ENVIRONMENTAL AND EARTH SCIENCES RESEARCH JOURNAL

ISSN: 2369-5668 (Print), 2369-5676 (Online)
Vol. 4, No. 2, June 2017, pp. 39-44
DOI: 10.18280/eesrj.040203

A publication of IIETA

IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

http://www.iieta.org/Journals/EESRJ

Increase in lifetime by harvested energy and analysis of RC5 along with efficient energy consumption in WBAN

Jayanti P. Rudra*, Mrittika Chakraborty

Department of Information Technology MCKVIE, Howrah 711204, India

Email: pathak.jayanti@rediffmail.com

ABSTRACT

Wireless Body Area Networks (WBANs) have emerged as a new technology for health care systems. It allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. Limited energy capacity to sustain the WBAN nodes for an extended period of time has always been a matter of concern. In this paper, we compare and analyze different types of standard symmetric cryptography based algorithms to be implemented in WBANs for security purpose. RC5 being a highly efficient and flexible cryptographic algorithm, with many flexible parameters (key size, block size, number of rounds) can be adjusted to tradeoff security strength with power consumption and computational overhead. Thus, RC5 with suitable parameters may perform well for WBAN applications with different data size. We propose an algorithm comprising of operating the sensor nodes in rest modes that is both in sleep as well as active mode accordingly, based on sets of data transmissions. Equal priority is set for all the cluster members (CMs) along with a fixed cluster head (CH). The concept of energy harvesting has also been implemented in our algorithm to maximize the power supply. Increase in the network lifetime using both rest mode and increased energy supply has been observed using different case studies.

Keywords: Cluster Head, Cluster Members, Cryptography, Health Care.

1. INTRODUCTION

The wireless body area network (WBAN) has emerged as a new technology for healthcare. It allows the data of a patient's vital body parameters and movements to be collected by small, wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. WBAN has been integrated into various human related applications like medical healthcare services, assistance to people with disabilities to promote healthy lifestyle. Instead of being measured face-to-face with WBANs patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. With this come two crucial issues that is meant to analyze upon which are energy consumption and security of the patient's data transmission.

The sensor nodes worn by patients in a WBAN collect and process large amount of data for continuous health monitoring analysis. However, as the data being dealt with is private and sensitive, even protected by law in many countries, secure data transmission in WBAN is one of the key issues and needs to be addressed before it can be widely deployed. The communication of the sensitive data among the sensors to health servers give rise to data security concerns like integrity, confidentiality, authentication, etc. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments. To design data security and privacy mechanisms for WBANs, there are a number of challenges one must overcome, including how to make tough balances between security, efficiency, and practicality. Stringent resource constraints on devices within a WBAN, especially the sensor nodes, basically require the security mechanisms to be as lightweight as possible.

The limited energy supply on sensor nodes becomes the bottleneck for data transmission and lifetime. One method to prolong the lifetime of the node is to reduce the energy consumption of the respective nodes by several consumption mechanisms. Energy harvesting schemes may also appear as an ultimate solution to the problems of energy consumption if used efficiently. Network lifetime may be then increased to a proportionally extended period thus ensuring longer longevity of the sensors and their functionalities.

This paper focuses on the study of the both major issues of security and energy consumption and finding solution of the same so that patient-related data is kept authentic, confidential at a node or local server along with reduced energy consumption mechanisms.

In WBANs the patient-related data is vital, and data if distorted would lead to disastrous consequences. Thus, data integrity needs to be dynamically protected all the time. In particular, we should be able to not only detect modification of data at end users, but also check and detect that during storage periods, in order to discover potential malicious modification in advance and alert the user.

Recent developments in the communication technologies have made it possible to support accurate operation and long lifetime of WBANs. Besides the research on reduced energy consumption techniques, development of energy harvesters is one of the keystones of the global ongoing research on WBANS as this would make the wireless sensing devices meshed in network form to be self-powered and cost effective to a huge extent.

Based on that, the thermal energy, solar and vibration energy based harvesting system can be designed and implemented for powering the sensor nodes. Energy harvesting that depends on a single energy source is not reliable. In order to obtain energy as much as possible, it is to be designed with hybrid energy harvesting system which can collect various kinds of energy from environment. For example, the lifetime of nodes for wireless body area based sensor nodes can be extended using the solar and thermal hybrid system. Piezoelectric harvesting system can also be added to the previously mentioned system to maximize the power output as a whole.

Therefore, it is seen that WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. Also, a lot of challenges and obstacles need to be tackled with each node getting adequate energy to complete the data acquisition, processing, transmission, and so forth in a well secured network.

2. RC5 AS A SECURITY SOLUTION

In recent research studies, many security schemes have been suggested for Wireless Body Area Network (WBANs), however very few of them can actually be used in WBANs. Generally symmetric cryptography based algorithms are used in case of wireless sensor nodes as asymmetric key based algorithms are slow with large execution times. The complexity that is required for making mathematically-paired keys demands calculation time and the extra resource-requirements for two separate keys: public and secret. The public key is used for message encryption and the secret key for decryption. In resource-constrained nodes, it is impractical to use a cryptosystem with high computation, communication and storage overheads. We know that a sensor node is equipped with one or more integrated sensors, embedded processors with limited capability, and short-range radio communication ability. These sensor nodes are powered using batteries with small capacity. Unlike in standard wireless networks, wireless sensor nodes are often deployed in unattended environments, making it difficult to change their batteries. These severe constraints have a direct impact on the lifetime of a sensor node. As a result, energy conservation becomes of utmost importance in WBANs to prolong the lifetime of sensor nodes. From this point, it is clear that a cluster node is basically associated with three main constraints that include i) energy consumption, ii) secure data transmission, and iii) time or computational overhead that needs to be dealt with. Among the various available security algorithms each security algorithm possesses different security properties and provides varying level of protection. RC5 is observed to be one such algorithm that is known to provide a better solution to these resources constrained based systems because of the following reasons:

RC5 is simple and easy to implement using only low microcontroller operations having low memory requirements.

Also, the standard key length for RC5 is 128 bits which helps it to overcome attacks like differential and linear cryptanalysis attacks.

The same lightweight algorithm can be used for both encryption and decryption and heavy use of data-dependent rotations provides high security.

The RC5 block cipher has built-in parameter variability that provides flexibility at all levels of security and efficiency.

Table 1. Represents the variety of parameters and values used in the RC5 operations in [3]

Rc5 Parameters	
Parameters	Values
Word Size (W)	16, 32, 64 bits
Block Size (2w)	32, 64, 128 bits
The Number of Rounds (R)	0 – 255
Key Length (B)	0 - 2040 bits

2.1 Algorithm

1. Start.
2. Firstly the input plain text is to be divided into two equals- sized blocks assuming them to be as A and B.
3. The first sub key s [0] is to be added to A and the second sub keys [1] is to be added to B that leads to the Generation of C and D blocks respectively.
4. Next the C and D generated above will be XORed together to form E
5. Then E is shifted circularly by D positions.
6. E is then added to the next sub key which is s [2] for the first round (Generally it is s [2i] for any round, where i starts with 1), that produces output F as the output.
7. Now D and F are XORed together in order to generate G.
8. G is shifted circularly by F positions.
9. In this step G is added to the next sub key which is s [3] for the first round (Generally it is considered to be s [2i+1] for any round where i starts with 1). This process produces H as the output.
10. In this step, in order to check the completion of all the rounds the following sub-steps are carried out:
    - i is incremented by 1
    - if i<r
    - call F as C again
    - call H as D again
    - go to step 4
    - else stop
    - end if
11. End.

2.2 Comparison of RC5 with other algorithms

Apart from the previously mentioned points it is also seen that when RC5 is compared to other existing security algorithms it still proves to be an efficient and a secure solution for WBAN ensuring secured transmission of patient related data's. The following points cover the inherent advantages of RC5 and also bring about a brief idea about the efficiency and security provided by RC5 when compared to other existing security algorithms:

Although the National Institute of Standards and Technology’s(NIST) AES cipher is more widespread with inbuilt hardware support among some microcontroller manufacturers, AES is found slower and has higher memory requirements than RC5, which makes RC5 a better cipher solution for devices with limited resources as in case of WBANS.

For different length encryption data, the energy consumption of RC5 is significantly lower than that of AES and DES. The design of RC5 is concise and it does not need a lookup table with large storage. The memory cost of RC5 is significantly lower than that of AES. We can customize the group size, secret-key length, and the number of iterations of RC5, which makes it flexible enough to be used in systems with different resource configurations.RC5 is better than DES with respect to security strength, energy consumption and implementation efficiency.

It has also been observed that apart from AES and DES, the above-mentioned points that RC5 proves to be a better security solution when compared to DES and AES; it has been observed that RC5 also has lower memory requirements, less computational overhead, better security strength and consumes significantly lower energy when compared to IDEA and RSA.

Moreover in [4] various schemes such as Public Key cryptography, Symmetric Key cryptography and Hybrid cryptography and their respective energy consumptions are evaluated. They assumed the three security schemes were executed on Atmega 128, 16MHz 8-bit architecture AVR. The energy consumptions depicted in [4] shows that energy consumed by the source node using RC5 saves about 72% of the energy consumed by the hybrid scheme and 82% of the energy consumed by the public key cryptography.

Another aspect apart from energy consumption that needs to be focused on is computational overhead as high efficiency is strongly demanded for data security in WBANs, not only because of the resource constraints, but also for the applications. As mostly it is seen that wearable sensors are often extremely small and have insufficient power supplies, which in turn affects the computation and storage capabilities. Thus, the cryptographic primitives to be used by the sensor nodes should be as lightweight as possible, in terms of both fast computation and low storage overhead. In this paper energy consumed for RC5 encryption (ERC5) is considered as 34.2mJ as in [6].

Table2. Comparison of different symmetric key algorithms

Features	Encryption Algorithms				
	AES	DES	RC5	IDEA	BLOW FISH
Key Size(Bits)	128, 192 or 256 bits	64	0 to 1020 bits generally 128 bits	128	32-448 bits
Block Size	128	64	32, 64 or 128	64	64
Rounds	10,12,14	16	1-255 (12 originally suggested)	8	16
Level Of security	Average security	Adequate security	Very Secure	Secure	Secure
Attacks found	Key recovery attack, Side channel attack	Exclusive Key search, Linear cryptanalysis, Differential analysis	Co-relation attack, Timing attack	Linear attack	Differential attack
Approximate Energy for Key Expansion and Encryption	1.2µJ	2.1µJ	0.8µJ	1.5µJ	0.9µJ
Encryption Speed	Slow	Slow	Fast	Fast	Average

2.3 Graphical study and analysis of RC5 algorithm

Represents and evaluates the performance of RC5 based on various parameters the details of which has been explained in the preceding section. In general, any particular RC5 algorithm is represented with the notation of RC5-w/r/b, where w is the word size in bits, r signifies the number of rounds and, b denotes the number of bytes in the secret in this section few graphs have been shown that key. The following table shows the time required to execute different file formats by the algorithms RC5, Blowfish and DES with varying word size/number of rounds. The following points can be observed by analyzing the following data recorded for different file sizes:

In [5], comparing the execution time of each algorithm on different-2 file types like text file, audio file & video files, 6 files and recorded their execution (encryption or decryption) times in milliseconds for the three algorithms RC5, Blowfish and DES, it is observed that RC5 has the least execution time than DES and Blowfish. It is graphically explained in Fig1. for 32 bytes’ key.

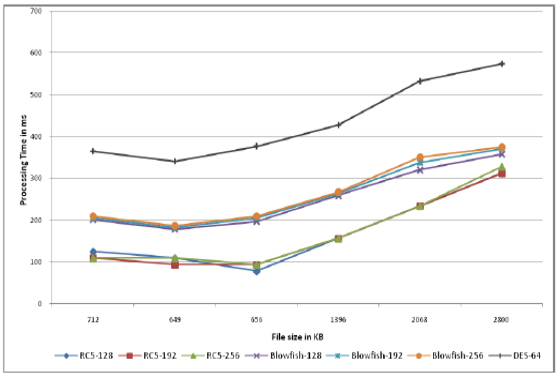

Figure 1. Execution time of RC5, Blowfish and AES for 32 bytes

The graph in Figure 2 shows the throughput vs. the number of loops unrolled for RC5 16 and 24-byte key sizes. As it can be observed from the figure itself that for 3 unrolled loops RC5-32/15/16 gives maximum throughput of 255Mbps whereas RC5-32/15/24 provides the maximum throughput of 245Mbps.Therfore making the fact evident that 3-loops unrolled outperforms 5 and 15-loops unrolled.

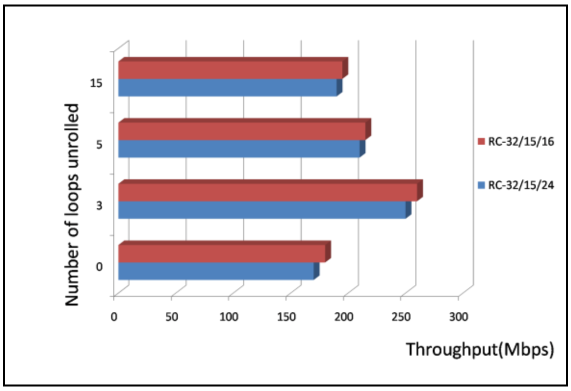

Figure 2. Throughput vs. number of rounds unrolled in RC5 implementations using 128 and 192 bit key

3. CONCEPT OF ENERGY HARVESTING IN WBAN

The concept of using harvesting energy is recently emerging as a potential power supply solution to minimize energy consumption as well as to extend the operational lifetime of the sensor nodes. As in [7], given a 1cm^3 of primary battery (0.8Wh/cm^3) volume, the sensor node, with an average power consumption of 100μW, can only last for around 11 months before the node goes into idle state. As such, the concept of energy harvesting from readily available energy sources present in the ambient environment such as

1. Solar Energy
2. Sound Energy
3. RF Energy

are directly at the deployed site to supplement and recharge the energy storage devices for powering the sensor nodes is being implemented. Many systems have already been developed but those reported in the recent times are mostly for outdoor applications where solar energy is plentiful. The problems with WBANs are that wearable devices used in it are limited in terms of size and outdoor accessibility. So, alternative energy sources like Thermal, Vibration, and Hybrid energies needs to be considered.

Table 3. Energy sources available

Energy	Source	Harvested power
Solar Energy	Indoor Outdoor	10µW/cm^2 10 mW/cm^2
Sound Energy	Noise	0.003µW/cm^3
RF Energy	Broadcast, WLAN battery	0.1µW/cm^2(GSM) 0.001mW/cm^2(WiFi)
Vibration Energy	Human motion, Machines	4µW/cm^3 100mW/cm^3
Thermoelectric Energy	Human body temperature/ solar panel	30µW/cm^2

In [8] thermoelectric generator based wearable device has been developed to be implemented in WBANs. Here heat energy is harvested using human warmth. However, in this paper we assumed a circuitry based on [8] which if implemented can harvest energy of about 950µJ for about each node. So, E_{hr} = 950µJ for our evaluation.

4. PROPOSED ALGORITHM

1. Start.
2. A cluster based topology with multi hop mode of communication between the cluster members (CM) and the cluster head (CH) is used, consisting of n nodes from which a cluster head (CH) is selected at random.
3. Next a synchronization message (SN_{msg}) containing a key is being sent to all the CMs with normal range of values for heartbeat, blood pressure, blood glucose level, ECG, EEG like parameters.
4. An acknowledgement (ACK_{msg}) is sent after receiving the SN_{msg} from CH.
5. A data counter (D_i) is set to 0 for every ith node. For every data transmission that will occur $D_i = D_i+1$.

If D_i = 5 then the ith node goes to rest mode else if D_i<5 then data transmission continues by the ith node else data is transmitted by any of (n-i)th node.

6. If n-i < n/2 then D_i = 0 and the respective rest nodes becomes active. Priority is given to the node which first went to rest mode, hence comes in active mode based on the queue maintained by CH.
7. RC5 is used as the security solution which is to be embedded along with this algorithm to ensure security of the data transmission.
8. For data transmission to occur each CM checks the values from the SN_{msg} with the current recorded value V_i. If V_i > V_{th} (the threshold value from $SN_{msg)}$ then data transmission begins.
9. After k sets of data transmission residual energy (RE_i) of each ith node is computed. If RE_i< RE_{th} (threshold value of the residual energy) then go to step 10.
10. For every ith node where I = (1...n), if step 9 holds true then $E_{i=}2RE_i$, where HE $_{total}$ = total harvested energy, E_i = current energy of the ith node. E_i is made twice the RE_i by taking the $RE_{i\ amount}$ of energy from HE_{total}. Then present $HE_{total\ becomes}$ initial HE_{total} - $RE_{i.}$
11. End.

5. EVALUATION OF PROPOSED ALGORITHM

Following the first order radio model the standard equations of energy consumption are:

$E_{TX}(k,d) = E_{elec}*k+E_{amp}*k*d^2$ ....(1)

$E_{RX}(k)$ = E_{elec}*k....(2) where E_{elec} = 50nJ/bit, E_{amp} = 10pJ/bit/m^2, k = message bits, d = distance between source node and sink node,

Let the number of data transmissions be ‘x’.

Equations of energy consumption in different modes using equation (1) and (2):

1. In rest mode with RC5 encryption,
   $E1 = x*k*[2* E_{elec} + E_{amp} *d^2]+n*E_{RC5}$
2. In rest mode without RC5 encryption,
   $E2= x*k*[2* E_{elec} + E_{amp} *d^2]$
3. In active mode with RC5 encryption,
   $E3=2* x*k*[2* E_{elec} + E_{amp} *d^2]+n*E_{RC5}$

4. In active mode without RC5 encryption,

$E4= 2*x*k*[2* E_{elec} + E_{amp} *d^2]$

Equations of longevity calculations for different modes using equation (1) and (2):

1. Longevity for active mode,

$T1=E_{totsuppl} / (E_{totactv} *3600*24)$

2. Longevity for rest mode,

$E_{totrest=} E_{totactv} * (n/2) + E_{totslp} * (n/2)$

$T2= E_{totsuppl} / (E_{totrest} *3600*24)$

where $E_{totsuppl}$ = Total energy supplied by both battery and harvested source (E_{hr}).

$E_{totactv}$ = Total energy consumed by nodes working in active mode,

$E_{totrest}$ = Total energy consumed by nodes working in rest mode,

E_{totslp} = Total energy consumed in sleep mode.

6. RESULTS

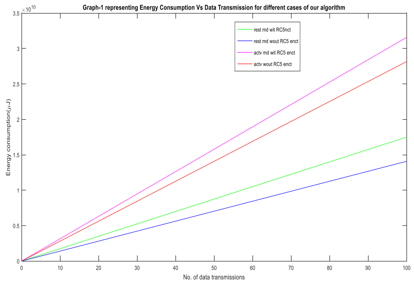

Figure 3. Representing energy consumption vs data transmission for different cases

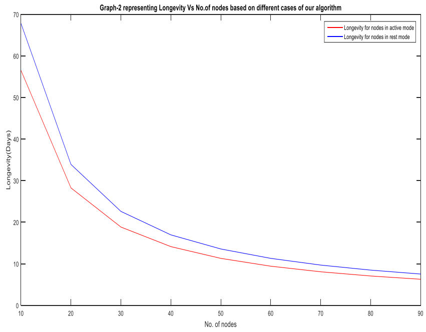

Figure 4. Representing longevity vs no. Of Nodes based on different cases

7. DISCUSSIONS AND ANALYSIS

Sensor nodes are, in general, capacitated with limited amount of energy to survive on.

Consequently, energy looms large as a constraint for these sensing devices, and, therefore, is crucially important to ensure that the rate of dissipation of energy can be minimized for these sensors. On the other hand, security has also emanated to be path breaking in the context of body sensor nodes. Our proposed algorithm primarily focuses on these two issues and provides an efficient solution for overcoming the existing challenges.

The graph 1 represents energy consumption vs number of data transmissions. Here four cases are being considered:

1. **Energy consumption in rest mode along with RC5 encryption** - Even though energy is conserved in rest mode, due to RC5 encryption some amount of energy is still consumed. But on the other hand, RC5 encryption promises security of the data being transferred. As we can observe that energy consumption increases at a slow pace along with the increase in the number of data transmission, the same has been illustrated by the following: For n = 20; where n is the number of data transmission, energy consumption is 0.3μJ. For n = 50; we see that energy consumed is 0.8μJ.

2. **Energy consumption in rest mode without RC5 encryption**- Here energy is conserved in rest mode without RC5 encryption which in turn saves a considerable amount of energy, but it does not guarantee the security of the data being transmitted. As observed from the graph, energy consumption increases at a very slow pace along with the increase in the number of data transmission. For n = 20; n is the number of data transmission, energy consumption is 0.25μJ. For n = 50; we see that energy consumed is 0.65μJ.

3. **Energy consumption in active mode without RC5 encryption -** Here energy is consumed in active mode without RC5 encryption so it does not guarantee the security of the data being transmitted. As observed from the graph, energy consumption increases steadily along with increase in the number of data transmission. For n = 20; n is the number of data transmission, energy consumption is 0.57μJ. For n = 50; we see that energy consumed is 1.55μJ.

4. **Energy consumption in active mode with RC5 encryption -** Here energy is consumed in active mode with RC5 encryption so the data being transmitted is secured. As observed from the graph, energy consumption increases rapidly along with increase in the number of data transmission.

For n = 20; n is the number of data transmission, energy consumption is 0.65μJ. For n = 50; we see that energy consumed is 1.85μJ.

Thus, comparing the above 4 cases, we observe that the best case best representing our algorithm is case 1 which shows that even though the energy consumption is not the least when compared to case 2, but better than other cases in terms of both energy consumption and security.

In both the cases as represented in the graph we observe that with the increase in number of nodes the longevity is decreased, but when compared for active and rest mode it is seen that longevity of nodes in rest mode is greater as compared to nodes in active mode and also decreases at a slow pace. This has been illustrated below: For n = 10 where n = no. of nodes, longevity is seen to be 57 days in active mode whereas longevity is seen to be 68 days in rest mode.

For n = 25 longevity is seen to be 21 days in active mode whereas longevity is seen to be 28 days in rest mode, so it is observed that longevity is increased by 25% when nodes are operating in rest mode.

8. CONCLUSIONS

Healthcare in modern days has been undergoing crucial changes, as the common practice of clinical treatment is gradually being overhauled by ubiquitous healthcare systems. In the past decade, healthcare organizations underwent steep rise of pressure to provide improved healthcare, as the number of chronic disease patients steeply increases every year worldwide. Chronic diseases such as heart and lung diseases require real time, continuous, and long-term followups. WBANs can help in ubiquitous and remote health monitoring of patients. Our documentation throws light upon analysing and providing efficient solutions to combat the two main issues which are energy consumption and secure data transmission.

We observed that RC5 encryption can prove to be a better security solution for ensuring the security of data transmission by stating various reasons and providing a comparison table which compares RC5 algorithm with other existing algorithms based on various parameters and shows that RC5 is efficient in terms of energy it consumes as well as provides good security. Next, we proposed an algorithm that primarily focuses as to how energy consumption can be reduced for which we incorporated the concept of rest mode in which a sensor is seen to consume lesser energy and providing increased longevity as compared to a node in active mode. We evaluated our algorithm by taking various cases into consideration, coding and simulating the same using Matlab, with the help of which we are able to state that our algorithm shows that longevity is increased by 25% when nodes are in rest mode and also that energy consumption is not the least but better than most of the cases.

ACKNOWLEDGEMENT

I acknowledge my B. Tech students that they help me very much for written this paper.

REFERENCES

[1] Kumar J., Ezhilarasi M. (2012). Adaptive security mechanism for PEAS in wireless sensor networks, *International Conference on Computing and Control Engineering (ICCCE 2012)*, ISBN 978-1-4675-2248-9 © 2012.

[2] Qiu M.K., Gao W.Z., Chen M., Niu J.W., Zhang L. (2011). Energy efficient security algorithm for power grid wide area monitoring system, *IEEE Transactions on Smart Grid*, Vol. 2, No. 4, pp. 715-723.

[3] Rivest R.L. (1994). The RC5 encryption algorithm, *Proc. 2nd International Workshop on Fast Software Encryption*, Leuven, Belgium, pp. 86-96. DOI: 10.1007/3-540-60590-8_7

[4] Mohammad A.R., Rjoub A., Baset A. (2009). A low-energy security algorithm for exchanging information in wireless sensor networks, *Journal of Information Assurance and Security*, pp. 48-59.

[5] Vermaand H.K., Singh R.K. (2012). Performance analysis of RC5, blowfish and des block cipher algorithms, *International Journal of Computer Applications (0975 – 8887)*, Vol. 42, No.16.

[6] Yang Z., Mohammed A. (2013). Self-organization and green applications in cognitive radio networks, Al-Dulaimi A., Cosmas J., Mohammed A., Eds, IGI Global, pp. 290-300. DOI: 10.4018/978-1-4666-2812-0

[7] Roundy S., Leland E.S., Baker J., Carleton E., Reilly E., Lai E., Otis B., Rabaey J.M., Wright P.K., Sundararajan V. (2005). Improving power output for vibration-based energy scavengers, *IEEE Pervasive Compute.*, Vol. 4, No. 1, pp. 28-36. DOI: 10.1109/MPRV.2005.14

[8] Hoang D.C., Tan Y.K., Chang H.B., Panda S.K. (2009). Thermal energy harvesting from human warmth for wireless body area network in medical healthcare system, IEEE. DOI: 10.1109/PEDS.2009.5385814

[9] Sohraby K., Minoli D., Znati T. (2007). Wireless sensor networks: technology, protocols, and applications, *Lecture Notes in Computer Scienc*e, pp. 129-139. DOI: 10.1002/047011276X

[10] Zhang Y., Xiong P., Luo Y., Li L. (2011). Design of remote home environment monitoring and health care monitoring system based on data confusion, *2011 IEEE International Conference on Automation and Logistics (ICAL)*. DOI: 10.1109/ICAL.2011.6024680

[11] Hanson M.A., Powell H.C. Jr., Barth A.T., Ringgenberg K., Calhoun B.H., Aylor J.H., Lach J. (2009). Body area sensor networks: challenges and opportunities, *Computer*, Vol. 42, No. 1, pp. 58-65. DOI: 10.1109/MC.2009.5

[12] Chen H., Liu M., Hao W., Chen Y., Jia C., Zhang C., Wang Z. (2009). Low-power circuits for the bidirectional wireless monitoring system of the orthopedic implants, *IEEE Transactions on Biomedical Circuits and Systems*, Vol. 3, No. 6, p.437. DOI: 10.1109/TBCAS.2009.2026283