic patients 1 and 2 showing the original noisy waveform and the filtered waveform.

Table 2 presents the result on respective ECG features extracted from diabetic patients 1 and 2 and the corresponding ECG key generated using the extracted features. The result as shown in Table 3 is the calculated values of the inter-node transmission energy consumption for n2n LR-WPAN and S2R-WBASN.

Fig. 6 is the result of inter-node energy consumption plot (graph) showing different node transmission energy utilised at different transmitting level index for n2n LR-WPAN and S2R-WBASN.

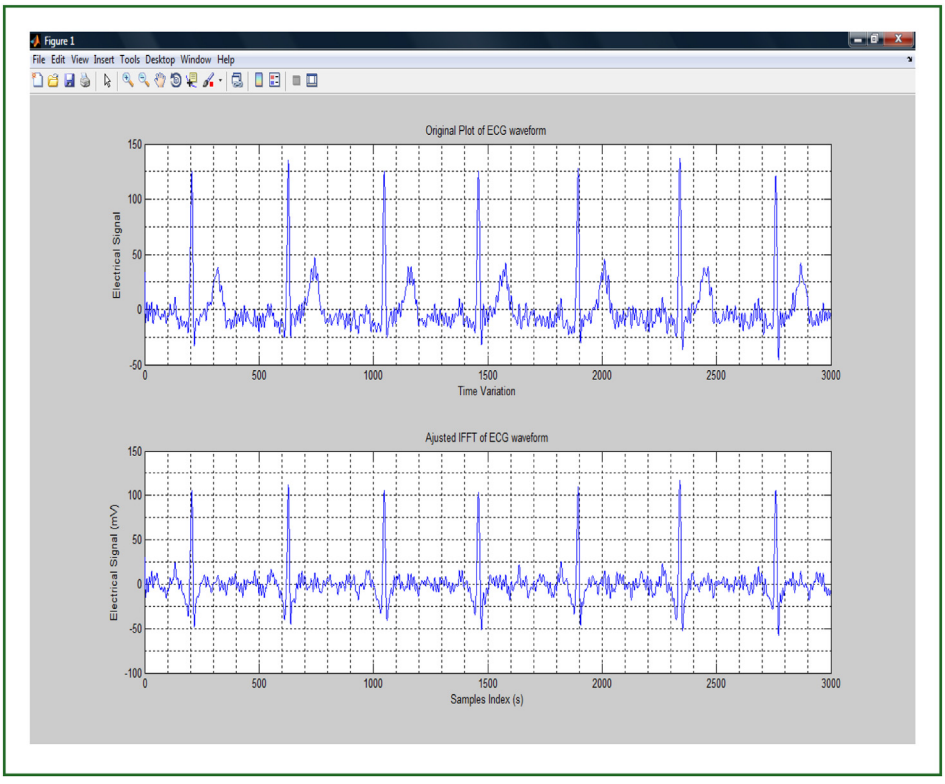

Figure 4. Generated ECG waveform for diabetic patient 1.
Création du tracé ECG pour le patient diabétique 1.

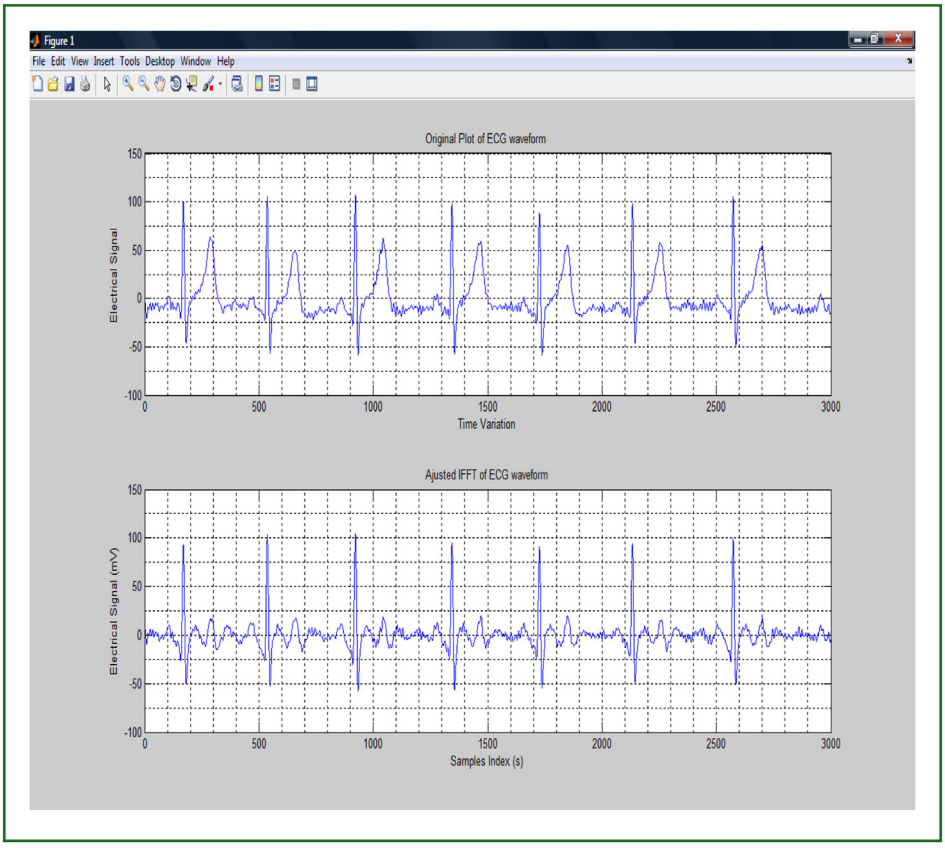

Figure 5. Generated ECG waveform for diabetic patient 2.
Création du tracé ECG pour le patient diabétique 2.

Table 2 ECG features extracted from diabetic patients 1 and 2.
Caractéristiques ECG extraites des patients diabétiques 1 et 2.

Heart Beat Index (*i*)	Diabetic Patient 1			Diabetic Patient 2		
	PLI1 (*i*)	IPI 1(*i*)	ECG Key 1 (*i*)	PLI 2 (*i*)	IPI 2 (*i*)	ECGKey 2 (*i*)
1	206	—	—	170	—	—
2	629	423	301.4526	537	367	532.7415
3	1047	418	243.0976	922	385	40.939
4	1459	412	854.5833	1343	421	2.0888e + 003
5	1895	436	−2.0008e + 003	1726	383	−1.0673e + 003
6	2339	444	1.34E + 03	2133	407	750.801
	2759	420	−2.4168e + 003	2573	440	−2.8043e + 003

Table 3 Node energy consumption values for N2N LR-WPAN and S2R-WBASN.
Valeurs de consommation énergétique des nœuds pour N2N LR-WPAN et S2R-WBASN.

Trans. Level Index (*i*)	E(S2R) WBASN(J)	E(n2n) LR-WPAN(J)
1	14.82984	20.21544
2	17.24904	23.52168
3	19.49544	26.59176
4	21.74184	29.66184
5	24.16104	32.96808
6	26.40744	36.03816
7	28.65384	39.10824
8	30.20904	41.23368

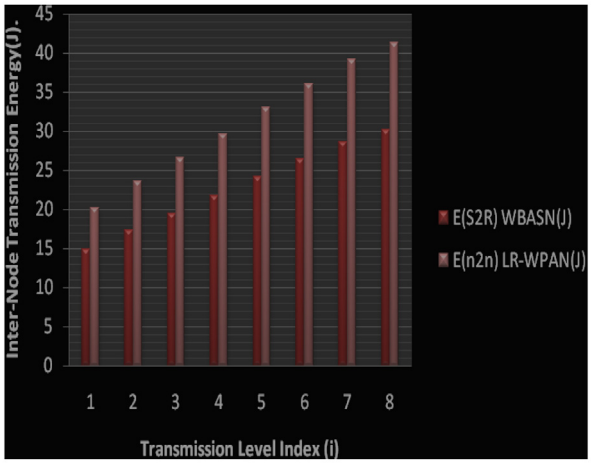

Figure 6. Inter-node energy consumption graph for n2n LR-WPAN and S2R-WBASN.
Graphique de la consommation énergétique inter-nœuds pour n2n LR-WPAN et S2R-WBASN.

Discussion

Figs. 4 and 5 present the results of the generated noisy and filtered ECG waveform. For every peak-point on the filtered ECG waveform, there is a corresponding PLI feature for each patient extracted on the sample index (*x*-axis). For every two successive peak-points, respective IPI features for the two patients are extracted. These are time variant features used to generate the authentication keys. The keys are observed to be dynamic for every successive beat and are also unpredictable.

From Table 2, at heart beat index 1, it can be seen that the ECG of diabetic patients 1 and 2 only generated respective PLI features; there is no IPI and there is no ECG key generation. At heart beat index 2, the patients' ECG generated respective PLI and IPI features and also different unpredictable ECG authentication keys. For every heart beat index in the two diabetic patients' ECG data sampled, there are unique time variant PLI and IPI features extracted and corresponding unpredictable ECG key generated.

The time variant ECG features (PLI and IPI) are biometric in nature, originating from the patient's physiological body signals. These features are different for each individual. Using these extracted biometric features to generate unpredictable authentication keys for inter-node transmission, the body can be said to be self-protective and WBASN security achieved.

Table 3 shows that inter-node transmission energy consumption for secured S2R-WBASN achieved a 25% energy reduction at every transmitting level index and can be said to be more energy efficient than n2n LR-WPAN. Twenty-five percent of node consumption energy was conserved for successful inter-node transmission in WBASN.

The results as presented in Fig. 6 show the inter-node energy consumption plot (graph) for n2n LR-WPAN and S2R-WBASN. From the results, the following has been observed:

- the energy consumption for successful n2n LR-WPAN at every transmitting level index is observed to be 25% higher than the energy consumption for successful S2R-WBASN. This is accounted for by the additional energy used by the nodes in n2n LR-WPAN to transmit and receive the authentication acknowledgement packets at every transmitting level index;
- the energy consumption for a successful S2R-WBASN at every transmitting level index is observed to be 25% lower. This energy reduction is accounted for by non-authentication acknowledgement packet considering that the nodes are on the same body generating the same authentication keys;
- the 25% reduction in energy consumption for S2R WBAN is also accounted for by non-additional energy used

by the nodes to transmit and receive the authentication acknowledgment packets at every transmitting level index;
- the energy plot in Fig. 6 can also provide the best transmitting level index for optimum node energy consumption. It can be seen from the graph that for the least energy consumption level at the nodes, the transmitting level index must not exceed index 1. At transmitting level index 1, the least energy is consumed for secured inter-node transmission. Node life span can be extended.

Conclusion

In this work, ECG feature biometric key generation algorithm was developed. Individually select ECG datasets of diabetic patients acquired from Physonet were processed using the fast Fourier transform method and noisy ECG signals were filtered out. Using a differential equation method, peak location index (PLI) and inter-pulse-interval (IPI) features of the heart beat were identified and extracted. Results of the research work showed extracted time variant ECG features for each selected dataset and unpredictable authentication keys for secure inter-node transmission. Using the energy consumption model of LR-WPAN Chipcon CC2420 specification, the performance of the algorithm was observed to be 25% energy efficient in terms of reduction in inter-node transmission energy consumption.

Disclosure of interest

The authors declare that they have no competing interest.

References

[1] Tan H, Wang Zhong S, Li Q. Body Sensor Network Security: an identity-based cryptography approach. In: Proceedings of the first ACM conference on wireless networks security. 2008. p. 148—53.
[2] Zhang G, Poon CC, Li Y, Zhang YT. A Biometric Method to Secure Telemedicine Systems. In: 31st Annual International Conference of the IEEE. 2006. p. 2—6.
[3] Van Dam K, Pitchers S, Barnard M. Body area networks: towards a wearable future. Munich, Germany: InProc. WWRF kick off meeting; 2001. p. 6—7.
[4] Latré B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks. Wireless Netw 2011;17(1):1—8.
[5] Sufi F, Han F, Khalil I, Hu J. A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. Secur Commun Netw 2011;4(5):515—24.
[6] Poon CC, Zhang YT, Bao SD. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. Commun Mag IEEE 2006;44(4):73—81.
[7] Ramli SN, Ahmad R, Abdollah MF, Dutkiewicz E. A biometric-based security for data authentication in wireless body area network (WBAN). In: Advanced Communication Technology (ICACT), 2013 15th International Conference. 2013. p. 998—1001.
[8] Wang H, Fang H, Xing L, Chen M. An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN). In: Communications (ICC), 2011 IEEE International Conference. 2011. p. 1—5.
[9] Chipcon SmartRF CC2420: 2.4 GHz IEEE 802.15.4/Zigbee RF transceiver for LR-WPAN. Retrieved September 4, 2015. Available from: http://www.chipcon.com.
[10] Gutierrez JA. IEEE Standard for Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPAN)-Draft D16. In: IEEE. 2002.
[11] Howitt I, Neto R, Wang J, Conrad JM. Extended energy model for the low rate WPAN. In: Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference. 2005.
[12] Zhang Z, Wang H, Vasilakos AV, Fang H. ECG-cryptography and authentication in body area networks. IEEE Trans Inf Technol Biomed 2012;16(6):1070—8.

Further reading

Bao SD, Poon CC, Zhang YT, Shen LF. Using the timing information of heartbeats as entity identifier to secure body sensor network. IEEE Trans Inf Technol Biomed 2008;12(6):772—9.

MIT-BIH. MIT-BIH arrhythmia database; 2013. Retrieved August 12, 2015. Available from Physionet database: http://physionet.org/physiobank/database/mitdb/.

Bao SD, Zhang YT, Shen LF. A new symmetric cryptosystem of body area sensor networks for telemedicine. In: Proc. 6th Asian—Pacific Conference on Medical and Biological Engineering. 2005.

Bao SD, Zhang YT, Shen LF. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems in Engineering, Medicine and Biology Society. In: IEEE-EMBS 2005. 27th Annual International Conference. 2005. p. 2455—8.

Venkatasubramanian KK, Banerjee A, Gupta SK. PSKA: usable and secure key agreement scheme for body area networks. IEEE Trans Inf Technol Biomed 2010;14(1):60—8.

Juels A, Sudan M. A fuzzy vault scheme. Des Codes Cryptography 2006;38(2):237—57.

Cherukuri S, Venkatasubramanian KK, Gupta SK. BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In: Parallel Processing Workshops, 2003. Proceedings. 2003. International Conference. 2003. p. 432—9.

Pan J, Tompkins WJ. A real-time QRS detection algorithm. IEEE Trans Inf Technol Biomed 1985:230—6.

Mitra SK, Kuo Y. Digital signal processing: a computer-based approach. New York: McGraw-Hill; 2006. p. 375—89.

Wac K, Bults R, van Beijnum B, Widya I, Jones V, Konstantas D, et al. Mobile patient monitoring: the MobiHealth system. Conf Proc IEEE Eng Med Biol Soc 2009:1238—41, http://dx.doi.org/10.1109/IEMBS.2009.5333477.

Biel L, Pettersson O, Philipson L, Wide P. ECG analysis: a new approach in human identification. IEEE Trans Instrum Meas 2001;50(3):808—12.