www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 7 July 2017, Page No. 21986-21994
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i7.15

Energy Efficient E0 Algorithm for Wireless Transceivers

S.Suresh[1], *R.Nagarajan*[2], *R.Prabhu*[3], *N.Karthick*[4]

[1]Asst. Professor, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Namakkal, India.
[2]Professor, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Namakkal, India.
[3,4]Asst. Professor, Department of Electronics and Communication Engineering, Gnanamani College of Technology, Namakkal, India.
krnaga71@yahoo.com

Abstract*: **The Bluetooth is main technology which was developed a group called Bluetooth Special Interest Group (SIG), formed in May 1998. The Bluetooth is a propose standard for short range wireless communication of devices. It uses radio waves to transfer information, so it is very susceptible to attacks. To protect the user's information, it uses algorithm. The Bluetooth offers methods for generate the authenticating keys for users and encrypting the data. The data encryption mechanism used within the Bluetooth security layer is the E0 stream cipher. A stream cipher is a symmetric cipher in other words; the same secret key is employed for both the encryption and the decryption. The E0 stream cipher is a linear feedback shift registers (LFSR) based key stream generator and the key stream thus generated is XORed with the plaintext to get the cipher text. Each time two Bluetooth devices are need to communicate securely; they first undergo authentication and key exchange protocols whose purpose is to agree on a shared secret, which is used to generate the encryption key. In this paper suggest a uniform framework for cryptanalysis of the E0 cipher. Our method requires 128 known bits of the key stream in order to recover the initial state of the LFSR, which reflects the secret key of this encryption engine. The key stream generator comprises of four LFSR of different lengths, which are combined by a simple finite state machine with 16 memory states. The output of this state machine is the key stream sequence or during initialization phase and the randomized initial start value.***

Keywords: Advanced Encryption Standard-AES, Bit Orientation Technique-BOT, Data Encryption Standard-DES

1. Introduction

The Bluetooth is the technology that enables all kind of electronic devices to communicate with each other. It is a wireless protocol and is usually used for short distance communications, about 10 to 100 meters. It is more light weight than other comparable protocols, such as IEEE 802.11 and is optimized for low power consumption. It was originally developed by Ericsson, though after 1999 it is being developed by a company consortium called the Bluetooth Special Interest Group or simply SIG. Today several versions of the Bluetooth specifications exist with the latest being Bluetooth 2.0, which is most of the products in the market are still Bluetooth 1.2 or 1.1. This protocol is also being standardized by IEEE as the 802.15.1 protocol [1]. The Bluetooth protocol is being used by numerous mobile phone devices as a cheap connection method with nearby devices, by printers and other home appliances. It can be seen as the wireless equivalent of the USB protocol. Even though this protocol is not used for high stake transactions, its popularity and widespread usage, triggers us into looking at its security offerings [2].

During the past two decades, the progress in microelectronics and VLSI drove the cost of many consumer electronic products down to an acceptable level for average people. Only in the 1st quarter of 2001, over 32.5 million PCs were sold. The number of cellular phones is predicted to reach one billion in 2005. With the increase of the number of these devices, so does the need of connecting them together. Today numerous kinds of special cables are used for interconnection. It's cumbersome, not interchangeable and expensive. The Bluetooth is devised to replace these cables [3].

The Bluetooth is a technology for short range wireless data and real time two-way voice transfer providing data rates up to 3 Mb/s. It can be used to connect almost any device to another device. Bluetooth enabled devices, such as mobile phones, headsets, PCs, laptops, printers, mice, and keyboards, are widely used all over the world. Already in 2006, the one billionth Bluetooth devices were shipped, and the volume is expected to increase rapidly in the near future. The target volume for 2010 is as high as two billion Bluetooth devices. Therefore, it is very important to keep Bluetooth security issues up-to date. As an interconnection technology, Bluetooth has to address all traditional security problems, well known from distributed networks. In addition, security issues in wireless ad-hoc networks are much more complex than those of more traditional wired or centralized wireless networks [4].

Moreover, Bluetooth networks are formed by radio links, which means that there are additional security aspects whose impact is not yet well understood. The aim of our work is to evaluate security threats in Bluetooth enabled systems counter measures against each type of attack are also proposed. Thirdly, some of the existing Bluetooth security attacks are enhanced and new attacks are proposed. To carry out these attacks in practice, Bluetooth security analysis tools are implemented counter measures that render these attacks impractical are also proposed. Finally, a comparative analysis of the existing Man-In-The-Middle attacks on Bluetooth is presented, a novel system for detecting and preventing intrusions in Bluetooth networks is proposed, and a further classification of Bluetooth-enabled ad-hoc networks is provided [5], [6].

After learning about and analyzing the security of Bluetooth, it was clear to that Bluetooth sniffing tools are still substandard compared to those available for sniffing other types of wireless traffic like WiFi [7]. This makes it harder for hackers to develop exploits for Bluetooth devices but also makes it more difficult for security researchers to realistically evaluate the Bluetooth security. The best way to address this problem is to continue development of the software for the Bluetooth module, currently the most cost effective hardware device for sniffing Bluetooth packets. The Bluetooth is a widespread technology with real privacy and security implications. Furthermore, explore the current capabilities of using inexpensive open source software and hardware to examine data from arbitrary Bluetooth devices.

The Random Block Size image encryption technique where encryption is done by first at block level and then using Blowfish method for encrypt the image. The original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The image can be decomposed into blocks each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation will be decreased and thus becomes difficult to predict the value of any given pixel from the values of it neighbors [8].

The Fixe Block Size image encryption technique where they introduce a block based transformation algorithm based on the combination of image transformation and a well know encryption and decryption algorithm called Blowfish. The plain image can be decomposed into blocks; each one contains a specific number of pixels (4 pixels × 4 pixels blocks). Increasing the number of blocks by using smaller block sizes resulted in a low correlation and higher entropy the blocks are transformed into new locations. The generated image is then fed to the Rijn Dael encryption algorithm [9].

The cryptography is one of the ways to secure electronic documents and encryption is the important in data and network security. The aim of this study is to enhance the strength of already existing technique. The drawback in that technique was in efficiency of generation which is essential for any encryption algorithm; the prolific growth of network communication system entails high risk of breach in information security. This substantiates the need for higher security for electronic information. The triple SV (3SV), with 256 block size and 112 bit key length method has suggested. Generally, the stream ciphers produce higher avalanche effect but Triple SV producing good avalanche effect with a block cipher implementation. The CBC mode has been used to attain higher avalanche effect suggested technique has implemented in C language. Another key generation technique is Fauzan-Mustafa Encryption Technique (FMET) has been suggested in this work in the field of high security.

A session based symmetric key cryptographic system has been used and it is termed as Bit Orientation Technique (BOT) [10]. The BOT consider the explain text (i.e. the input file) as binary string with finite no. of bits. The input binary string is broken down into manageable sized blocks to fit diagonally upward from left to right into a square matrix of suitable order.

RC4 has been the most popular stream cipher in the history of symmetric key cryptography. Designed in 1987 by Ron Rivest, RC4 is the most widely deployed commercial stream cipher, having applications in network protocol such as SSL, WEP, WPA and in Microsoft Windows, Apple OCE, Secure SQL, etc. For the first time in RC4 literature, was report significant key stream biases depending on the length of RC4 secret key. The identified and partially solved by Ohigashi,Watanabe and Morii in FSE 2013 [11].

2. Stream Cipher Algorithm

Wireless networking standards, such as IEEE802.11 and Bluetooth, provide local connectivity. In particular, with Bluetooth, various devices can work together through ad hoc networks, marking the beginning of a standard that enables wireless machine-to-machine communications between each and every intelligent device and every appliance. Many low level protocols are not secure, and the use of more secure high level protocols is limited by the processing capabilities of mobile devices [12]. The Bluetooth could enhance and extend privacy applications because it is well suited to the power requirements of mobile applications. The software 1 implementation was coded in C language and executed on a 200 MHz Pentium PC. The Software 2 implementation was coded in Assembly language and executed on an 8 bit MCS-51 family processor. The general purpose processors that can be handle the necessary crypto functions in a negligible fraction of their capacity. In recent years, the custom circuits that inexpensively fulfill the crypto demands of specialized applications. However, the cost and power requirements of high performance general purpose processors still make their use in mobile devices impractical. Hardware support for low power microprocessors will play a significant role in the security implementations for Bluetooth solutions [13]. In the past, they use many low security protocols such as data encryption standard (DES) algorithm and advanced encryption standard (AES) algorithm.

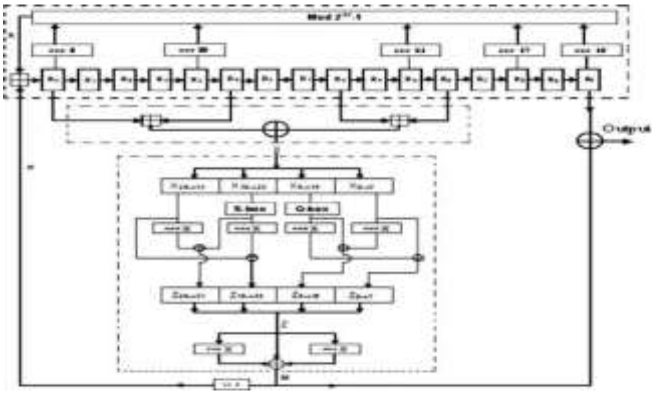

Figure 1 Block Diagram of Wireless Networking System

The key length used in this algorithm is very low. It allows the attackers to easily hack the transmitted information, by breaking the security code. The proposed algorithm was the block cipher protocol. It provides only minor security, relatively low speed, especially for 32 and 64 bit microprocessor based implementations. Figure 1 shows the block diagram of wireless networking system.

The A5/1 is one of the stream cipher algorithm that is currently using by the most of the countries around the world in order to ensure privacy of conversations on GSM mobile phones. The A5/1 consists of 3 shift registers named R1, R2 and R3 with method of majority clocking and 22 bit frame number which these are first shifted into the left side of all 3 registers and XORed with the feedbacks. Then A5/1 is clocked by using the majority clocking for 100 cycles to initial mix the bits. Then, next 114 bits of output from A5/1 is XORed with the plain text to encrypt/decrypt. The second one is the method of Barkan. Here the cipher text only attack on A5/1 that can recover by using only four frame of text cipher A5/2 stream cipher algorithm: The A5/2 is the 2nd stream cipher algorithm that currently support by GSM protocol in many countries. In 2006, Elad Barkan Eli Biham and Nathan Keller demonstrated attacks against A5/1 and A5/2, that allow attackers to tap GSM mobile phone conversations and decrypt them either in real time, or at any later time. The protocol weaknesses of GSM allow to recovery of the secret key [14], [15].

According to survey on the attacks against A5/2 stream cipher algorithm, it has been determined that exist linear relations among the output sequence bits and the vast majority of the unknown output bits can reconstructed. Furthermore some researcher have shown the time complexity of the attack proportional to 2, while according on GSM declaration the complexity of A5/2 should be 2^64. A5/1 stream cipher algorithm have some disadvantages: such as all information of a plaintext symbol is contained in a single cipher text symbol and an active interceptor who breaks the algorithm might insert spurious text that looks authentic [16], [17].

3. E0 Stream Cipher Algorithm

The E0 is a stream cipher used in the Bluetooth protocol. It generates a sequence of pseudorandom numbers and combines it with the data using the XOR operator. The key length may vary, but is generally 128 bits. At each iteration the E0 generates a bit using four shift registers of differing lengths (25, 31, 33, 39 bits) and two internal states, each 2 bits long. At each clock tick, the registers are shifted and the two states are updated with the current state, the previous state values in the shift registers and the E0 algorithm XOR that sum with the value in the 2 bit register. The first bit of the result is output for the encoding. The E0 is divided in three parts such as payload key generation, Key stream generation and encoding [18].

The setup of the initial state in Bluetooth uses the same structure as the random bit stream generator. This are dealing with two combined E0 algorithms. An initial 132 bit state is produced at the first stage using four inputs such as 128 bit key, Bluetooth address on 48 bits and 26 bit master counter. The key has variable length, but is always a multiple of 2 between 8 and 128 bits and the 128 bit keys are generally used. These are stored into the second stage of the shift registers. The 200 pseudorandom bits are then produced by 200 clock ticks, and the last 128 bits are inserted into the shift registers. It is the stream generators initial state [19], [20].

In cryptography, a stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (key stream), typically by an exclusive-or (XOR) operation. In a stream cipher the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption. An alternative name is a state cipher, as the encryption of each digit is dependent on the current state. In practice, the digits are typically single bits or bytes. In this paper suggest a uniform framework for cryptanalysis of the E0 cipher. In this method requires 128 known bits of the key stream in order to recover the initial state of the Linear Feedback Shift Registers (LFSR), which reflects the secret key of this encryption engine. The key stream generator comprises of 4LFSR of different lengths, which are combined by a simple finite state machine called the summation combiner with 16 memory states. The output of this state machine is the key stream sequence or during initialization phase, the randomized initial start value [21], [22].

The security for Bluetooth is provided on the various wireless links, in other words, link authentication and encryption may be provided, but true end-to-end security is not possible without providing higher layer security solutions on the top of Bluetooth. Briefly, the three basic security services defined by the Bluetooth specifications are given below [23]:

(i). Authentication – A goal of Bluetooth is the identity verification of communicating devices. This service provides an abort mechanism if a device cannot authenticate properly.

(ii). Confidentiality – Confidentiality or privacy, is another security goal of Bluetooth. The intent is to prevent information compromise caused by eavesdropping (passive attack).

(iii). Authorization – A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses the question, has this device been authorized to use this service.

During the establishment of personal area networks security process based on the Bluetooth link key generation. The link key is generated during an initialization phase, while two Bluetooth devices that are communicating are associated per Bluetooth specification; two associated devices simultaneously derive link keys during the initialization phase when a user enters an identical PIN into both devices. After initialization is complete, the devices automatically and transparently authenticate and perform encryption of the link. It is possible to create a link key using higher layer key exchange methods and then import the link key into the Bluetooth modules. The PIN code used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4 digit PIN may be sufficient for some applications; however, longer codes may be necessary [24].

The Bluetooth authentication procedure is in the form of a challenge response scheme. Two devices interacting in an authentication procedure are referred to as the claimant and the verifier. The challenge response protocol validates devices by verifying the knowledge of a secret key (a Bluetooth link key). One of the Bluetooth devices (the claimant) attempts to reach and connect to the other (the verifier). The steps in the authentication process are the following: The claimant transmits its 48 bit address (BD ADDR) to the verifier. The verifier transmits a 128 bit random challenge (AU RAND) to the claimant. The verifier uses the E1 algorithm to compute an authentication response using the address, link key and random challenge as inputs. The claimant returns the computed response, SRES, to the verifier. The verifier compares the SRES from the claimant with the SRES that it computes. If the two 32 bit SRES values are equal, the verifier will continue connection establishment [25].

Figure 2 shows the block diagram of Bluetooth encryption system. The Bluetooth specification also allows three different encryption modes to support the service confidentiality such as: Encryption Mode 1: No encryption is performed on any traffic. Encryption Mode 2: Broadcast traffic goes unprotected (not encrypted), but individually addressed traffic is encrypted according to the individual link keys and Encryption Mode 3: All traffic is encrypted according to the master link key [26].

DOI: 10.18535/ijecs/v6i7.15

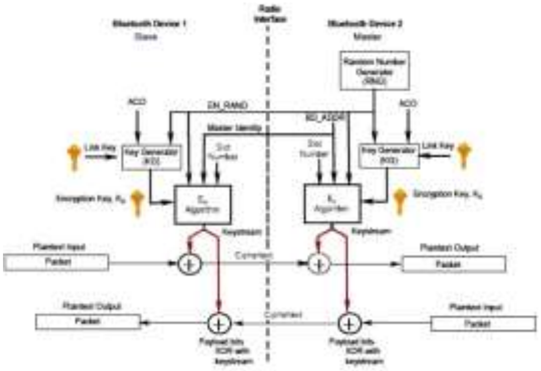

Figure 2 Block Diagram of Bluetooth Encryption

The Bluetooth has three different modes of security. Each Bluetooth device can operate in one mode only at a particular time. The three models are the following: Mode-1-Non secure mode, Mode-2-Service level enforced security mode and Mode-3-Link level enforced security mode.

In Mode-1, a device will not initiate any security procedures. In this non-secure mode, the security functionality (authentication and encryption) is completely bypassed. In effect, the Bluetooth device in Mode-1 is in a mode that allows other Bluetooth devices to connect to it. This mode is provided for applications for which security is not required, such as exchanging business cards.

In Mode-2, the service level security procedures are initiated after channel establishment at the logical link control and adaptation protocol (L2CAP) level. The L2CAP resides in the data link layer and provides connection oriented and connectionless data services to upper layers. For this security mode, a security manager controls access to services and to devices. The centralized security manager maintains polices for access control and interfaces with other protocols and device users. Varying security polices and "trust" levels to restrict access may be defined for applications with different security requirements operating in parallel. This is a built in security mechanism, and it is not aware of any application layer security that may exist. This mode supports authentication (unidirectional or mutual) and encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key, a pairing procedure is used when the two Bluetooth devices communicate for the first time.

In Mode-3, the Bluetooth allows two levels of trust and three levels of service security. The two levels of trust are "trusted" and "untrusted". The trusted devices are ones that have a fixed relationship and therefore have full access to all services. The untrusted devices do not maintain a permanent relationship; this results in a restricted services access. For services, three levels of security have been defined. These levels are provided so that the requirements for authorization, authentication and encryption can be set independently.

Service level 1: Those that are require authorization and authentication. Automatic access is granted only to trusted devices. The untrusted devices need manual authorization.

Service level 2: Those that are require authentication only, access to an application is allowed only after an authentication procedure.

Service level 3: Those that are open to all devices, the authentication are not required, and access is granted automatically. Associated with these levels are the following security controls to restrict access to services: authorization and encryption required link is encrypted before the application is accessed [27], [28].

The Bluetooth architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices can get access only to specific services and not to others. It is important to understand that, the Bluetooth core protocols can authenticate only devices and not users. This is not to say that user based access control is not possible. Thus, it is possible to enforce user based authentication and fine grained access control within the Bluetooth security framework [29].

It is possible to grant access to some services without providing access to other services, example: on a cellular phone, service discovery records shall be accessible, whereas dialup networking shall only be available for specific devices. The security architecture supports security policies for devices with some services communicating with changing remote devices, example: file transfer or business card exchange. Access granted to a service on such device does not open up access to other services on the device not grant future access automatically or in an uncontrolled way to services on the device. The user intervention for access to services is avoided as much as possible. It is only needed to allow devices limited access to services or for setting up trusted relationship with devices allowing unlimited access to services. This architecture does not deal with application level security, but such concepts are not excluded. The following scenarios have been considered in identifying the limitations.

Scenario - 1: There are two Bluetooth devices (e.g., PDAs). Each device has a set of applications: calendar, file synchronization, etc. The two devices will communicate, over a Bluetooth link, to perform a certain task such as file synchronization.

Scenario - 2: There are more than two of scenario 1 devices. All devices will communicate over Bluetooth links to perform tasks that do not require security such as exchanging business cards.

Scenario - 3: A small device such as a PDA requires access, over a Bluetooth link to infrastructure services: the Internet, e-commerce applications, corporate database, etc.

Such device will be connected to a "LAN Access Point" over the BT link. The LAN Access Point will be connected to the infrastructure services via a wired or wireless LAN. This is a 3-tier configuration where tier-1 is the small device, tier-2 is the LAN access point, and tier-3 is the infrastructure services.

The Bluetooth Security architecture has the following limitations such as: Support for legacy applications. In all scenarios, the legacy application will not make calls to the security manager. Instead a Bluetooth aware "adapter" application is required to make security related calls to the Bluetooth security manager on behalf of the legacy application. Only a device is authenticated and not its user. If there is a need for authentication of the user, other means – e.g., application level security features – will be necessary. Refer to scenario 1. There is no mechanism defined to preset authorization per service. However, a more flexible security policy can be implemented with this architecture, without a need to change the Bluetooth protocol stack. Of course, modifications of the security manager and the registration processes would be necessary.

The approach only allows access control at connection set-up. The support for the 3-tier configuration in scenario 3: The security architecture presented in this paper is built upon the

Bluetooth baseband security procedures that address the BT link security and mutual device authentication at each end of the link. To address the end-to-end security issue present in cases like in scenario 3, this paper assumes the existence of a "higher-level" end-to-end security solution which may utilize the Bluetooth security architecture presented for accessing devices and services directly present at the two ends of as Bluetooth link. The authentication is the process of verifying "who" is at the other end of the link. Authentication is performed for devices (BD_ADDR). The Bluetooth is achieved by the authentication procedure based on the stored link key or by pairing (entering a PIN) [30]. Figure 3 shows the flowchart for authentication procedure.

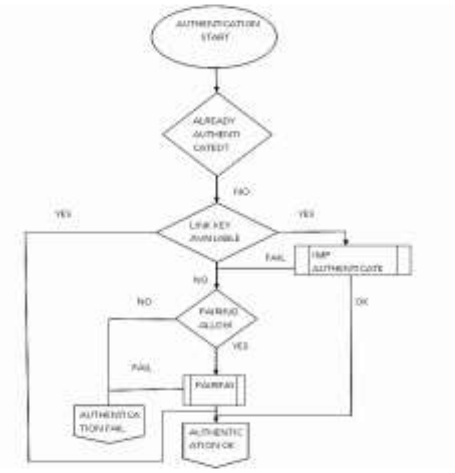

Figure 3 Flowcharts for Authentication Procedure

The authorization is the process of deciding if device X is allowed to have access to service. This is where the concept of trusted exists. The trusted devices (authenticated and indicated as "trusted"), are allowed access to services. The untrusted or unknown devices may require authorization based on user interaction before access to services is granted. This does not principally exclude that the authorization might be given by an application automatically. Authorization always includes authentication [31]. Figure 4 shows the flowchart for authorization procedure.

The user can change the unit key, but this will not be done in practice. It is sorted in non-volatile memory. The unit key is only used if one of the devices does not have enough memory to store session keys. It is generated as follows: first, the device calculates a random number and the Bluetooth address, which is a factory established parameter unique for every device. More information about the key generation algorithm E21 can be found in the Bluetooth standard.

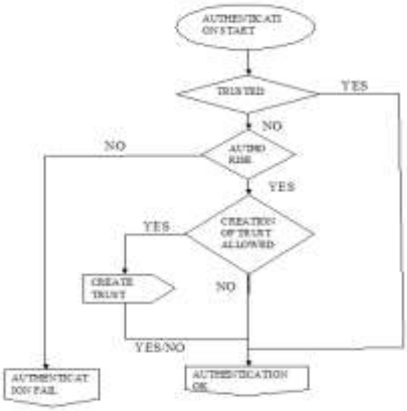

Figure 4 Flowcharts for Authorization Procedure

The Bluetooth devices still do not share a session key. This will be done in different steps. First, an initialization key is generated. This temporary key is a function of a random number IN_RAND, which is generated by the device that initiated the communication and sent to the other device, a shared PIN and the length L of the PIN. The PIN should be entered in the both devices. The length of the PIN can be chosen between 8 and 128 bits. Typically it consists of 4 decimal digits. If one of the devices does not have an input interface, a fixed PIN is used; often the default value is 0000. This procedure is shown in the Figure 5. The result is a temporary shared key (the initialization key). More information about the key generation algorithm E22 can be found in the Bluetooth standard [32].

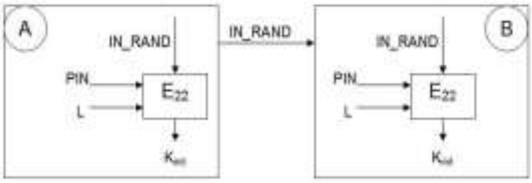

Figure 5 Generation of Initialization Key

The both devices now share an initialization key. This will be used to agree on a new; semi permanent key is called the link key. The link key will be stored on both devices so that it can be used for future communication. Depending on the memory constraints of both devices, the link key can be the unit key of the memory constrained device or combination key derived from the input of the both devices. If the unit key of device A is the link key, it is transmitted encrypted from A to B. This encryption is done by XORing with the initialization key as shown in the Figure 5. If the link key is a combination key, then both devices first generate a random number LK_RAND. These random numbers are encrypted with the initialization key and sent to the other device. Now they both can calculate LK_KA and LK_KB. The combination key KAB is the XOR of LK_KA and LK_KB. This is shown in the Figure 6. The key generation algorithm E21 is the same as the algorithm used for the generation of the unit key. After the generation of the link key, the procedure shown in the Figure 7 and it also executed when a new link key is calculated. The only difference is that the random numbers LK_RAND are encrypted with the old link key. The result is a new link key which will replace the old link key (this old link key will be discarded).

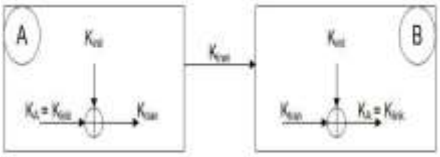

Figure 6 Link Key and Unit Key for A

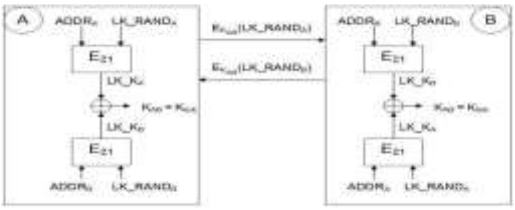

Figure 7 Link Key and Combination Key for A

After a successful generation of the link key and mutual authentication protocol and the encryption key can be generated. The generated random number EN_RANDA and sends this to B. the Both devices generates the encryption key KC = E3 (EN_RANDA, Klink, COF). The CO F value (Ciphering O set Number) is the ACO value which was generated during the mutual authentication protocol. There is however one exception. If the encryption key is used to broadcast encrypted messages, the CO F is equal to the concatenation denoted by || of the Bluetooth address of the sender for broadcast encrypted communication, so COF=ADDR||ADDR. The encryption key KC can be reduced in length to an encryption key KC if necessary. Finally, the encryption key KC or the length reduced key KC is fed to the encryption scheme E0 together with the Bluetooth address and the clock of the master. The result is the key stream K cipher. The master clock is used in order to make the key stream harder to guess. The key stream K cipher is XORed with the data that has to be encrypted.

There are many security weaknesses in the Bluetooth standard. Some of these problems can very easily be exploited by an attacker; other security weaknesses are rather theoretical. An extensive overview of the most important problems will now be given. The initialization key is a function of a random number IN RAN D, a shared PIN and the length L of the PIN. The random number is sent in clear and hence known by an attacker, which is present during the initialization phase. If an attacker obtains the PIN, he knows the initialization key. It even gets worse! Since all the other keys are derived from the initialization key, they also will be known by the attacker. The security of the keys depends on the security of the PIN. If it is too short or weak (e.g., 0000), it is very easy for an attacker to guess the PIN. Note that it is always possible to guess the PIN. The reason is that mutual authentication protocol is executed after the generation of the initialization key. If an attacker observes this protocol, that obtains a challenge and the corresponding response. It is now very easy to perform a brute force attack. The attacker tries every PIN and calculates for every PIN the corresponding response. The shorter the PIN, the faster this brute force attack can be executed. Sometimes axed PIN is used the default value is 0000 or the PIN is sent in clear to the other device. In those cases, the PIN is publicly known and the keys only depend on public values. It is then trivial for an attacker to obtain the secret keys. This certainly has to be avoided in security-sensitive applications [33].

4. Quartus II Design Planning

The first stage in the design planning is the choosing best device for the user application. The device selection affects the rest of the user design cycle, including board specification and layout. Most of this planning is performed outside of the Quartus II software, but this section provides a few suggestions to aid in the planning process. The user should also consider feature requirements, such as I/O standards support, high speed transceivers, global/regional clock networks, and the number of phase locked loops (PLLs) available in the device. The user can review important features of each device family in the selector guides available on the Altera website. Determining the required device density can be a challenging part of the design planning process. The devices with more logic resources and higher I/O counts can implement larger and potentially more complex designs, but may have a higher cost. Select a device that meets the user design requirements with some safety margin, in case the user want to add more logic later in the design cycle or reserve logic and memory for on-chip debugging, consider requirements for specific types of dedicated logic blocks, such as memory blocks of different sizes or digital signal processing (DSP) blocks to implement certain arithmetic functions [34].

If the user has prior designs that target Altera devices, the user can use their resource utilization as an estimate for our new design. The user can compile existing designs in the Quartus II software with the device selection set to Auto to review the resource utilization and find out which device density fits the design. The device power consumption must be accurately estimated to develop an appropriate power budget and to design the power supplies, voltage regulators, heat sink, and cooling system. The power estimation and analysis has two significant.

To ensure the cooling solution is sufficient to dissipate the heat generated by the device. In particular, the computed junction temperature must fall within normal device specifications. The power supplies must provide adequate current to support device operation. The power consumption in FPGA devices in thermal planning is dependent on the design, providing a challenge during early board specification and layout. The Altera power play early power estimator spreadsheet allows the user to estimate power utilization before the design is complete, by processing information about the device resources that will be used in the design, as well as the operating frequency, toggle rates, and environmental considerations [35].

Altera recommends that the user can use the most recent version of third party synthesis tools, because tool vendors frequently add new features, fix tool issues, and enhance performance for Altera devices. The Quartus II software release notes lists, the version of each synthesis tool that is officially supported by that version of the Quartus II software. Specify the user synthesis tool in the new work wizard or the EDA tools settings page of the settings dialog box to use the correct library mapping file (LMF) for the user synthesis net list. The synthesis tools may offer the capability to create a Quartus II work and pass constraints, such as the EDA tool setting, device selection, and timing requirements that the user can specified in the synthesis work. The user can use this capability to save time when setting up user Quartus II work for placement and routing. If the user wants to take advantage of an incremental compilation methodology, the user should partition the design for synthesis and generate multiple output net list files [36].

The ports and parameters for each Mega Wizard Plug-In are described in Quartus II. Help and in the mega function user guides on Altera‟s website. The user should use these references to determine appropriate values for each port and parameter required for a particular variation configuration. Refer to strategies, to determine port and parameter values for more information. The user does not have to specify every port and supported by a Plug-In. The Mega Wizard Plug-In Manager uses default values for any port. For example: <Port>=used, <Port>=unused. The user can specify port names in any order, grouping does not matter. The separate port configuration options from each other with spaces. To specify the value for a parameter with the equal sign, for example: <Parameter>=<value> the user can specify parameters in any order, grouping does not matter. The separate parameter configuration options from each other with spaces. The user can specify the port names and parameter names in upper or lower case; case does not matter.

5. Simulation Results

To perform yhe functional simulations with Quartus II simulator, first to generate a functional simulation net list. A functional net list file is a flattened net list extracted from the design files that does not contain timing information. For timing simulations, first to perform place-and-route and static timing analysis to generate a timing simulation net list. A timing simulation net list includes timing delays of each device atom block and the routing delays. If the user wants to use third party EDA simulation tools, the user can generate a net list using EDA net list writer. The user can use this net list with test bench files in third party simulation tools.

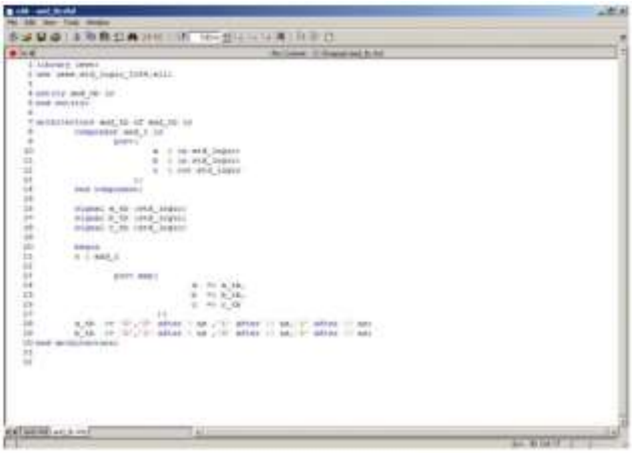

Figure 8 Simulated Programs

The Quartus II simulator supports functional, timing, and timing using fast timings model simulations. The following sections describe how to perform this simulation. The simulation of the work is made in model-sim software by using VHDL language. Thus the programs are coded in the window as shown in Figure 8. After compiling the program, the simulation output is obtained through Graphical Interface mode as shown in Figure 9.

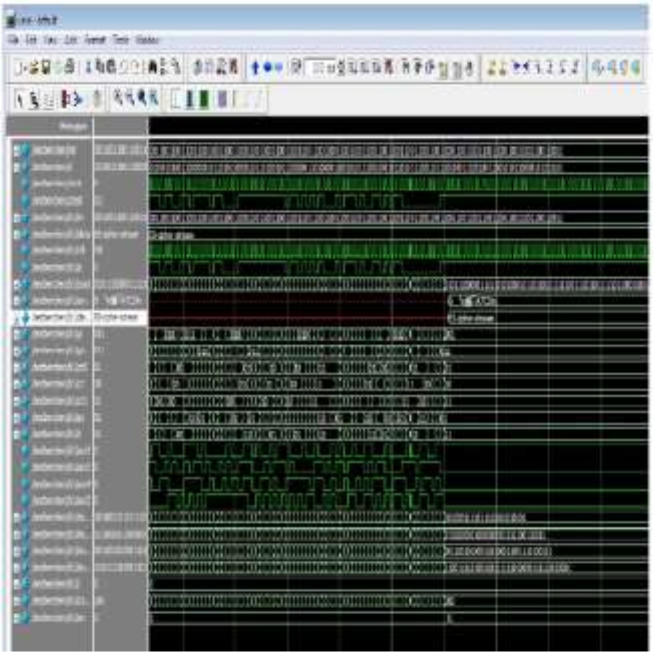

Figure 9 Simulated Outputs

6. Conclusion

In this paper presents the short overview of the security architecture of Bluetooth and especially focus on the key exchange protocol in Bluetooth. This is the most important security critical part of the security architecture. Unfortunately, there are lots of security flaws in the Bluetooth standard. Some are rather theoretical, but most of the problems can be exploited by an attacker. An extensive overview of the security flaws in Bluetooth will be given in this paper. The proposed system presents the Bluetooth security using E0 stream ciphers protocol. The proposed E0 algorithm is implemented in this system and the performance of the proposed E0 algorithm are analyzed. The key generation mechanism functions execute in less than 1.5 ms. The critical path of the key stream generation is short, the achieved throughput is much high in the proposed E0 algorithm.

References.

[1] A. Wang, S. Cho, C. Sodini, and A. Chandrakasan, "Energy efficient modulation and MAC for asymmetric RF micro sensor systems," in Proc Int. Symp. Low Power Design (ISLPED), 2001, pp. 106-111

[2] G. Vidhya Krishnan, R.Nagarajan, T. Durka, M.Kalaiselvi, M.Pushpa and S. Shanmuga priya, "Vehicle Communication System Using Li-Fi Technology," International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20651-20657, March 2017.

[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless micro sensor net works," IEEE Trans. Wireless Commun., pp. 660-670, October 2002.

[4] R.Prabhu, R.Nagarajan, N.Karthick and S.Suresh, “Implementation of Direct Sequence Spread Spectrum Communication System Using FPGA,” International Journal of Advanced Engineering, Management and

Science (IJAEMS), Vol-3.Issue-5, pp. 488-496, May. 2017

[5] A.Mahendran, K.Muthulakshmi and R.Nagarajan, “Triangular Multicarrier SPWM Technique for Nine Level Cascaded Inverter,” International Journal of Scientific & Engineering Research, Vol.4, No.5, pp. 269-275, May-2013.

[6] J.-C. Chen, K. Sivalingam, P. Agrawal, and S. Kishore, "A comparison of MAC protocols for wireless local networks based on battery power consumption," in Proc. Conf IEEE Comput. Commun. Societies, 1998, pp. 150-157.

[7] J.Chandramohan, R.Nagarajan, K.Satheeshkumar, N.Ajithkumar, P.A.Gopinath and S.Ranjithkumar, "Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi," International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20694-20698, March, 2017.

[8] S. Cho and A. Chandrakasan, "Energy efficient protocols for low duty cycle wireless microsensor networks," in Proc. Int. Conf Acoustics, Speech, and Signal Processing, 2001, pp. 2041-2044.

[9] K. Anandhi and Dr. R. Nagarajan, “Mutex-Heart: Fail Safe Dual Chamber Cardiac Pacemaker Device with Rate Responsive Control and Cryptographic Security,” IJSRD-International Journal for Scientific Research & Development. Vol. 3, Issue- 2, pp. 489-493, 2015.

[10] J.Chandramohan, R.Nagarajan, M.Ashok kumar, T.Dineshkumar, G.Kannan and R.Prakash, “Attendance Monitoring System of Students Based on Biometric and GPS Tracking System,” International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol-3.Issue-3, pp. 241-246, Mar. 2017.

[11] S. Cui, A. Goldsmith, and A. Bahai, "Energy-constrained modulation optimization for coded systems," in Proc. IEEE Global Telecomm. Conf:, 2003, pp. 372-376.

[12] R.Nagarajan and M, Saravanan, “Comparison of PWM Control Techniques for Cascaded Multilevel Inverter” International Review of Automatic control (IRACO), Vol.5, No.6, pp. 815-828. Nov. 2012.

[13] R Rameshkumar and R Nagarajan, “Sine Multicarrier SPWM Technique for Seven Level Cascaded Inverter,” CiiT-Programmable Device Circuits and Systems. Vol. 5, Issue- 6, 2013.

[14] Dr.R.Nagarajan, S.Sathishkumar, K.Balasubramani, C.Boobalan, S.Naveen and N.Sridhar. “Chopper Fed Speed Control of DC Motor Using PI Controller,” IOSR-Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 11, Issue 3, Ver. I, pp. 65-69, May – Jun. 2016.

[15] A. Wang and C. Sodini, "A simple energy model for wireless micro sensor transceivers," in Proc. IEEE Global Telecomm. Conf:, November 2005, pp. 3205-3209.

[16] R.Nagarajan and M, Saravanan. “Performance Analysis of a Novel Reduced Switch Cascaded Multilevel Inverter,” Journal of Power Electronics, Vol.14, No.1, pp. 48-60, Jan.2014.

[17] J. Proakis, Digital Communications. New York: McGraw-Hill, 1995.

[18] M.Padmavathi and R.Nagarajan, “Smart Intelligent ATM Using LABVIEW,” International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 5, Issue 5, pp. 41- 45, May-2017.

[19] R.Nagarajan, S.Sathishkumar, S.Deepika, G.Keerthana, J.K.Kiruthika and R.Nandhini, "Implementation of Chopper Fed Speed Control of Separately Excited DC Motor Using PI Controller", International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20629-20633, March, 2017.

[20] A. Molnar and et al., "A single-chip quad-band (850/900/1800/1900 MHz) direct conversion GSM/GPRS RF transceiver with integrated VCOs and fractional-N synthesizer," in IEEE Int. Solid-State Circuits Conf (ISSCC) Dig. Tech. Papers, February 2002, pp. 232-233.

[21] R.Nagarajan, R.Yuvaraj, V.Hemalatha, S.Logapriya, A.Mekala and S.Priyanga, "Implementation of PV - Based Boost Converter Using PI Controller with PSO Algorithm," International Journal of Engineering And Computer Science (IJECS), Volume 6, Issue 3, pp. 20479-20484, March, 2017.

[22] Ms. C. Hemalatha, Mr. R. Nagarajan, P. Suresh, G. Ganesh Shankar and A. Vijay, “Brushless DC Motor Controlled by using Internet of Things,” IJSTE - International Journal of Science Technology & Engineering, Volume -3.Issue-09, pp. 373-377, March-2017.

[23] R. Meyer, W. Mack, and J. Hageraats, "A 2.5 GHz BiCMOS transceiver for wireless LAN," in IEEE Int. Solid-State Circuits Conf: (ISSCC) Dig. Tech. Papers, February 1997, pp. 310-311.

[24] R.Nagarajan and M,Saravanan, “A Carrier - Based Pulse Width Modulation Control Strategies for Cascaded Multilevel Inverter,” International Review on Modeling and Simulations (IRMOS), Vol 6.No1, pp-8-19, Feb. 2013.

[25] S.Suresh, R.Nagarajan, L.Sakthivel, V.Logesh, C.Mohandass and G.Tamilselvan, “Transmission Line Fault Monitoring and Identification System by Using Internet of Things,” International Journal of Advanced Engineering Research and Science (IJAERS), Vol - 4.Issue - 4, pp. 9-14, Apr- 2017.

[26] R.Nagarajan and M,Saravanan “Staircase Multicarrier SPWM Technique for Nine Level Cascaded Inverter,” 2013 International Conference on Power, Energy and Control (ICPEC), IEEE Press, pp-668-675. 2013.

[27] N. Filiol, N. Birkett, J. Cherry, F. Balteanu, G. Gojocaru, A. Namdar, T. Pamir, K. Sheikh, G. Glandon, D. Payer, A. Swaminathan, R. Forbes, T. Riley, S. Alinoor, E. Macrobbie, M. Cloutier, S. Pipilos, and T. Varelas, "A 22mW Bluetooth RF transeiver with direct RF modulation and on-chip RF filtering," in IEEE Int. Solid-State Circuits Conf (ISSCC) Dig. Tech. Papers, February 2001, pp. 202-203.

[28] R.Nagarajan, J.Chandramohan, S.Sathishkumar, S.Anantharaj, G.Jayakumar, M.Visnukumar and R.Viswanathan, “Implementation of PI Controller for Boost Converter in PV System,” International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE). Vol.11, Issue.XII, pp. 6-10, December. 2016.

[29] M.Elangovan, R.Yuvara, S.Sathishkumar and R.Nagarajan, “Modelling and Simulation of High Gain Hybrid Boost Converter,” International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 5, Issue 6, pp. 9- 14, June-2017

[30] R.Nagarajan, J.Chandramohan, R.Yuvaraj, S.Sathishkumar and S.Chandran, “Performance Analysis of Synchronous

SEPIC Converter for a Stand-Alone PV System," International Journal of Emerging Technologies in Engineering Research (IJETER), Vol. 5, Issue - 5, pp. 12-16, May-2017

[31] J. Haartsen and S. Mattisson, "Bluetooth - a new low-power radio interface providing short-range connectivity," in Proc. IEEE, 2000, pp. 1651-1661.

[32] M. Sridhar, S.Sathishkumar, R.Nagarajan and R.Yuvaraj, "An Integrated High Gain Boost Resonant Converter for PV System," International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 5, Issue 6, pp. 54- 59, June-2017

[33] S.-H. Cho and A. Chandrakasan, "A 6.5 GHz CMOS FSK modulator for wireless sensor applications," in IEEE Symp. VLSI Circuits Dig. Tech.Papers, June 2002, pp. 182-185.

[34] N.Karthick, R.Nagarajan, S.Suresh and R.Prabhu, "Implementation of Railway Track Crack Detection and Protection," International Journal Of Engineering And Computer Science (IJECS), Volume 6, Issue 5, May 2017, pp. 21476-21481, DOI: 10.18535/ijecs/v6i5.47

[35] C.Mallika devi and R.Nagarajan, "High-Power Transformer-Less Wind Energy Conversion System with three phase Cascaded Multilevel Inverter," International Journal of Scientific & Engineering Research. Vol. 4, Issue- 5, pp. 67-70, May-2013.

[36] R.Nagarajan and M,Saravanan, "Performance Analysis of Multicarrier PWM Strategies for Cascaded Multilevel Inverter," European Journal of Scientific Research (EJSR), Vol.92 No.4, pp. 608-625, Dec. 2012.

Author Profile

S. Suresh received his B.E. in Electrical and Electronics Engineering from Anna University Chennai, India, in 2010. He received his M.E. in Applied Electronics from Anna University, Chennai, India, in 2012. He is currently working toward his Ph.D. in High Voltage Engineering and Communication System at Anna University Chennai, India. He is currently working as a Assistant Professor of Electrical and Electronics Engineering at Gnanamani College of Technology, Namakkal, Tamilnadu, India. His current research interest includes High Voltage Engineering.

R. Nagarajan received his B.E. in Electrical and Electronics Engineering from Madurai Kamarajar University, Madurai, India, in 1997. He received his M.E. in Power Electronics and Drives from Anna University, Chennai, India, in 2008. He received his Ph.D in Electrical Engineering from Anna University, Chennai, India, in 2014. He has worked in the industry as an Electrical Engineer. He is currently working as Professor of Electrical and Electronics Engineering at Gnanamani College of Technology, Namakkal, Tamilnadu, India. His current research interest includes Power Electronics, Power System, Soft Computing Techniques and Renewable Energy Sources.

R.Prabhu received his B.E. in Electronics and Communication Engineering from Anna University, Chennai, India, in 2006. He received his M.E. in Computer and Communication from Anna University, Chennai, India, in 2008. He is currently working as a Assistant Professor of Electronics and Communication Engineering at Gnanamani College of Technology, Namakkal, Tamilnadu, India.

N.Karthick received his B.E. in Electronics and Communication Engineering from Anna University, Chennai, India, in 2011. He received his M.E. in VLSI Design from Karpagam University, Coimbatore, India, in 2013. He is currently working as a Assistant Professor of Electronics and Communication Engineering at Gnanamani College of Technology, Namakkal, Tamilnadu, India.