Journal of Cardiovascular and Thoracic Research, 2013, 5(3), 119-124
doi: 10.5681/jcvtr.2013.025
http://journals.tbzmed.ac.ir/JCVTR

Home and Clinical Cardiovascular Care Center (H4C): a Framework for Integrating Body Sensor Networks and QTRU Cryptography System

Ali Zakerolhosseini[1], Massoud Sokouti[1*], Massoud Pezeshkian[2]

[1]*Faculty of Electrical & Computer Engineering, Shahid Beheshti University, Tehran, Iran*
[2]*Cardiovascular Research Center, Tabriz University of Medical Sciences, Tabriz, Iran*

ARTICLE INFO

Article Type:
Original Article

Article History:
Received: 17 July 2013
Accepted: 2 Sep 2013

Keywords:
QTRU Cryptography
Body Sensor Network
Personal Digital Access
Heart Attack
Wireless Networks

ABSTRACT

Quick responds to heart attack patients before arriving to hospital is a very important factor. In this paper, a combined model of Body Sensor Network and Personal Digital Access using QTRU cipher algorithm in Wifi networks is presented to efficiently overcome these life threatening attacks. The algorithm for optimizing the routing paths between sensor nodes and an algorithm for reducing the power consumption are also applied for achieving the best performance by this model. This system is consumes low power and has encrypting and decrypting processes. It also has an efficient routing path in a fast manner.

Introduction

Recent reports show that coronary artery disease (CAD) risk factors have been increased among Iranian people.[1] Moreover, cardiovascular diseases are one of the important results of these risk factors which lead to high rate of mortality and disability according to WHO reports on worldwide people.[2-4] Both the Heart rhythmic disorders and the arrhythmia are popular alarm signs in patients who are suffering from heart disease. Although, ECG (Electrocardiogram) can detect myocardial infarctions, however exercising and Holter monitoring tests are more accurate for medical diagnosing than a simple experimental diagnosis. Analysis of ECG with or without exercising tests is being done by a medical doctor and there are challenges over these clinical cases.[5]

These days, Wireless Sensor Network (WSN) system is being used for cardiac monitoring which transfers ECG signals to Personal Digital Assistant (PDA) by using a cellular network. As a result, the combination of WSN and computer electronic infrastructures can assist the healthcare monitoring era efficiently.[6-9]

Some examples of WSN hardware designs are as follows: *(i)* Berkeley's Mica2, *(ii)* ETH's *(iii)* BTNodes, *(iv)* Intel's iMote, *(v)* UCC's DSYS25, *(vi)* SmartITs, and *(vii)* MITes.[9-12] The Body Sensor Network (BSN) is a hardware platform that it uses a wide range of bandwidth because of using the IEEE 802.15.4 standard. In the design of this platform, a lot of sensors are used to detect signals easily; the most of them are those which can detect Physiologic signals whereas stress and nervous tensions signals are omitted from the main signals.[13]

The security of data among medical doctor, patient, and ICU is an important issue which should be well addressed in the implementation of this system. The cryptographic algorithms such as RSA (i.e., stands for Ron Rivest, Adi Shamir and Leonard Adleman) and ECC (i.e. Elliptic Curve Cryptography) have a great security for transferring data through an unsecured channel but they are slow in encrypting and decrypting processes. The NTRU encryption system has a hard and unbreakable core which is standardized by IEEE with the most acceptable cryptography algorithm and because of its high speed and promising security, it can be implemented in WSNs. The most advantage of NTRU system over RSA and ECC is based on its lattice-based architecture which has the complexity of $O(n^2)$. This means it is the cheapest, fastest and the most effective cipher algorithm.[14,15]

In this article, we present a combination of Quaternion algebra with NTRU in WSN for healthcare and cardiovascular disease in order to increase the security of data transferred in WSNs environments. The new system is known as QTRU with the ability of parallel processing and encrypting four vectors at the same time. The complexity orders of encrypting and decrypting in QTRU system is

***Corresponding author:** Massoud Sokouti, E-mail: m_sokouti@yahoo.com

$O(4n^2)$ and the dimension of lattice matrix which is needed to attack this cipher is $8N\times8N$. Having the high speed property in encrypting and decrypting is an advantage of QTRU over NTRU with degree of four, at the same security level. Also, we represent algorithms for energy optimization between WSN nodes and for reducing hops between modes in order to reduce the possible distance rate between WSN nodes.

NTRU

The first version of NTRU cipher algorithm was proposed by Silverman *et al.* in 1998.[14] This system is based on lattice using Multi sentences ring complexity which uses matrices. It uses Shortest Vector Problem (SVP) to reduce its lattices. The basis of NTRU is the ring of $Z[x]/(x^N-1)$ and is described by the complexity of the ring, while N is a primitive number. In these rings, complexity order of adding operation is $O(n)$ and the complexity order of multiplying is $O(n^2)$.[16] Using this ring in the NTRU structure provides high speed and efficiency. According to[16,17], we define three following rings: $R= Z[x]/(x^N-1)$, $R_p=Z/Z_p[x]/x^N-1$, $R_q=Z/Z_q[x]/x^N-1$.

Key Generation

Let d_f, d_g, d_φ and d_m be constant integer numbers less than N which are known as public parameters, N is a prime number, p and q are two co-prime numbers which are relatively prime and q is a number more greater than p. To create an NTRU key, at first two small polynomials g and f are generated randomly. The polynomial f must be invertible in R_p *and* R_q. The inverse of f *over* R_p *and* R_q are computed using the extended Euclidian algorithm. The two inverses are denoted by f_p^{-1} and f_q^{-1}, respectively. Hence, we have $f_p^{-1}*f\equiv 1\,(\mathrm{mod}\,p)$, $f_q^{-1}*f\equiv 1\,(\mathrm{mod}\,q)$. While f,g,f_p^{-1},f_q^{-1} are kept private, the public key h is computed based on formula (1):

$$h=f_q^{-1}*g\,(\mathrm{mod}\,q) \qquad (1)$$

Encrypting process

By considering φ as ephemeral key and converting the input message to a polynomial m, the cipher text is computed as below [i.e., formula (2)]:

$$e=p.h*\varphi+m\,(\mathrm{mod}\,q) \qquad (2)$$

In this step, the number of total multiplications is N^2 where that of additions is N mod q.

Decrypting process

After receiving polynomial e, the encrypted message can be decrypted by using the private key f and the formula (3) is used for this calculation:

$$\begin{aligned}&f*e\,(\mathrm{mod}\,q)=f*(p.h*\varphi+m)\,(\mathrm{mod}\,q)\\&=p.f*h*\varphi+f*m\,(\mathrm{mod}\,q)\\&=p.f*f_q^{-1}*g*\varphi+f*m\,(\mathrm{mod}\,q)\\&=p.q*\varphi+f*m\,(\mathrm{mod}\,q)\end{aligned} \qquad (3)$$

QTRU

The QTRU cipher system[18] uses the Quaternion algebra, so a little information about this algebra is needed to be described. The real quaternion, denoted by H is a vector space of dimension 4 over R.

The two lattice spaces denoted by L_p, L_q are being described in quaternion algebra as below:

$$L_p:=\{a+bi+cj+dk\mid a,b,c,d\in GF(p)\}. \qquad (4)$$

$$L_q:=\{a+bi+cj+dk\mid a,b,c,d\in GF(q)\} \qquad (5)$$

In quaternion algebra, two polynomials $Z_p[x]/(x^N-1)$, $Z_q[x]/(x^N-1)$ are described as follows:

$$A_0=\left(\frac{-1,-1}{Z_p[x]/(x^N-1)}\right)=\{f_0(x)+f_1(x).i+f_2(x).j+f_3(x).k\mid f_0,f_1,f_2,f_3\in Z_p[x]/(x^N-1),\\ i^2=-1,j^2=-1,ij=-ji=k\}$$

(6)

$$A_1=\left(\frac{-1,-1}{Z_q[x]/(x^N-1)}\right)=\{g_0(x)+g_1(x).i+g_2(x).j+g_3(x).k\mid g_0,g_1,g_2,g_3\in Z_q[x]/(x^N-1),\\ i^2=-1,j^2=-1,ij=-ji=k\}$$

(7)

For generating public keys and private keys, two quaternion polynomials are generated randomly based on formula (8):

$$\vec{F}=f_0+f_1.i+f_2.j+f_3.k\ \textit{such that}\ f_0,f_1,f_2,f_3\in L_f \qquad (8)$$

$$\vec{G}=g_0+g_1.i+g_2.j+g_3.k\ \textit{such that}\ g_0,g_1,g_2,g_3\in L_g \qquad (9)$$

Where $\circ$ is used for multiplying in quaternion algebra and is computed as follows:

$$\begin{aligned}\vec{F}\circ\vec{G}&=(f_0+f_1.i+f_2.j+f_3.k)\circ(g_0+g_1.i+g_2.j+g_3.k)\\&=(f_0*g_0-f_1*g_1-f_3*g_3-f_2*g_2)\\&+(f_0*g_1+f_1*g_0-f_3*g_2+f_2*g_3).i\\&+(f_3*g_1+f_2*g_0+f_0*g_2-f_1*g_3).j\\&+(f_1*g_2+f_0*g_3-f_2*g_1+f_3*g_0).k.\end{aligned} \qquad (10)$$

Where $\vec{F}$ must be invertible in $A_0=\left(\dfrac{-1,-1}{Z_p[x]/(x^N-1)}\right)$ and $A_1=\left(\dfrac{-1,-1}{Z_q[x]/(x^N-1)}\right)$.

$\vec{F}_p,\vec{F}_q$ are computed as follows:

$$\vec{F}_p = \langle (f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1} \; over \; Z_p[x]/(x^N - 1) \rangle \circ \vec{F}^* = \mu_0 + \mu_1.i + \mu_2.j + \mu_3.k$$

(11)

$$\vec{F}_q = \langle (f_0^2 + f_1^2 + f_2^2 + f_3^2)^{-1} \; over \; Z_q[x]/(x^N - 1) \rangle \circ \vec{F}^* = \eta_0 + \eta_1.i + \eta_2.j + \eta_3.k$$

(12)

The public key will be calculated according to formula (13):

$$\begin{aligned} &\vec{H} = \vec{F}_q \circ \vec{G} = \\ &(\eta_0 * g_0 - \eta_1 * g_1 - \eta_3 * g_3 - \eta_2 * g_2) + \\ &+(\eta_0 * g_1 + \eta_1 * g_0 - \eta_3 * g_2 + \eta_2 * g_3).i \\ &+(\eta_3 * g_1 + \eta_2 * g_0 + \eta_0 * g_2 - \eta_1 * g_3).j \\ &+(\eta_1 * g_2 + \eta_0 * g_3 - \eta_2 * g_1 + \eta_3 * g_0).k. \end{aligned} \tag{13}$$

Where $\vec{F}, \vec{F}_p, \vec{F}_q$ are private and can be used in decrypting process. Although, the QTRU cipher system is 16 times slower than NTRU cipher system, however QTRU can work on small dimensions without reducing the system's security. The message and Blinding Quaternions are shown as below:

$$\begin{aligned} &\vec{M} = m_0 + m_1.i + m_2.j + m_3.k \\ &\left\{ m_0 \overset{\Delta}{=} m_0(x), m_1 \overset{\Delta}{=} m_1(x), m_2 \overset{\Delta}{=} m_2(x), m_3 \overset{\Delta}{=} m_3(x) \right\} \in L_m \end{aligned} \tag{14}$$

$$\begin{aligned} &\vec{\varphi} = \varphi_0 + \varphi_1.i + \varphi_2.j + \varphi_3.k \\ &\left\{ \varphi_0 \overset{\Delta}{=} \varphi_0(x), \varphi_1 \overset{\Delta}{=} \varphi_1(x), \varphi_2 \overset{\Delta}{=} \varphi_2(x), \varphi_3 \overset{\Delta}{=} \varphi_3(x) \right\} \in L_\varphi \end{aligned} \tag{15}$$

The cipher text can be calculated by the following equation and we can decrypt the cipher text by formula (17):

$$\vec{E} = p.\vec{H} \circ \varphi + \vec{M} \tag{16}$$

$$\begin{aligned} &\vec{F} \circ \vec{E} = (\vec{F} \circ (p.\vec{H} \circ \vec{\varphi} + \vec{M}) \; (\text{mod } q) \\ &= (\vec{F} \circ p.\vec{H} \circ \vec{\varphi} + \vec{F} \circ \vec{M}) \; (\text{mod } q) \\ &= (p.\vec{F} \circ \vec{F}_q \circ \vec{G} \circ \vec{\varphi} + \vec{F} \circ \vec{M} \; (\text{mod } q) \\ &= (p.\vec{G} \circ \vec{\varphi} + \vec{F} \circ \vec{M}). \end{aligned} \tag{17}$$

The new system has a parallel processing feature which can encrypt 4 vectors at the same time. The complexity order of encrypting and decrypting of QTRU system is $O(4n^2)$ and the dimension of lattice matrix which is needed to attack this cipher is *8N×8N*. As mentioned before, the high speed in encrypting and decrypting processes is counted as an advantage of QTRU over NTRU with degree 4, at the same security level.

BSN and its architecture design

BSN[13] is a WSN hardware platform which works on a wide range bandwidth using the IEEE 802.15.4 standard. It incorporates the wireless physiological sensors for measuring the status of the patient. In Figure 1 we can see a simple BSN on the human body. To minimize the usage of bandwidth, a BSN and a PDA is used before sending the data to the server. The architecture design of BSN is illustrated in Figure 2.

This node uses Texas Instrument (TI) MSP40 16-bit ultra low power RISC processor accompanied by a flash memory 60 KB+256 B, 2 KB RAM, 12-bit ADC and 6 analog channels. The throughput bandwidth is 250 kbps with a range of over fifty meters. The flash memory is used for either storing or buffering the data. The operating system (OS) which is used in BSN is TinyOS by U.C Berkeley. Being small, open source and efficient power usage sensors are the advantages of this OS. It has small files designers that can choose the components they need. Also, the OS manages the hardware and the wireless network, takes sensor measurements, makes sensor routing decisions, and finally reduces the usage of power. Since the TI microcontroller is used, the BSN node only needs 0.01 mA in active mode and 1.3 mA in calculating mode. In the BSN architecture, a lot of wireless biosensors such as 3-lead ECG, 2-lead ECG strip, and context sensors such as accelerometers and also temperature and humidity sensors are being used. The compact flash BSN card in the PDA can gather the sensor signals. Furthermore, the PDA can display, analyze and process the sensor signals as

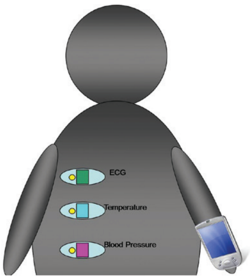

Figure 1. Body Sensor Network

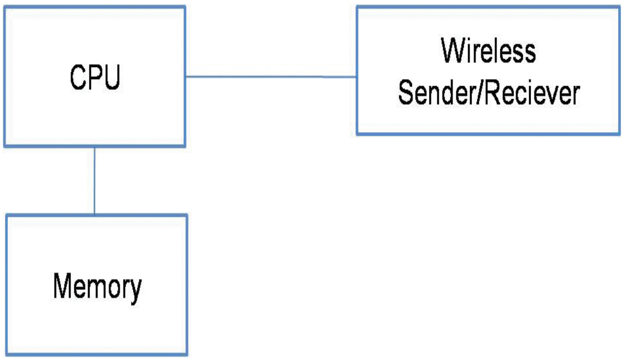

Figure 2. Architecture design of BSN

well as working as a router too. The transmission of sensor networks is being done through a Wifi or GPRS network.

Probabilistic distance vector for sensor networks

The probabilistic distance distributions are used for random sensor networks that can calculate the distance and send data with high accuracy.[19] The two nodes (X_1, Y_1) and (X_2, Y_2) are supposed, the distribution of node distance $P(D \leq d)$ is needed to be calculated, where $D=\sqrt{(X_1-X_2)^2+(Y_1-Y_2)^2}$

In grid-based clustering scheme, there are two cases of cluster head communications: between cluster heads in diagonal adjacent grids or parallel grids, such as *PQ* and *RS* in Figure 3.

We will suppose non-uniform griding with a fixed ratio *q* is a special case of variable-size griding.

Two random nodes in diagonal neighbor grids

By normalizing the *A* × *A* sensing field to a unit-size square as shown in Figure 3. The grids 1 and 3 are diagonal squares with size of (1-q^2) and q^2(1-q^2) respectively. By using the Heaviside Step Function $H(x)$ we can formulate the coordinate distributions for *P* and *Q* as follows:

$$\begin{cases} f_{X1}(x)=f_{Y1}(x)=\dfrac{H(x)-H[x-(1-q)]}{1-q} \\ f_{Y2}(x)=f_{Y2}(x)=\dfrac{H[x+q(1-q)]-H(x)}{q(1-q)} \end{cases} \qquad (18)$$

Where

$$H(x)=\begin{cases} 0 & x<0 \\ 1 & x \geq 0 \end{cases}$$

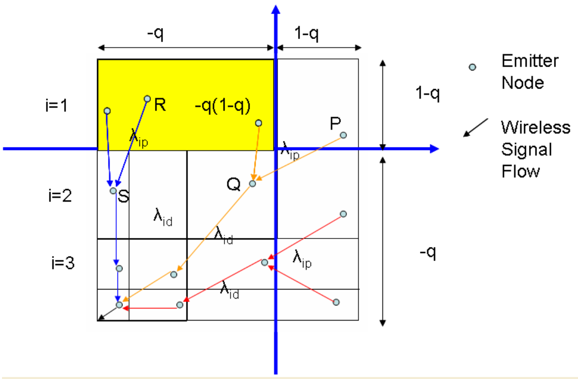

Figure 3. Non-uniform griding with size ratio *q*

X_1, $Y_1 \approx U$ [0, 1-*q*] and X_2, $Y_2 \approx U$[-*q*(1-*q*),0]

Two random nodes in parallel neighbor grids

The grids 2 and 4 shown in Figure 2 are parallel rectangles with size of (1-*q*)×*q* and *q*(1-*q*)×q_2 respectively. For the nodes in these parallel rectangles, the coordinate distribution is formulated as below:

$$\begin{cases} f_{X1}(x)=\dfrac{H(x+q)-H(x)}{q} \\ f_{Y1}(x)=\dfrac{H(x)-H[x-(1-q)]}{(1-q)} \end{cases} \qquad (19)$$

$$\begin{cases} f_{X2}(x)=\dfrac{H(x+q)-H(x+q(1-q))}{q^2} \\ f_{Y2}(x)=\dfrac{H[(x+q(1-q)]-H(x)}{q(1-q)} \end{cases} \qquad (20)$$

Now let $V=X_1-X_2$ or $V=Y_1-Y_2$, $S=V^2$, $Z=S_X+S_Y$ and $D=\sqrt{Z}$ so we can obtain f_D(d). According to BT node Platform we can easily find the Distance distribution.[9]

Probabilistic energy optimization

It is very important to reduce the usage of energy in wireless sensor networks.[19] According to Barroso *et al.* study[10] the energy which is consumed by the radio transmitter is calculated by equation (21):

$$E_{Tx}=\lambda\varepsilon\int x^a f_D(x)dx \qquad (21)$$

λ is a data transmitter rate, *ε* is a constant related to the environment, and a is known as the path loss exponent. The traffic pattern of "many to one" in WSNs is also illustrated in Figure 3.

Let *Ei* be the energy consumed in the *i*-th ring:

$$Ei=\lambda_i(E_{Re}+E_{Te})+\ \lambda_i E_{Tx} \qquad (22)$$

λ_i is the data rate going through the *i*-th ring. The parameters E_{RE} and E_{TE} are the energies consumed by the receiver and transmitter circuitry, and E_{TX} is used by the transmitter power amplifier. According to Pentland *et al.* study[7] we have $E_{Re}=E_{Te}=E_e$. so,

$$Ei=\lambda_i(2E_e+E_{Tx}) \qquad (23)$$

The aggregated data can be divided into two parts: between parallel rectangles λ_{ip}, and between diagonal squares λ_{id}, i.e., $\lambda_{i=2}\lambda_{ip}+\lambda_{id}$ and ρ is the node density. The λ_{ip} and λ_{id} parameters can be calculated as follows:

$$\lambda_{ip}=\frac{A^2q}{1+q}(1-q^{2i})\rho\lambda$$
$$\lambda_{id}=\frac{A^2(1-q)}{1+q}(1-q^{2i})\rho\lambda \qquad (24)$$

Therefore,

$$E_i=2\lambda_{ip}(2E_e+\varepsilon\int x^a f_{D_{Par}}(x)dx)+\lambda_{id}(2E_e+\varepsilon\int x^a f_{D_{Diag}}(x)dx) \qquad (25)$$

For minimizing the total network energy consumption we have the following equation:

$$\min\sum_{i=1}^{K}E_i$$
$$s.t. \quad Aq^{K-1}>r_0$$
$$Aq^k \leq r_0$$

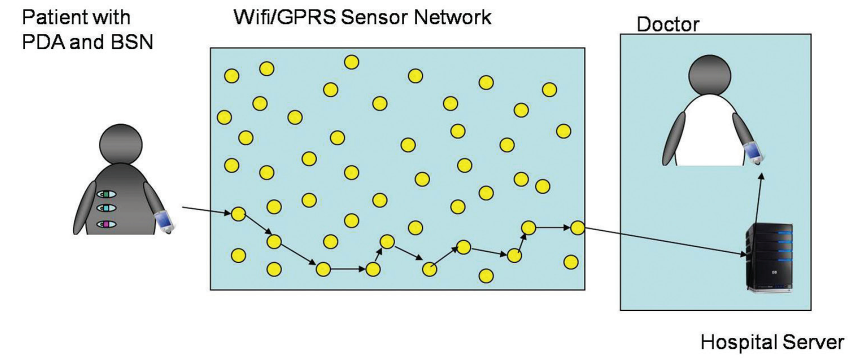

Figure 4. Implementation of proposed framework

Where *r*0 is the minimal distance between wireless transceivers, and *K* is the maximum number of hops from the source node to the sink.

Implementation of framework

Initially assume the patient is stationed in his/her house. The patient is relaxed and the ECG and the body temperature and the blood pressure sensors do not detect any suspicious. Suddenly, the sensors detect heart rhythmic disorders, arrhythmia, and a change in the body temperature and the blood pressure. The alert signals are accordingly sent to the PDA (i.e., mostly ECG signals). The BSN which is located inside the PDA does a processes these signals and makes a decision on whether the occurred condition is life threatening or not. If the condition is life threatening, an appropriate signal is generated and routed to the PDA. As previously indicated, the PDA also performs as a router as initially encrypts the alert data signals. The importance of encrypting these signals lie on protecting patients information. These information regarding patient health is secret and except the doctor no other persons would have access to these information's Also other hospitals can't decrypt other patients' data which do not belong to their hospital. The encryption is being done by the QTRU algorithm. We used this cipher system since it is faster in comparison to NTRU in 4 dimensions. In this way, the speed of transferring data will increase. On the other hand, there is a Wifi or GPRS network between the server of the hospital and patient's PDA which includes lots of sensor networks for receiving data signals and transferring them to the others just as a router. In this part, the best and closest path to the server should be chosen which consumes small amount of power. When the data signal has arrived at the server of the hospital, the server immediately decrypts the data and alerts the emergency. Also, it sends the encrypted data to the doctor who decrypts the data by his PDA and checks the condition of the patient and as a result may make the doctor become ready for the operation if necessary. The implementation of this scenario is shown in Figure 4. Also, this system can work inside the hospitals so the Wifi or GPRS Sensor Network is not needed and transfer of data is done directly between the server of the hospital and the patient's PDA and doctor's PDA.

Discussion

Cardiovascular disease is one of the most important reasons of sudden death in Iran. In this study we present a low consuming power and high speed cryptographic Body Sensor Network architecture which is used to detect arrhythmias in cardiovascular disease patients. Wifi or GPRS Sensor networks are the main related networks that are mainly addressed to BSNs and PDAs and server of hospital by using QTRU cipher system in this paper. It can also be used by patients for self-monitoring or alerting the doctors and ICU healthcare personnel. Generally, usual health care systems perform monitoring and analysis for a variety of cardiac care functions but our presented system can detect arrhythmias in cardiovascular patients with high speed and security. The QTRU cryptosystem can encrypt and decrypt 4 vectors at the same time with the complexity order of $O(4n^2)$ while NTRU cryptosystem with 4 dimensions can encrypt and decrypt with the complexity order of $O(16n^2)$. Although, they are at the same security level, however QTRU cryptosystem is faster than NTRU cryptosystem in 4 dimensions. Also we used probabilistic distance vector for Sensor Networks in order to reduce the hops between WSN node and increasing the speed of transferring and routing process. For reducing the usage of power, the Probabilistic Energy optimization is used. Energy optimization is very important since most of WSNs use rechargeable batteries.

Conclusion

In this paper a new H4C system is proposed by which the number of human deaths resulted by cardiovascular disease can be reduced. This system is a very fast and low power consumption system that uses the cheap chips in comparison to other healthcare chips. The encryption and decryption algorithm used for securing the insecure channel of communication reduces the calculations.

Additionally, the methods used for reducing distances and energy make the overall operations and functions faster.

Ethical issues: The study was approved by the ethics committee of the University.

Competing interests: The authors had no competing interests to declare in relation to this article.

References

1. Hatmi ZN, Tahvildari S, Gafarzadeh Motlag A, Sabouri Kashani A. Prevalence of coronary artery disease risk factors in Iran: a population based survey. **BMC Cardiovasc Disord** 2007;7:32.
2. Braunwald S. Heart disease: a textbook of cardiovascular medicines. 7th ed. Philadelphia: WB Saunders; 2005.
3. Campbell RL, Banner R, Konick-McMahan J, Naylor MD. Discharge planning and home follow-up of the elderly patient with heart failure. **Nurs Clin North Am** 1998;33:497-513.
4. WHO. Cardiovascular diseases. [cited 2012 Dec]. Available from: http://www.who.int/cardiovascular_diseases/en/
5. Standing P, Dent M, Craig A, Glenville B. Changes in referral patterns to cardiac out-patient clinics with ambulatory ECG monitoring in general practice. **Br J Cardiol** 2001;8:396-8.
6. Liszka KJ, Mackin MA, Lichter MJ, York DW, Pillai D, Rosenbaum DS. Keeping a beat on the Heart. **IEEE Pervasive Computing** 2004; 3:42-9.
7. Pentland A. Healthwear: Medical Technology Becomes Wearable. **IEEE Computer** 2004;37:42-9.
8. Ross PE. Managing care through the air. **IEEE Spectrum** 2004;41;14-9.
9. BTnode Platform. [cited 2013 Feb]. Available from: http://www.btnode.ethz.ch
10. Barroso A, Benson J, Murphy T, Roedig U, Sreenan C, Barton J, *et al*. The DSYS25 Sensor Platform. Proceedings of the 2nd international conference on Embedded networked sensor systems. New York: ACM, 2004. p. 314-314.
11. Intel Labs. [cited 2013 Feb]. Available from: http://www.intel.com/research/exploratory/motes.htm
12. TinyOS. [cited 2013 Feb]. Available from: http://www.tinyos.net
13. Lo BPL, Thiemjarus S, Panousopoulou A, Yang GZ. Bioinspired Design for Body Sensor Networks [Life Sciences]. **IEEE Signal Processing Magazine** 2013; 30:165-70.
14. Hoffstein J, Pipher J, Silverman J. NTRU: A new high speed public key cryptosystem. Algorithmic Mumber Theory (ANTS III). Lecture Notes in Computer Science 1998;143:267-88.
15. Bailey DV, Coffin D, Elbirt A, Silverman JH, Woodbury AD. NTRU in Constrained Devices, Cryptographic Hardware and Embeded Systems, CHES 2001 Lecture Notes in Computer Science, Third International Workshop, Proceedings, Springer-Verlag, Paris, France, 2001; 2162: 262-272.
16. Pipher J. NTRU Cryptosystems. Lectures on the NTRU encryption algorithm and digital signature, 2005.
17. Kouzmenko R. Generalizations of the NTRU cryptosystem. [Master's thesis]. Polytechnique, Montreal, Canada, 2006.
18. Malekian E, Zakerolhosseini A, Mashatan A. Qtru: Quaternionic Version of the NTRU Public-Key Cryprosystems. **ISeCure** 2011;3:29
19. Zhuang Y, Pan J, Cai L. Minimizing energy consumption with probabilistic distance models in wireless sensor networks. INFOCOM, 2010 Proceedings IEEE, 14-19 March 2010, p. 1-9.