APPLICABILITY OF RC4 ALGORITHM IN BLUETOOTH DATA ENCRYPTION METHOD FOR ACHIEVING BETTER ENERGY EFFICIENCY OF MOBILE DEVICES

Sivalingham Latchmanan[1] Dr.Sharmin Parveen[2]
Department of Computer System and Technology, Faculty of Computer Science and Information Technology,
University of Malaya, 50603 Kuala Lumpur, Malaysia.
[1]Email: sivalingham@sensata.com
[2]Email: sharmin@um.edu.my

ABSTRACT

This paper focuses on the applicability of RC4 algorithm in Bluetooth data encryption method for achieving better energy efficiency of mobile devices during data transfer. Present E0 encryption algorithm of the Bluetooth standard has the difficulty of slow operational speed which in turn consumes more battery life of Bluetooth devices and also there are chances for the attacker to break the encryption. In this paper, RC4 encryption algorithm has been implemented replacing the E0 to strengthen the encryption as well as to overcome the power limitations that mobile devices exhibit. A simulation was conducted to verify the applicability of RC4 encryption algorithm by comparing the encryption time and memory usage among RC4 and E0 while encrypting and decrypting. The simulation result shows significant improvement to support the "go green" concept by reducing the energy consumption while encryption took place.

Keywords: ***Bluetooth, Encryption, E0, RC4, Energy Efficiency, Green ICT***

1.0 Introduction

The global information and communications technology (ICT) industry accounts for approximately 2 percent of global carbon dioxide (CO2) emissions which contribute to global warming and climate change [1]. Mobile Telecom is one of the contributing factors in the ICT carbon footprint. Hence, there is a need for solution to optimize energy consumption in the ICT sectors. Such solutions are collectively referred to as Green ICT [1]. Green ICT focused more on protecting environment by reducing the emissions of energy (CO2). In order to design more energy efficient mobile devices the battery consumption of the mobile devices should be reduced in various mobile applications. In this direction Bluetooth technology was reviewed especially on its encryption method that could be enhanced for green ICT through algorithmic efficiency.

Bluetooth technology is one of the wireless connections available for free communication between devices in short range. It operates at 2.4 GHz radio frequency range and has the capabilities of point-to-multipoint connection at the speed up to 1 Mbps [3].It has gained quick popularity among mobile user to share data, images and other applications. As countries around the globe is seeking ways to ensure stability in supply and energy demand, Bluetooth as low energy technology promises to change the way we think about power consumption [4].Recent years witnessed strains in electrical grid as the demand for electricity has shooted up. High-profile blackouts, like the one in August 2003 that crippled New York City[4] or the blackout that disrupted services in Italy and Switzerland just a month later [4], Bluetooth as a low energy technologies is being introduced and able to deliver a robust solution.

Encryption and transmission seem to be inevitable process in wireless or mobile technologies to provide security measure. Encryption is the conversion of data into another form called cipher text. Cipher text is an unreadable format of text by unauthorized viewer until it is converted again to plain text with a predefined key [5]. Bluetooth technologies use E0 encryption method. E0 is a stream cipher which generates a sequence of random numbers and combines it with the data using XOR operator. Bluetooth security architectures are weak, especially during initial pairing and if a weak PIN were used. [6] There are also direct attacks on E0 cipher with the high complexity (2^{100} & 2^{66}). Moreover E0 algorithm is very slow in terms of operational speed [7] and theoretically consumes more battery life of Bluetooth devices. In contrast, RC4 encryption method [8] has its strength that would increase the security of Bluetooth environment. It is a shared key stream cipher algorithm requiring a secure exchange of a shared key. It applies a variable length key from 1 to 256 bytes to initialize a 256-byte state table [8].This encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using a 40 and 128-bit keys [9].It is also proven that, RC 4 encryption method still being the best in term of encryption speed compare to other encryption method [10]. While echoing the go green solution being introduced by bluetooth technologies, this paper will be elaborating on the applicabbility of RC4 as the improved encryption algorithm for bluetooth to ensure better security as well as reduction in energy usage while transfering data using bluetooth.

The rest of the paper is organized as follows: Section 2 introduces the background and related work, Section 3 describes the applicability of RC4 algorithm, in Section 4, the implementation of RC4 algorithm in a simulation application is presented. Simulation results are given in Section 5. Finally we concluded the paper in Section 6.

2.0 Background and Related Work

2.1 Green ICT

One of the major challenges being faced in transforming to Green ICT is limited maturity of technical knowledge and also the awareness amongst the ICT users on its emission of carbon footprint. It is evident that ICT sector has a significant carbon footprint [1, 22] and there are researches going on about creating eco-friendly ICT sectors. In general, carbon footprints of the ICT sector are mainly being measured in terms of electricity usage. Besides, there are also other contributors like telecommunication infrastructure, data center etc. Mobile devices have a significant role in this scenario. Fig 1 shows the percentage of the ICT's global carbon emissions. In [1] the authors have presented their investigated result which shows that in telecommunication infrastructure the global carbon footprint of the telecom devices was 18 MtCO2e in 2002 and expected to increase to 51 MtCO2e by 2020. Hence, Green ICT became essential to maximize the energy gains and efficiency increase. One of the strategies in this regard is algorithmic efficiency [23].

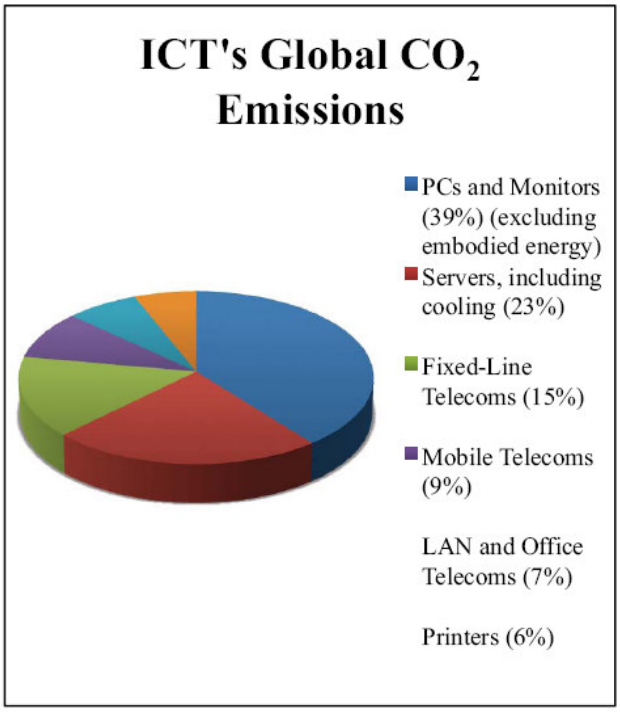

Fig. 1: ICT's Carbon Footprint [2]

2.2 Encryption Methods

Encryption is the conversion of data into another form called cipher text. Basically, there are two methods of generating cipher text, which are stream cipher and block cipher. The two methods are the same except for the size of data on each transfer [11]. Stream ciphers are one of the simplest methods [12] used in encryption where each bits of data is consecutively encrypted using a bit of key. In order to strengthen the stream ciphers, varying length of crypto key could be used which would make the cracking process difficult. Unlike stream ciphers which encrypt every bit, block ciphers are designed to encrypt chunks of data of a specific size. Size of data for each pass (known as block) as well as size of crypto key will be determined before the encryption process [12]. However, stream cipher is still being a favorite method for mobile devices for the following valid reasons:

(1) Stream ciphers are typically faster than the block cipher which ensures the low consumption in energy and memory- both of which could drain the battery life.

(2) Block cipher typically requires more memories , since they work on a larger chunks of data and often have "carry over" from previous blocks, whereas since stream ciphers work s on only few bits at a time they have relatively low memory requirements
(3) Stream ciphers doesn't need padding as requires by block ciphers which operates on complete blocks.

Bluetooth technologies use E0 encryption method. E0 is a stream cipher method which generates a sequence of random numbers and combines it with the data using XOR operator. 128 bits key is the common key used in this technology. E0 generates each bit using four shift registers (LFSR) of various lengths (25, 31, 33, and 39) of bits. Besides that, there are two internal states which carry 2 bits each. For every clock tick, there will be a shift on registers and the internal states get updated with the current state, previous state and the value of shift registers. Those bits will be added with another four bits which are extracted from the shift registers. The first bit of the 2 bit register would be the output for the encoding. Besides that, Bluetooth compute different key for the authentication and encryption as not the case for 802.11. Bluetooth security architectures are weak, especially during initial pairing and if a weak PIN were used [6]. There are also direct attacks on E0 cipher with the high complexity (2^{100} & 2^{66}).

2.3 Limitation of E0 Encryption of Bluetooth Technology

Researches [5, 6, 13, and 14] reveal that, E0 encryption method has significant drawbacks. This can be mentioned as follows:

(1) E0 algorithm is very slow in terms of operational speed and theoretically consumes more battery life of Bluetooth devices.
(2) E0 is an standard algorithm which is not highly comparable on secure environment [7]
(3) The chances for the attacker to break the encryption are by considering two cryptanalytic models:-
    a. If an attacker know the key stream bits and want to recover the secret key
    b. An attacker uses a truly random key stream to guess the right key stream generated.
(4) GSM security could be compromised due to the possibility of key replay and poorly designed co-existence of encryption algorithm. E0 algorithm is considered inadequate to support current needs during data transferring process.
(5) Theoretically, Bluetooth security mechanism which has authentication and encryption should be sufficient to set up local trust domain but due to limitation, the security of WPANs mostly compromises [13]. Most mobile devices have a fixed PIN value and maximum carries four digits value. The quality of random number generators is also questionable.
(6) At the moment, encryption were used only if its needed and each request will be using different encryption key since it uses short encryption key and also to prevent the weakening strength of the key [6]. Encryption is only being done on payload and would need complex algorithm for higher security.

3.0 Applicability of RC4 Encryption Method

Wide investigation has been performed on the basic features of RC4 encryption algorithm to prove this as the appropriate algorithm for Bluetooth encryption method. First of all from the discussion in section 2.2, it clear that stream cipher encryption method is still preferred instead of block cipher method. Listed below, the features of RC 4 encryption method:

(1) RC 4 applies a variable length key from 1 to 256 bytes to initialize a 256-byte state table. The state table will be used for succeeding generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to transform into cipher text. Each element in the state stable is swapped at least once.
(2) Two phases involves in RC 4 algorithm, key setup and ciphering. Key setup carries the most difficult portion of the algorithm where during an N-bit key setup (N = key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of swapping operations. Swapping operation mostly consists of bytes, modulo and some other formulas.
(3) The produced encryption key from key setup would be used in ciphering phase where it is XORed with the plain text message to create an encrypted message. The receiver would decrypt the encrypted message with the same encrypting key.
(4) The RC 4 key is mostly limited to 40 bits but can also goes as high as 128 bits key. The capability is restricted within 1 and 2048 bits and also attracts a lot commercial software package such as bit-torrent, Skype, SSL and Oracle Secure SQL.

Besides that, RC4 has its strength that would increase the security of Bluetooth environment as listed below:-

(1) The difficulties of knowing values in the table

(2) The difficulties of knowing the location in the table used to select each value in sequence
(3) A meticulous RC4 key can be utilized only once
(4) Encryption process is 10 times faster than DES

While this paper focusing on the applicability of RC4 as a replacement for E0 encryption method to reduce energy consumption, research was conducted on the various types of encryptions regardless of stream cipher or block cipher methods. In [10] a comparison has been done among different encryption method based on encryption time. Fig 2 shows the simplified graphs of speed over data comparison for various encryption methods. It is proven that, RC 4 encryption method still being the best in terms of encryption speed compare to other leading encryption methods. As the main objective of this paper is to introduce low energy consumable encryption method for mobile devices, it is important to ensure the low energy consumption of mobile devices which run on limited energy source.

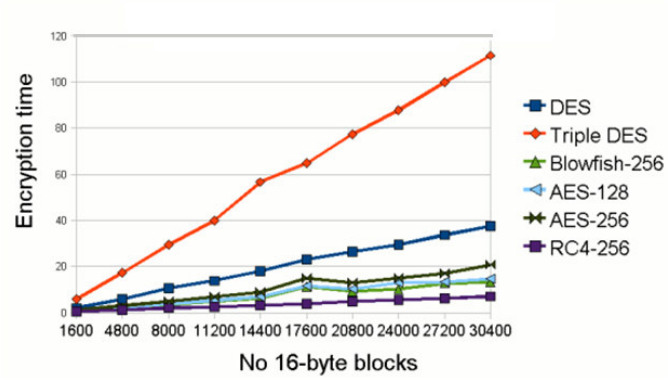

Fig. 2: Comparison of encryption times for various common symmetric encryption algorithms provided as standard in Java 6 [10]

4.0 RC4 Encryption pseudo-code

RC 4 encryption algorithm is given below:

As discussed earlier, the algorithm can be broken into two stages: key setup (initialization) and ciphering (operation). In the initialization stage, the S is populated using 256-bit state table using K (key) as a seed. Once the state table is obtained, it continues to modify in a regular pattern as data is encrypted

The initialization process shown by the pseudo-code [15];

```
j = 0;
for i = 0 to 255:
S[i] = i;
for i = 0 to 255:
j = (j + S[i] + K[i]) mod 256;
swap S[i] and S[j];
```

It is noticeable that the swapping of the 0 to 255 occurs only once in the state table and the values of the state table are being provided. Upon completion of initialization process, the operation process will be as below

```
i = j = 0;
for (k = 0 to N-1)
 {
        i = (i + 1) mod 256;
        j = (j + S[i]) mod 256;
        swap S[i] and S[j];
        pr = S[ (S[i] + S[j]) mod 256]
        output M[k] XOR pr
 }
```

Where M [0...N-1] is the input message consisting of N bits.

The algorithm constructs a stream of pseudo-random values. The input stream is XORed with these values, bit by bit. The encryption and decryption process is the same as the data stream is simply XORed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version [15].

5.0 Implementation of RC4 in a Simulation Application

A simulation application was developed to investigate more on the comparison of E0 and RC 4 encryption method in term of encryption speed and transfer rate as well as battery consumption. The application was developed using Java and with the aid of Blue Cove (Bluetooth DLL). Nokia E71 was used as the mobile devices to receive data from the server. Dell Latitude E6400 was used as the server to transmit data via Bluetooth connection. The server will be creating a dedicated port for the data transfer and will keep it active for a client to send request. Upon successful request, the server re-verify the encryption method proposed by the client and if that is differ from the server preference than, the communication will be dropped. Fig 3 has shown the interface of server simulation which has the multiline text box that records the interaction between client and server. As for comparison purposes, no encryption and E0 encryption were also added as an option that could be selected while transferring data. Fig 4 displays the client simulation application where it has a simple interface to indicate searching for device mode, encryption option and also data transfer details.

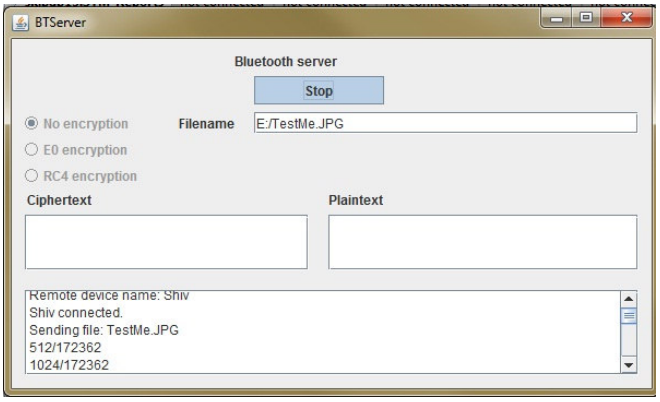

Fig.3: Server Simulator using Java

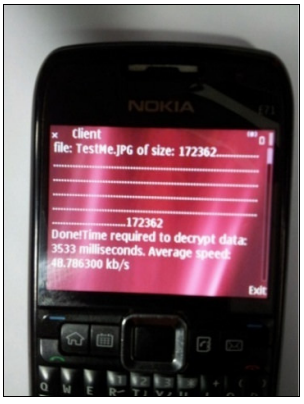

Fig.4: Client Simulator using Java

Since this is the simulation, the encryption method was not embedded into physical layer but just used in application layer to prove its applicability.

6.0 Simulation Results

The simulation above shows that RC4 encryption algorithm has a better hold on complexity as well as performance speed. It has also proven that the faster the encryption process the lesser the energy being used.

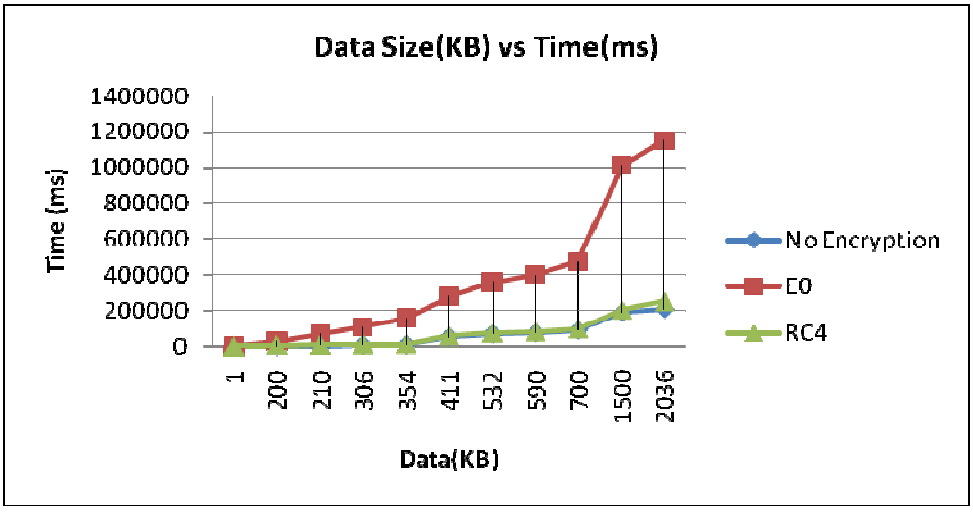

Fig.5: Time comparison for a full encryption cycle between E0 and RC 4 using Java

Besides, Table 1 shows the transfer rate applied while transferring data between server and client with selected encryption method used. This has also proved that, the higher the memory being used the slower the transfer rate. RC 4 again has proved its applicability to keep the energy consumption at the lower end.

Table 1: Transfer Rate to transfer data between server and client

Encryption Method	Data Size	Transfer Rate (Kb/s)
E0	2MB	3.9
E0	4MB	3.2
E0	6MB	2.8
RC4	2MB	9.6
RC4	4MB	8.9
RC4	6MB	8.4

Last comparison was on battery power consumption during a large number of encryption cycles. It was proven again for on the final simulation where RC 4 has better battery power management while E0 encryption method drains more battery power. Fig 6 shows the results charts.

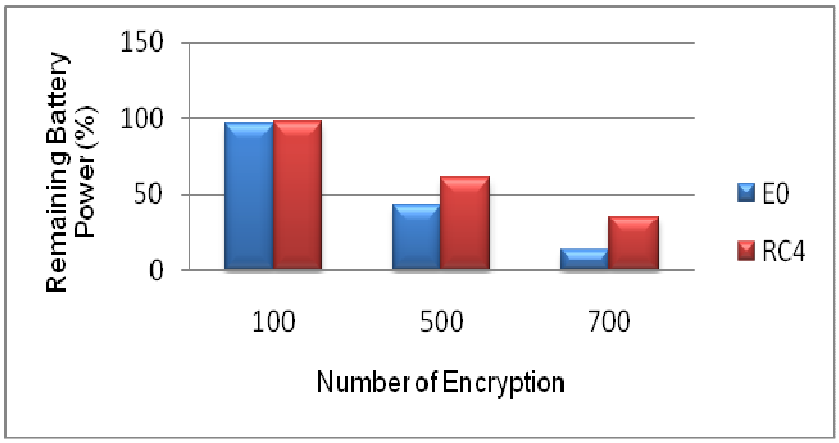

Fig.6: Comparison between E0 and RC 4 on battery power consumption

7.0 Conclusion

There are many advantages of having RC4 encryption algorithm compare to E0. Simulation of RC 4 encryption algorithm, proven to be better in terms of battery power consumption, speed of encryption cycle and memory usage that reflects transfer rate while transferring encrypted data. RC 4 encryption is contributing more towards eco-system in Bluetooth environment compare to E0 encryption method. So the application of RC4 encryption algorithm in Bluetooth data encryption method will reduce energy consumption in mobile devices and makes ICT services green friendly.

8.0 References

[1] Vineetha Paruchuri "Greener ICT: Feasibility of Successful Technologies from Energy Sector", 13th *International Conference on Advanced Communication Technology (ICACT),* 2011, pp. 1398 - 1403

[2] Gartner, "Green IT : The New Industry Shockwave" *Symposium ITXPO conference*, April 2007, doc. 373/494 - pp.1-11

[3] Usman Sarwar, Sureswaran Ramadass, Rahmat Budiarto "A framework For Detecting Bluetooth Mobile Worm*" Malaysia International Conference on Communications*, May 2007, pp. 343 - 347

[4] Bluetooth SIG -*http://www.bluetooth.com/Pages/Going-Green.aspx*, accessed on 2011-08-03

[5] Eric Filiol "Zero Knowledge-like Proof of Cryptanalysis of Bluetooth Encryption", 2006, pp. 285 - 293

[6] Thomas G.Xydis Ph.D. Simon Blake-Wilson "Security Comparison: Bluetooth Communications vs. 802.11", 2002, pp. 1 - 7

[7] Guo F, Zhuang Y.Q. "Analysis of the E0 Encryption System in Bluetooth" *Journal of UEST of China*, Vol.35 No.2 Apr.2006, ISSN:1001-0548.0.2006-02-005

[8] RC4-*https://secure.wikimedia.org/wikipedia/en/wiki/RC4,* accessed on 2011-09-20

[9] RC4 Encryption Algorithm-*http://www.vocal.com/cryptography/rc4.html*, accessed on 2011-09-20.

[10] Comparison of Ciphers-*http://www.javamex.com/tutorials/cryptography/ciphers.shtml* , accessed on 2011-08-03

[11] Wenbo Mao "Modern Cryptography Theory and Practise",*Prentice Hall, New Jersey* 2004, 707 p

[12] Allam Mousa , Ahmad Hamad "Evaluation of the RC 4 Algorithm for Data Encryption" *International Journal of Computer Science and Applications* Vol.3, No.2, June 2006, pp. 44 - 56

[13] M.Othman, W.H.Hassan, A.H. Abdalla, "Developing A Secure Mechanism for Bluetooth based Wireless Personal Area Networks(WPANs)", *Electrical Engineering, ICEE '07. International Conference* 2007, pp.1 - 4

[14] Levy 0. , Wool A. "A Uniform Framework for Cryptanalysis of the Bluetooth E0 Cipher", *Security and Privacy for Emerging Areas in Communications Networks,SecureComm,* 2005 pp. 365 - 373

[15] William Stallings, *Cryptography and network security: Principles and practice*, 5th Edition, NJ,USA, Prentice Hall Press, 2010, Cryptographic algorithms, including public-key cryptography, pp 289 - 310

[16] Peter Dell, Khwaja Shan-ul-Hasan Ghori "A Simple Way to Improve the Security of Bluetooth Devices", *Applications and the Internet, 2008. SAINT 2008. International Symposium*, 2008, pp. 444 - 447

[17] Eric Ke Wang , Yunming Ye , Xiaofei Xu , S. M. Yiu , L. C. K. Hui , K. P. Chow, "Security Issues and Challenges for Cyber Physical System", *Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, 2010, pp.733-738

[18] Lu Y. , Meier W. , Vaudenay S. "The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption*" in Advances in Cryptology*,CRYPTO'05, 2005, pp. 97 – 117

[19] Shaked Y., Wool A. "Cracking the Bluetooth PIN. In Proc 3rd USENIX / ACM Conference, Mobile Systems, Application and Services, 2005, pp 39 - 50.

[20] C.E. Jones, and et. al. "A Survey of Energy Efficient Network Protocols for Wireless Networks*," Wireless Networks*, 2001, pp. 343 – 358

[21] P.Prasithsangaree, P.Krishnamurthy "Analysis of Energy Consumption of RC 4 and AES Algorithms in Wireless LANs" *Telecommunication Program of University of Pittsburgh*,Vol.3, 2003, pp. 1445 - 1449

[22] M. Tahir Riaz, José M. Gutiérrez, Jens, M. Pedersen, "Strategies for the next generation green ICT Infrastructure*",* *2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies, 2009. ISABEL,* 2009, pp. 1 - 3

[23] Agarwal, S.; Nath, A, "Green Computing - a new Horizon of Energy Efficiency and Electronic waste minimization a Global Perspective", *International Conference on Communication Systems and NetworkTechnologies (CSNT),* 2011, pp. 688 - 693

[24] *http://greenict.org.uk/intro* , accessed on 2011-09-20

BIOGRAPHY

Sivalingham Latchmanan is a student at Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya. His research areas include encryption algorithm for Bluetooth based mobile

Sharmin Parveen received the Honors Bachelor of Science degree and M.Sc. degree in Applied Physics, & Electronics from the University of Dhaka, Bangladesh. She received her Ph.D. degree from the University of Dhaka, Bangladesh in 2008. During her Ph.D. research she worked under the joint program of University of Dhaka & Jadavpur University, WB, India. Currently, she is a Visiting Lecturer in the department of Computer System and Technology, University of Malaya. As an academician she has worked in different Universities in different countries (Bangladesh, India and Indonesia). She is an IEEE member for 8 years. Her research interests include wireless and mobile communication, green ICT, multimedia traffic analysis, video over wireless, Telemedicine