ENERGY ANALYSIS OF LIGHTWEIGHT BLOCK CIPHERS FOR SECURE ECG TRANSMISSION IN WBAN NODES

Narmadha T **Meenakshi M**
Department of Electronics and Communication Engineering, College of Engineering Guindy, Anna University, Chennai, India. 044-22203170,
narmadha.thangamani@gmail.com, meena68@annauniv.edu

Kalaiarasi M
Department of Electronics and Communication Engineering, College of Engineering Guindy, Anna University, Chennai, India. . 044-22203170,
kalaibhuvan26@gmail.com

Abstract: *Information security in Wireless Body Area Networks (WBAN) is required to maintain confidentiality, integrity and privacy of a person's health data. Bio-signal like Electrocardiogram (ECG) has patient's sensitive information and needs secure transmission. The WBAN sensors have limited resources and hence the traditional cryptographic algorithms are not suitable. Compared to asymmetric (public-key) cryptography, symmetric (private-key) cryptography provides good efficiency in terms of energy because of its less computational requirement. In private-key cryptography, the lightweight block ciphers which are small in block size and key size are suitable for WBAN to meet the energy efficiency and security concerns. This paper investigates the energy efficiency performance of the lightweight block ciphers PRESENT (80,128) and AES while transmitting feature extracted ECG data using TelosB mote running Contiki OS. The implementation and analysis result show that the PRESENT cipher achieves good energy efficiency and is well suitable for low profile sensor nodes in WBAN.*

Key words: *Body area networks, Lightweight block ciphers, ECG, TelosB, Contiki OS*

1. Introduction

Wireless Sensor networks are used in many application areas. The application areas are: medical and non-medical. The sensors used in medical areas can be wearing by the person or implanted in the body. With these recent developments in wearable medical sensors, WBANs help to collect human related vital information like Electrocardiogram (ECG), Blood sugar, Blood pressure (BP), Oxygen level (SpO2), activity tracking and so on. Since the data related to human personal information, WBANs pose certain challenges in both security and privacy. The Health Insurance Portability and Accountability Act (HIPAA) [1] mandates that the data collected from the human body by using the medical sensors should be kept secure against unauthorized access or from eavesdropping. Efficiency of WBAN in medical industry and the requirement of information security in WBAN are discussed in [2-3].The main challenge is to transmit the acquired signals securely with low power.

Traditional encryption mechanisms is not applicable for the environments like resource constrained WBANs. Designing a cryptographic algorithm for WBAN needs less computation for low energy consumption and also to achieve the desired security. Symmetric (Private-key) cryptography consumes low memory than asymmetric (Public-key) cryptography and it is quite opted for such low resource environments [4-5].Recently many lightweight block ciphers have been designed for resource constrained devices [6-10]. The extensive survey on lightweight block ciphers shows that the PRESENT cipher consumes less memory and register area in both hardware and software environment and at the same time offers better power efficiency [11-13]. This paper deals with the implementation and analysis of PRESENT block cipher in MSP430 processor running in TelosB mote working on ContikiOS and its performance is compared with the popular AES algorithm. Contiki OS is an open source and multi-threading operating system for energy efficient

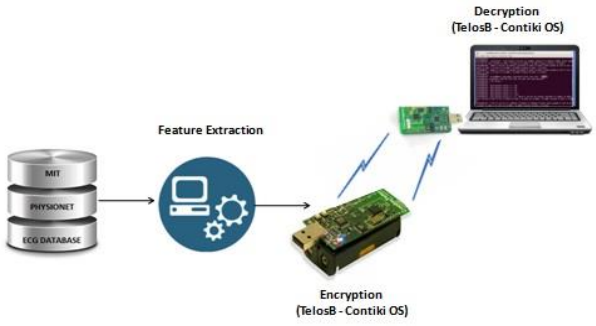

Fig.1. Architecture of secure ECG transmission in TelosB

embedded systems and wireless sensor networks [14]. It runs on cooja simulator which permits the emulation of real hardware platforms. The system implementation architecture used in this work is shown in the Fig1.

Recently there has been a lot of research interest in

WBAN for healthcare and entertainment. In [15] performance of WBAN in medical field and the requirement of security were analyzed. Various types of devices, data rates, security requirements, bandwidths, energy requirements, and interferences have been surveyed and an extensive research in the field of WBAN has been conducted. The authors in [16] proved that the timing information of heart beat can be used as a biometric trait and hence the ECG signal has been demonstrated for the same. The feature like QRS can be derived from the ECG signal and can be used for securing the key distribution. Authors in [17] developed an algorithm for the real time QRS detection in ECG waveform. The QRS edges are based on slope, width and amplitude of the raw ECG signal. Due to various interferences available in the ECG signal, the digital bandpass filter is used to reduce false positives, thereby improves detection sensitivity.

The control unit and the radio unit are considered as the primary sources of energy and power overhead in WSN security design. The authors in [18] proposed a lightweight security scheme for WBAN along with a new microcontroller design. The symmetric key cryptographic technique used in this work supports confidentiality, integrity, and authentication and replay protection. A threat model is created in the WBAN communication model and tested against eavesdropping, inserting, deleting etc. Their proposed system also shows that the energy consumption of the microcontroller is greater than the radio. The new microcontroller design was made with the replacement of MSP430F1611 controller with a custom processor that runs AES in all modes of operation (AES-CTR, AES-CBC and AES-CCM). This customized microprocessor design needs lesser clock cycles when compared with the other works that use AES for security analysis. Additionally, the memory, cost and power for encryption are shown to be less compared to the previous works.

The authors of [19] proposed a hybrid way of key generation for inter-WBAN and intra-WBAN communication. Initially the secret key is preloaded and the remaining keys are generated using biometrics. The proposal is compared with BARI+ protocol in terms of memory overhead, communication overhead and energy consumption. The results showed that the energy consumption is higher due to key refreshment phase than BARI+. The energy cost of the lightweight ciphers implemented on an FPGA platform is discussed in [20]. It is observed that if the data path increases faster, the supply voltage decreases causing an impact on throughput which decreases non-linearly. The authors in [21] implemented AES and 11 lightweight block ciphers on cadence tool and modelSIM simulator. It is observed that the use of affine transformations consumes very less area when compared to isomorphic transformations. The results suggest that the number of bit toggles during execution of ciphers directly affects the dynamic power dissipation and hence based on this, energy consumption of the ciphers can be calculated. Lightweight block ciphers and their implementation in both hardware and software are discussed in [11] [21].The authors have suggested that the PRESENT cipher is best suited for hardware environments in terms of least memory (RAM), area occupation and power efficiency. The software performance analysis was done on LED, Piccolo and PRESENT cipher in x86 architecture. In that, Piccolo and PRESENT are reported to show better software speed on Core i3-2367M, Core 2 Duo P8600 (Core micro architecture) and XEON X5650 processors. The above survey of lightweight block ciphers, suggest that the PRESENT lightweight block cipher algorithm is well suited for resource constrained environments and also it supports hardware or software platform implementations.

This paper analyzes two widely used symmetric-key algorithms: PRESENT (80,128) and the AES and determines the suitability for WBAN environment. The major contributions in this paper are:

- Extraction of ECG signal features by Pan-Tompkins algorithm. The extracted features are given as input to the selected ciphers.
- Encryption of extracted features of ECG signals using PRESENT and AES cipher in TelsoB mote and broadcast to the server.
- Performance comparison such as power consumption, memory requirement, duty cycle and throughput for the radio during encryption in TelsoB for both the algorithms and also determine its suitability for resource constrained WBAN environment.

The paper is organized as follows: Section 1 introduce the work undertaken in this paper along with the discussion on the related works in literature. Section 2 discusses the need for ECG features extraction and the details of the same. In Section 3, the block ciphers used for the encryption of ECG parameters are explained. Section 4 explains the experimental implementation using TelosB for secure ECG transmission. In Section 5, the performance analysis such as power efficiency and CPU cycles needed for the process are compared for the implemented algorithms and Section 6 highlights the conclusions derived from this work.

2. ECG feature extraction

ECG is a primary tool used for diagnosis of human body functionality [22]. ECG signal differs from each person's by size, location and shape of the heart. Real-time ECG recording device records the ECG signal of the heart by fixing the electrodes on the patient's limb and chest and the results are investigated by the clinician. The ECG electrodes

are 12-lead or 3-lead type. ECG signals captured from the sensor in a WBAN undergoes some low power data processing and then is wirelessly transmitted to the end server by heterogeneous devices like Wi-Fi, Bluetooth, Zigbee etc. In such wireless transceiver systems, the major power consumption occurs for continuous transmission of ECG signals. Hence a preliminary ECG signal analysis followed by feature extraction and digitization is required. This data conversion will reduce the energy and power consumption in the sensor node. ECG signal feature extraction parameters (amplitude and intervals) help in cardiac analysis of each person. Since these values are human sensitive, they need to be securely transmitted using encryption and decryption.

2.1. ECG Data

The datasets used for this work are taken from MIT-BIH Normal sinus Rhythm database. The reading has been taken from different leads and is shown in the fig.2. In this work, five seconds dataset is taken for feature extraction. The common features (P,Q,R,S,T) are extracted using Pan-Tompkins algorithm. Raw ECG signals need to be pre-processed in order to reduce noise and to improve signal to noise ratio. The Pan-Tompkins algorithm is used for the same [24].

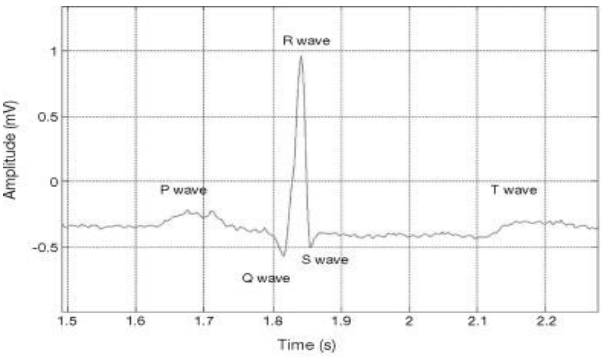

Fig 2. ECG signal from MIT database

2.2. Pan-Tompkins algorithm

The parameter QRS complex from an ECG signal is extracted using Pan-Tompkins algorithm [24]. It extracts the QRS complexes based on amplitude, interval and slope. The bandpass filter used here increases the detection sensitivity thereby reduce false detections. In this work, the datasets are taken for healthy persons ECG only [25]. Fig.3 explains the ECG signal feature extraction using Pan-Tompkins algorithm.

The raw signal is passed to digital band-pass filter which is cascading of high-pass and low-pass filters in order to attenuate the noise. This filter design is based on integer arithmetic and hence the computational power for QRS detection is less.

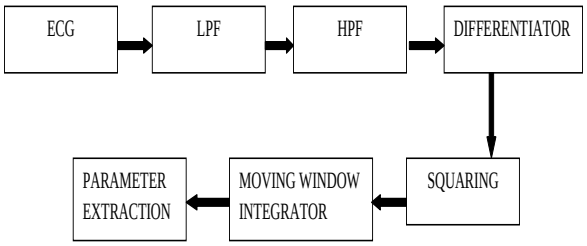

Fig.3. ECG feature extraction using Pan Tompkins algorithm

Equations (1) and (2) are used for low-pass filter design [24].

The second-order low-pass filter transfer function is given by

$$H(z) = \frac{(1-z^{-6})^2}{(1-z^{-1})^2} \quad \text{- (1)}$$

The difference equation of the filter is

$$y(nT) = 2y(nT-T) - y(nT-2T) + x(nT) - 2x(nT-6T) + x(nT-12T) \quad \text{-(2)}$$

Where, T is the sampling period and the cutoff frequency is about 11 Hz and the gain is 36.

The output of first-order lowpass filter is subtracted from the output of all-pass filter. The transfer function and the difference equation for such a high-pass filter is given in (3) and (4)

$$H(z) = \frac{(-1+32z^{-16}+z^{-32})}{(1+z^{-1})^2} \quad \text{- (3)}$$

$$y(nT) = 32x(nT-16T) - [y(nT-T) + x(nT) - x(nT-32T)] \quad \text{- (4)}$$

The lower cutoff frequency of this filter is about 5 Hz, the gain is 32, and the delay is 16 samples [24]. After filtering, most of the signal left is QRS complex only. The filtered signal is then differentiated to highlight the slope of the QRS complex. Here five point derivatives is used for the transfer function. The differentiators equations are given in (5) and (6) are

$$H(z) = \frac{(1/8T)}{(-z^{-2}-2z^{-1}+2z^{1}+z^{2})} \quad \text{- (5)}$$

The difference equation is

$$y(nT) = (1/8T)[-x(nT-2T) - 2x(nT-T) + 2x(nT+T) + x(nT+2T)] \quad \text{-(6)}$$

The filtered signal is passed to squaring and is shown by the equation (7)

$$y(nT) =]x(nT)]^2 \quad \text{- (7)}$$

This function will emphasize the high frequency signal which is the QRS complex from the derivative function. The slope of R waveform is extracted using moving window integration and is given in the equation (8) as,

$$y(nT) = (1/N)[x(nT-(N-1)T) + x(nT-(N-1)T) + ... + X(Nt)] \quad -(8)$$

where N is the number of samples within the integration window. The width of the moving window integration should be greater or same as the QRS complex duration. If the window is too wide, the QRS and T wave will merge together and lead to error signal. The five features over six periods are extracted namely, Heart rate, P-R interval, P-P interval, R peak and the QRS complex. These features are then given as a input to the symmetric ciphers for secure transmission.

3. Block ciphers

This section discusses about the selected block ciphers used for implementation and analysis in this paper. The lightweight block ciphers are selected for their better energy efficiency and reduced power consumption. The encryption parameters of the ciphers considered in this paper are listed in Table.I

TABLE I
CIPHER PARAMETERS

Cipher	Block length	Key length	Rounds
PRESENT -80	64	80	31
PRESENT-128	64	128	31
AES-128	128	128	10

3.1. PRESENT - 80 cipher

Among many light weight block ciphers, the cipher which is most secure and lightweight is PRESENT. This cipher is designed for low resource constrained applications like RFID tags and low power sensors. Also, the International Organization for Standardization and the International Electro-technical Commission (ISO/IEC 29192-2:2012) have announced the PRESENT cipher as a new international standard under lightweight cryptographic method [12]. PRESENT cipher can be implemented in TelosB mote because of its low memory consumption and better hardware efficiency. PRESENT cipher is based on substitution-permutation network. It has 64 bit input data and 80 bit key size and has 31 rounds. It uses a 4×4 bit S-box with 16 S-box allowing 4 bits as input. Fig.4 shows the algorithmic description of the cipher [25].

Key scheduling in PRESENT-80 is as follows

$[K_{79},K_{78},\ldots K_1K_0] = [K_{18},K_{17},\ldots K_{20},K_{19}]$

$[K_{79},K_{78},K_{77},K_{76}] = S[K_{79},K_{78},K_{77},K_{76}]$

$[K_{19},K_{18},,K_{17},K_{16},K_{15}] = [K_{19},K_{18},,K_{17},K_{16},K_{15}] \oplus$ round_counter

3.2. PRESENT -128 cipher

PRESENT-128 has 64 bit input data and 128 bit key size and involves 31 rounds. It also uses the 4-bit to 4-bit S-box as in PRESENT-80.It has 16 S-boxes

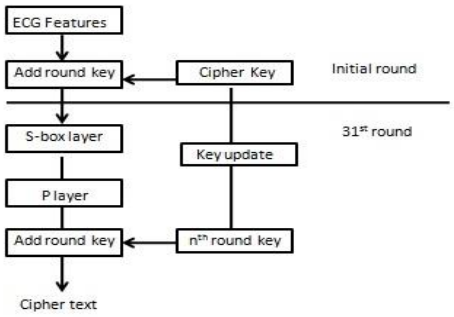

Fig. 4. PRESENT Cipher algorithm

with each S-box allowing 4-bit as input. The algorithmic steps are same as in Fig.4. However the Key scheduling is different for PRESENT-128 and is as follows:

$[k_{127}k_{126} \ldots k_1k_0] = [k_{66}k_{65} \ldots k_{68}k_{67}]$

$[k_{127}k_{126}k_{125}k_{124}] = [k_{127}\, k_{126}\, k_{125}\, k_{124}]$

$[k_{123}k_{122}k_{121}k_{120}] = S[k_{123}k_{122}k_{121}k_{120}]$

$[k_{66}k_{65}k_{64}k_{63}k_{62}] = [k_{66}k_{65}k_{64}k_{63}k_{62}] \oplus$ round counter

3.2. AES-128 cipher

The Advanced Encryption Standard (AES)- Rijndael is accepted as a standard encryption method by National Institute of Standards and Technology (NIST) in U.S.AES also comes under substitution-permutation network. It uses 128-bits of plaintext as 16 bytes. AES has 10 rounds for 128-bit keys. Each round has different keys and it is calculated from original key. The steps in AES are, AddRoundKey, SubBytes, ShiftRows and MixColumns. This cipher is best suited for 8-bit architectures because of its byte-oriented operation. Fig.5. shows the algorithmic description of AES.

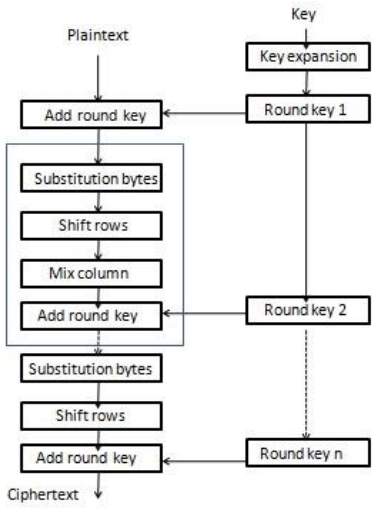

Fig. 5. AES algorithm

3.3. Security strength of the ciphers

The resilience of a cipher to attacks shows its security strength. When a cipher faces many attacks

from its date of launch and still is resistant against the attacks, it is considered as a good cipher. Most of the cryptanalysis starts at reduced-round version of the cipher and is then extended to full cipher.

The best known cryptanalysis of PRESENT-80 is 16-rounds attack by differential cryptanalysis using chosen plaintext attack [26]. Related key attack was done in PRESENT-128 and the attack reaches up to 17 rounds of the cipher [27]. Differential cryptanalysis attacks with public S-boxes recovered 80-bit key at the 12th round of the PRESENT-80 with lesser time and data complexity [28]. Currently PRESENT-80 and PRESENT-128 are running on 31 rounds, respectively. Thus, both of them are not yet breakable.

The best known cryptanalysis of AES-128 is chosen-plaintext attack that breaks seven rounds out of the 10. Biclique cryptanalysis on full AES-128 version increases the time complexity [29]. Another well known cryptanalysis of AES-128 is meet-in-the-middle attack on 7 rounds which takes very less time and complexity [30] and an improved meet-in-the-middle attack in [31]. The attack on AES-128 is Impossible differential attack up to 7 rounds is proposed in [32]. The side-channel attack recovers all 128 bit key in 6-7 blocks of plaintext/ciphertext with minimal operations when compared to previous side-channel attacks [33]. Still AES full version is unbreakable in all the key sizes (128-bit, 192-bit, 256-bit), and this cipher is considered as a standard reference among all the block ciphers.

4. Experimental setup

The ECG signal from the database is feature extracted and given as an input to the ciphers for secure transmission using TelosB sensor mote. Telosb is IEEE 802.15.4 standard with a low power microcontroller TI MSP430 of 8 MHz and CC2420 radio chip. It has features of Zigbee with 250kbps data rate and with ISM band. It has incorporated sensor suites like temperature, humidity and light sensors, which runs TinyOS or Contiki OS. Fig.6 shows the experimental setup for the process. Here two TelosB motes are used as source and sink with a distance of 30cm between them [25].

There are many operating systems available for Zigbee mote and selecting the best OS is of great challenge. One of the popular lightweight operating system is Contiki. Contiki is an open source operating system based on C programming language and connects low power sensors to the cloud environment. It runs on 8 bit processor, footprint not higher than 4KB of RAM and very low power consumption of 10 mW makes it suitable for memory constrained systems [34-35]. In this experimental setup, Contiki OS is installed in the system and the TelosB mote can easily been ported. The Cooja simulated mote is compiled and executed in the Contiki OS.

The ECG transmission using RIME protocol is

Fig. 6. Experimental setup

shown in the Fig.7 and Table.II describes security notations used in the overall process.

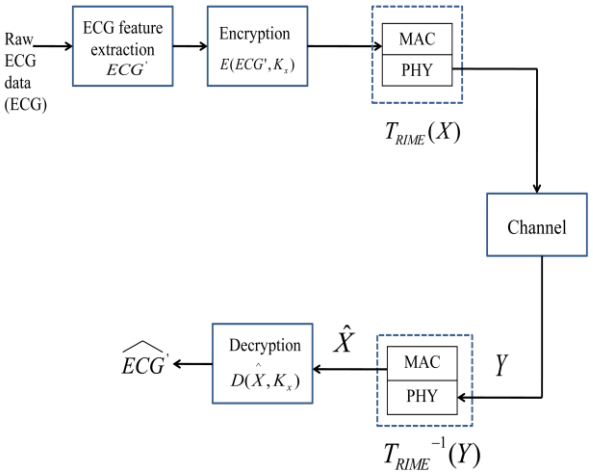

Fig. 7. Secure ECG transmission using RIME protocol

Step 1: Normal sinus rhythm ECG data's from MIT physionet database is taken and its features are extracted using Pan Tompkins algorithm.

$$ECG_{PT}(ECG_i) = ECG'_i=(HR,PP,PR,RR,QRS)_i$$

for i=1 to N , where N is the number of ECG data set from the database.

Step 2: The extracted features are then encrypted using PRESENT cipher (80,128) and AES-128 with the secret key K_x

$$X_i= E\ [ECG'_{i,}, K_x]\ for\ \ i = 1\ to\ N$$

Step 3: The encrypted data from the transmitter is then broadcast using RIME protocol through PHY and MAC layer.

Encapsulation function $T_{RIME}(X)$ represents the overall processing of both layers.

Step 4: The broadcast data is then received at the receiver and the de-capsulation function is applied to recover the transmitted bits. Let Y be the bits received at receiver PHY layer. Transmitted bits can be estimated as

$$\hat{X} = T^{-1}_{RIME}(X)$$

TABLE II
SECURITY NOTATIONS

Notations	Description
ECG	Raw ECG data from the physionet database
K_x	Secret key between the transmitter and receiver
$ECG_{PT}(ECG)$	ECG feature extraction using Pan Tompkins algorithm
ECG'	Feature extracted parameters using Pan Tompkins algorithm
HR	The extracted Hear Rate value
PP	The extracted PP interval value
PR	The extracted PR interval value
RR	The extracted RR interval value
QRS	The extracted QRS value
$E(ECG', K_X)$	Encryption function of ECG' using secret key
X	Encrypted output at the transmitter
$T_{RIME}(X)$	Encapsulation function which represents the impact of PHY and MAC process using RIME protocol
$T^{-1}{}_{RIME}(X)$	Decapsulation function which represents the impact of PHY and MAC process using RIME protocol
$\hat{X}_i$	Estimated received bits
$D(\hat{X}_i, K_X)$	Decryption function of Xi using secret key
$\widehat{ECG_i}$	Recovered ECG data

Step 5: The original data is thus recovered at the receiver by decryption function.

$$\widehat{ECG_i} = D(\hat{X}_i, K_X)$$

5. Performance analysis and comparison

The selected cipher's encryption and decryption program runs in Rime protocol in broadcast mode of operation in Contiki. There are many applications available in Contiki OS. One such application is powertrace and can be used in all modes of operation (Broadcast, Unicast, etc) and is used to estimate energy and power consumption. Simulation parameters used in the work are listed in Table.III.

TABLE III
SIMULATION PARAMETERS

Parameter	Value
Radio Medium	Unit Disk Graph Medium
Mote type/start-up delay	Tmote sky/ 1000ms
MAC layer	CSMA/CA
Bit rate	250kbps
Radio duty cycling	NULLRDC
Node transmission range	50m
Node carrier sensing range	100m
Transmitter/Receiver ratio	100%
Protocol	RIME

5.1. Energy and Power analysis

The powertrace application calculates the power of the node in each stage. The stages are CPU usage, RADIO-TRANSMIT, RADIO-LISTEN, IDLE-RADIO LISTEN and IDLE-RADIO TRANSMIT. The energy consumption (mJ) is calculated using (9)

Energy_consumption =

$$\frac{Energest\_value \times Current \times Voltage}{runtime} \quad - (9)$$

The power consumption (mW) is calculated using (10)

Power consumption =

$$\frac{Energy\_consumption}{RTIMER\_SECOND} \quad - (10)$$

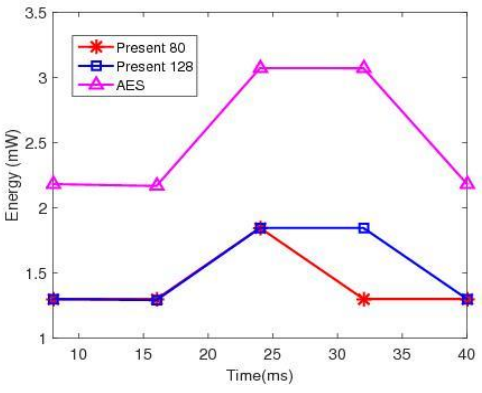

Fig. 8. Energy consumption of block ciphers running on TelosB mote

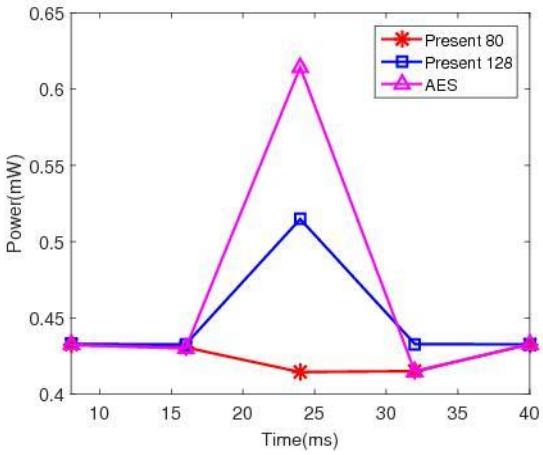

Fig. 9. Power consumption of block ciphers running on TelosB mote

where the "Energest_value" denotes the number of cycles between two radio time instants, the "current" value for all radio stages are given in Sky mote datasheet [36-37] and the "voltage" is 3V. The "runtime" is the time interval the measurements are taken and it is set to 8ms here and "rtimer" has a value of 32768 ticks per second for greater time resolution and real-time interrupts.

The cipher's energy and power consumption during encryption and decryption are compared in Fig.8 and Fig.9, respectively. The energy comparison reveals that energy consumption for PRESENT 80 bit and 128 bit key is almost similar for encryption and transmission and it is less when compared to that of the AES cipher. The difference lies in the size of the key and the variation occurs in the range of 23-24ms. AES and PRESENT-128 has key size of 128 bit, whereas PRESENT-80 is 80-bit key. The key scheduling process consumes more energy and power for AES and PRESENT-128, however it is within acceptable range for low power devices.

5.2. Dutycycle and Memory analysis

The contiki OS will implement the duty cycling of radio on IEEE 802.15.4. In Low power listening mode, the receiver will keep ON to poll the available radio medium for its operation. If any of the nodes are synchronized, the duty cycling protocol will set up a schedule between the nodes for communication. When the Rime protocol turns the radio 'ON' and the neighbour nodes can start sending packets to the other nodes. The duty cycle in (%) for transmitter and receiver can be calculated using equations (11) and (12) where the terms Energest_TXD, Energest_RXD, Energest_CPU and Energest_LPM denote the number of cycles in a consumed in each time period, over which the transmitter, receiver, CPU and LPM (listen power mode) are active, respectively. The number of active cycles of the transmitter includes encryption as well as the cipher data broadcast as per the MAC. Similarly the number of active cycles of the receiver includes cipher data reception and the decryption process. Duty cycle for transmitter is calculated as

$$\text{Transmitter\_Dutycycle} = \frac{Energest\_TXD}{Energest\_CPU + Energest\_LPM} \quad - (11)$$

Duty cycle for receiver is calculated as

$$\text{Receiver\_Dutycycle} = \frac{Energest\_RXD}{Energest\_CPU + Energest\_LPM} \quad - (12)$$

The duty cycle plots for the transmitting mode and the receiving mode shown in Fig.10 and Fig.11 show that PRESENT-80 and PRESENT-128

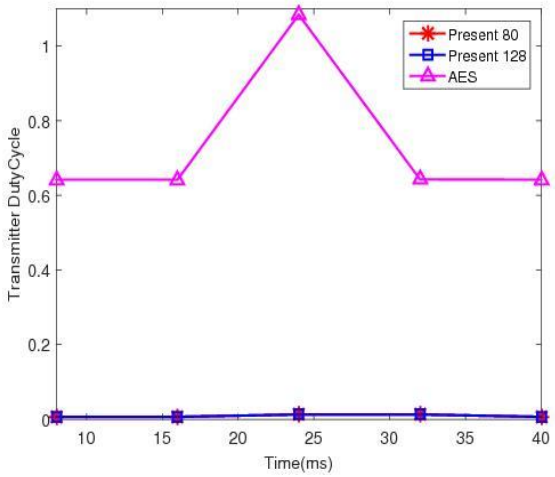

Fig. 10. Encryption Throughput of block ciphers in ContikiOS

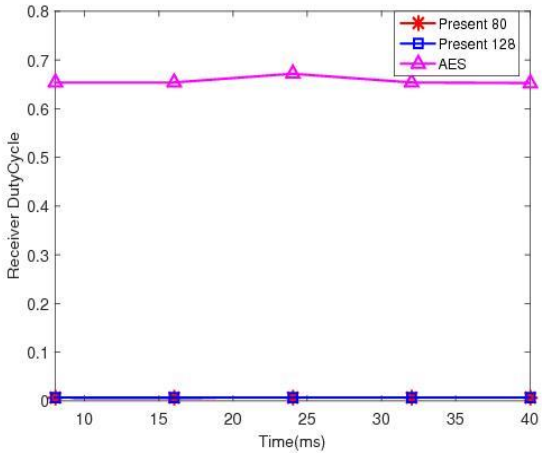

Fig. 10. Decryption Throughput of block ciphers in ContikiOS

perform almost similarly and consume lesser number of cycles when compared to the AES-128 cipher. Lower duty cycle is indicative of better power efficiency.

Since WBAN have low power sensors, it is essential to check the memory consumption of Contiki OS based application implementations. Table.IV shows the memory consumption of the ciphers in ContikiOS. Here the parameter "Text" denotes the code and read-only data, "Data" denotes read-write value, "Bss" denotes the uninitialized data , "Dec" sums up the Text, Data and Bss and "Hex" is the hexadecimal value of "Dec". The flash memory consumption of the ciphers will be Text+Data, and RAM consumption is Data+Bss [25].

5.2. Throughput

The speed at which the bits are processed during encryption and decryption can be referred to as the encryption and decryption throughputs in bits/second and are derived by considering the processed input block size and the count of CPU cycles required for the same. In the present setup the clock frequency is 8 MHz.

The encryption throughput shown in Table.V shows that the AES cipher processing speed is higher than PRESENT(80,128), mainly because of the larger input block size used per operation. The key size has a moderate influence on the throughput value. Similar observations are noted for decryption also. However the decryption speed is seen to be almost double the encryption speed. The decryption throughput is shown in Table.VI. Decryption is the inverse process of encryption. However, the inverse operation is applied to all round sequences. But Allroundkey does not require inverse operation because the XOR operation is its own inverse. It is also observed that AES has a higher throughput than PRESENT cipher. This indicates that the PRESENT cipher requires almost twice the duration as compared to AES for encryption/decryption of the same given data. The encryption and decryption throughput speeds are compared pictorially in Fig.12. for all the three ciphers.

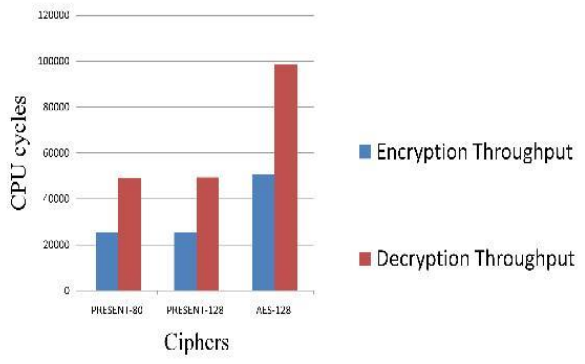

Fig. 12. Throughput of encryption and decryption in ContikiOS

TABLE IV
MEMORY CONSUMPTION OF BLOCK CIPHERS IN CONTIKIOS (BYTES)

Cipher	Text	DATA	Bss	Dec	Hex	Flash	RAM
PRESENT -80	25490	172	5858	31520	7b20	25662	6030
PRESENT-128	25634	172	5858	31664	7bb0	25806	6030
AES-128	26536	682	6238	33456	82b0	27218	6920

TABLE V
ENCRYPTION THROUGHPUT OF BLOCK CIPHERS IN CONTIKIOS

Cipher	Block size (bits)	Encryption (cycles)	Encryption (cycles/bit)	Throughput (cycles/sec)
PRESENT - 80	64	20063	313.48	25520
PRESENT-128	64	20048	313.25	25538
AES-128	128	20126	157.23	50880

TABLE VI
DECRYPTION THROUGHPUT OF BLOCK CIPHERS IN CONTIKIOS

Cipher	Block size (bits)	Encryption (cycles)	Encryption (cycles/bit)	Throughput (cycles/sec)
PRESENT - 80	64	10399	162.48	49236
PRESENT-128	64	10367	161.98	49388
AES-128	128	10394	81.20	98522

6. Conclusion and Futurework

The proposed framework in this paper investigates the energy efficiency performance of the lightweight block ciphers PRESENT-80 and PRESENT-128 and compares them with the benchmark AES-128, while transmitting feature extracted ECG data using TelosB mote running ContikiOS. The TelosB platform provides a WBAN environment of working with a power and memory constrained device. The implementation in hardware and the subsequent power consumption and transmit/ receive duty cycle analysis suggests that the PRESENT cipher can achieve good energy efficiency which is better than the AES cipher. The memory requirement comparison also shows the feasibility of PRESENT implementation in low form factor and lesser memory sensor motes. However AES has the advantage of higher throughput than the PRESENT

cipher. Hence it can be concluded that the PRESENT cipher is a preferable option for implementation in low form factor, resource constrained hardware. The future work would focus on carrying out the side channel cryptanalysis of PRESENT cipher and AES in TelosB platform.

References

1. Moshaddique Al Ameen, Jingwei Liu , Kyungsup Swak, *Security and privacy issues in wireless sensor networks for healthcare applications*, Journal of Medical systems.36(1) 2012 93- 101.doi:10.1007/s10916-010-9449-4.
2. Sofia Najwa Ramli , Rabiah Ahmad, *Surveying the wireless body area network in the realm of Wireless communication*, IEEE 7th International Conference on Information Assurance and Security (IAS).2011 58-61.doi: 10.1109/ISIAS.2011.6122845.
3. Krishna K.Venkatasubramanian , Sandeep K.S Gupta, *Physiological value based efficient usable security solutions for body sensor networks*, ACM Transactions on sensor networks.6(4) ,doi:10.1145/1777406.1777410.
4. Daojing He,Sammy Chan,Yan Zhang , Haomiao Yang, *Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks*, Journal of Biomedical and Health Informatics.18(2) 2014 440-448.doi: 10.1109/JBHI.2013.2293620.
5. Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, Konstantinos Rantos, *Lightweight Cryptography for Embedded Systems - A Comparative Analysis,Data Privacy Management and Autonomous Spontaneous Security.*,LNCS,Springer.8247 2014 333-349.doi: 10.1007/978-3-642-54568-9_21.
6. Zheng Gong,Svetla Nikova , YeeWei Law, *Klein: A new family of lightweight block ciphers,Security and Privacy*. RFIDSec 2011.LNCS,Springer.7055 2012 1-18,doi:10.1007/978-3-642-25286-0_1.
7. Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, Eita Kobayashi, *TWINE: A lightweight block cipher for multiple platforms*, Selected Areas in Cryptography, LNCS, Springer.7707 2013 339-354.doi: 10.1007/978-3-642-35999-6_22.
8. Wenling Wu, Lei Zhang, *Lblock:A lightweight block cipher*,Applied Cryptography and Network Security,LNCS,Springer.6715 2011 327-344.doi:10.1007/978-3-64221554-4_19.
9. Wentao Zhang,Zhenzhen Bao, Dongdai Lin,Vincent Rijmen,Bohan Yang, Ingrid Verbauwhede, *Rectangle: A bit-slice ultra-lightweight block cipher suitable for multiple platforms*, Journal of Science China Information Sciences.58(12)2015 1-15.doi: 10.1007/s11432-015-5459-7.
10. Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita , Taizo Shirai, Piccolo: An UltraLightweight Blockcipher, International conference on Cryptographic Hardware and Embedded systems,LNCS,Springer.6917 2011 342-357.doi:10.1007/978-3-64223951-9_23.
11. Bassam J.Mohd, Thaier Hayajneh, Ahtanasios V.Vasilakos, *A Survey on Lightweight Block ciphers for Low-resource devices: comparative study and open issues*, Journal of Network and Computer Applications,58(C) 2015 73-93.doiI:10.1016/j.jnca.2015.001.
12. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J.B.Robshaw, Yannick Seurin, C. Vikkelsoe, *PRESENT:An ultra-lightweight block cipher. In Cryptographic Hardware and Embedded Systems* LNCS,Springer. 4727 2007 450-466.doi:10.1007/978-3540-74735-2_31.
13. Mickael Cazorla, Kevin Marquet, Marine Minier, *Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks*, International conference on Security and Cryptography.2013 1-6.
14. A. Dunkels, B.Gronvall , T.Voigt, *Contiki-a lightweight and flexible operating system for tiny networked sensors*, IEEE International Conference on Local Computer Networks.2004 455-462.doi:10.1109/LCN.2004.38.
15. Mohammad Ghamari, Balazs Janko, R.Simon Sherratt, William Harwin, Robert Piechockic, Cinna Soltanpur, *A Survey on Wireless Body Area Networks for e-Healthcare Systems in Residential Environments*, Sensors journal.16(6) 2016 831.doi:10.3390/s16060831.
16. Lin Yao, Bing Liu, Guowei Wu, Kai Yao , Jia Wang, *A Biometric Key Establishment Protocol for Body Area Networks*, International Journal of Distributed Sensor Networks.7(1) 2011.doi:10.1155/2011/282986.
17. Ivaylo I Christov, *Real time electrocardiogram QRS detection using combined adaptive threshold*. BioMedical Engineering OnLine. 3(28) 2004.doi:10.1186/1475-925X-3-28.
18. Georgios Selimis , Li Huang, Fabien Mass,Ioanna Tsekoura, Maryam Ashouei, Francky Catthoor,Jos Huisken,Jan Stuyt , Guido Dolmans Julien Penders, Harmke De Groot, *A Lightweight Security Scheme for Wireless Body Area Networks:Design, Energy Evaluation and Proposed Microprocessor Design*, Journal of Medical systems. 35(5) 2011 1289-1298.doi:10.1007/s10916-011-9669-2.
19. Sarah Irum,Aftab Ali,Farrukh Aslam Khan , Haider Abbas, *A Hybrid Security Mechanism*

for Intra-WBAN and Inter-WBAN Communications, International Journal of Distributed Sensor Networks.13(5) 2013 1-11.doi:10.1155/2013/842608.

20. S. Kerckhof,F. Durvaux,C. Hocquet,D. Bol , F.-X.Standaert, *Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint*, Cryptographic Hardware and Embedded Systems,Springer.7428 2012 390-407.doi:10.1007/978-3-642-33027-8_23.
21. Lejla Batina, Amitabh Das, Bars Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede, Tolga Yalc, *Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures*, RFIDsec, LNCS, Springer,8262 2013 101-110.
22. Carmen C.Y.Poon , Yuan-Ting Zhang, *A Novel biometrics method to secure wireless body area sensor networks for Telemedicine and M-Health*, EEE Communications Magazine.44(4) 2006 73-81.doi: 10.1109/MCOM.2006.1632652.
23. MIT Physionet database.[Online]. http://www.physionet.org/physiobank/database/nsrdb/
24. Jiapu pan ,Willis j.Tompkins, *A real-time QRS detection algorithm*, IEEE transactions on biomedical engineering.32(3) 1985 230-236.doi:10.1109/TBME.1985.325532.
25. Narmadha T, Kalaiarasi M, Meenakshi M, *Lightweight secure ECG transmission in Wireless body area networks- a PRESENT cipher based implementation*, IEEE conference on communication and signal processing.2017.
26. Meiqin Wang, *Differential Cryptanalysis of Reduced-Round PRESENT*, International Conference on Cryptology in Africa ,Progress in Cryptology AFRICACRYPT,LNCS.5023 2008 40-49.doi:10.1007/978-3-540-68164-9_4.
27. Onur zen,Kerem Varc,Cihangir Tezcan, elebi Kocair, *Lightweight Block Ciphers Revisited:Cryptanalysis of Reduced Round PRESENT and HIGHT*. Australasian Conference on Information Security and Privacy.5594 2009 90-107.doi:10.1007/978-3-642-02620-1_7.
28. Guo-Qiang Liu , Chen-Hui Jin, *Differential cryptanalysis of PRESENT-like cipher*, Journal of Designs, Codes and Cryptography archive,76(3) 2015 385-408.doi:10.1007/s10623-014-9965-1.
29. Andrey Bogdanov,Dmitry Khovratovich , Christian Rechberger, *Biclique Cryptanalysis of the Full AES*, International Conference on the Theory and Application of Cryptology and Information Security,ASIACRYPT.7073 2011 344-371.doi:10.1007/978-3-642-25385-0_19.
30. Charles Bouillaguet,Patrick Derbez, Pierre-Alain Fouque, *Automatic Search of Attacks on Round-Reduced AES and Applications*. Advances in Cryptology CRYPTO 2011, 6841 2011 169-187,doi:10.1007/978-3-642-22792-9_10.
31. Huseyin Demirci, Ihsan Taskn, Mustafa Coban, Adnan Baysal, *Improved Meet-in-the-Middle Attacks on AES*, Progress in Cryptology - INDOCRYPT,2009 144-156.doi:10.1007/978-3-642-10628-6_10.
32. B Bahrak, M.R Aref, *Impossible differential attack on seven-round AES-128*, IET Information Security.2(2) 2008 28-32.doi:10.1049ietifs:20070078.
33. Ashokkumar C , Ravi Prakash Giri , Bernard Menezes, *Highly Efficient Algorithms for AES Key Retrieval in Cache Access Attacks*, IEEE European Symposium on Security and Privacy.2016.doi:10.1109EuroSP.2016.29.
34. Muhammad umar farooq, Thomas kunz, Operating systems for wireless sensor networks-a survey.Sensors,mdpi,11(6) 2011 5900–5930.doi:10.3390/s110605900.
35. Contiki: The Open Source OS for the Internet of Things.[Online].www.contiki-os.org.
36. Tmote Sky-Ultra low power IEEE 802.15.4 compliant wireless sensor module. [Online].http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/tmote-sky-datasheet.pdf.
37. TelosB mote platform. [Online]. http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf.