Performance Analysis of SAFER+ and Triple DES security algorithms for Bluetooth Security Systems

D.Sharmila *(Research Scholar), Associate Professor, Bannari Amman Institute of Technology, Sathyamangalam.* Tamil Nadu-638401.

Dr.R.Neelaveni, *Asst.Prof. PSG College of Technology, Coimbatore.Tamil Nadu -638401.*

Abstract - In this paper, comparison of the SAFER+ encryption algorithm and Triple DES algorithm for Bluetooth security systems is done. Performance of the above security algorithms are evaluated based on the efficiency of the algorithm. The whole design was captured entirely in matlab. In order to check the efficiency of the algorithm, noise is being added to the encrypted data and the output is seen to be obtained without any incorrectness which justifies the level of security. On comparison, Triple DES algorithm proves to be better for implementation in Bluetooth devices than the SAFER+ algorithm.

Key words: *Secure And Fast Encryption Routine, Triple Data Encryption Standard, Pseudo Hadamard Transform, Encryption and Decryption.*

1. Introduction

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets. This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data. This document provides an overview of Bluetooth technology and discusses related security concerns. There have been several versions of Bluetooth, with the most recent being 2.0 + Enhanced Data Rate (EDR) (November 2004) and 2.1 + EDR (July 2007). While 2.0 + EDR provided faster transmission speeds than previous versions (up to 3 Mbits/second), 2.1 + EDR provides a significant security improvement for link key generation and management in the form of Secure Simple Pairing (SSP).

This publication addresses the security of these versions of Bluetooth, as well as the earlier versions 1.1 and 1.2. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized usage of Bluetooth devices and other systems or networks to which the devices are connected.

There are several security algorithms available to ensure the security in wireless network devices. Some of the major methods are AES, DES, Triple DES, IDEA, BLOWFISH, SAFER+, RC2 to RC5. The SAFER+ algorithm is based on the existing SAFER family of ciphers. Although SAFER+ is the most widely used algorithm, it seems to have some vulnerabilities. Our objective is to compare the Triple DES algorithm and SAFER+ algorithm for the Bluetooth security systems. The Triple DES algorithm uses multiple stages of permutation and substitution, results in a more complex algorithm, which increases the difficulty of cryptanalysis. This shows that TRIPLE DES algorithm proves to be a better one for the implementation in Bluetooth devices than SAFER+ algorithm.

In this paper, section 2 describes the overview of Bluetooth technology, section 3 deals with Bluetooth security. The SAFER+ algorithm is explained in section 4. Section 5 describes the TDES algorithm.

2. Bluetooth Technology

Bluetooth operates at 2.4 GHz frequency in the free ISM-band (Industrial, scientific, and Medical) by using frequency hopping. Bluetooth frequency hopping uses a maximum of 79 different Baseband frequencies to avoid channels that suffer from interference. It also enables a

Manuscript received February 5, 2009
Manuscript revised February 20, 2009

large number of Bluetooth devices to operate at the same 2.4 GHz ISM-band.
Bluetooth communication is described in Section 2.1. Section 2.2 explains the special characteristics of Bluetooth medium. Bluetooth protocols are briefly described in Section 2.3

2.1 Bluetooth communication

Connection types define the possible ways Bluetooth devices can exchange data. Bluetooth has three connection types: ACL (Asynchronous Connection-Less), SCO (Synchronous Connection-Oriented) and eSCO. ACL links are for symmetric (maximum of 1306.9 kb/s for both directions) or asymmetric (maximum of 2178.1 kb/s for send and 177.1 kb/s for receive) data transfer. Retransmission of packets is used to ensure integrity of data. SCO links are symmetric (maximum of 64 kb/s for both directions) and they are used for transferring realtime two-way voice. Retransmission of voice packets is not used. Therefore, when the channel BER is high, voice can be distorted. eSCO links are also symmetric (maximum of 864 kb/s for both directions) and they are used for transferring realtime two-way voice. Retransmission of packets is used to ensure the integrity of data (voice). Because retransmission of packets is used, eSCO links can also carry data packets, but they are mainly used for realtime two-way voice. Only Bluetooth 1.2 or 2.0+EDR devices can use eSCO links, but SCO links must also be supported to provide backward-compatibility.

Bluetooth devices that communicate with each other form a piconet. The device that initiates a connection is the piconet master. One piconet can have maximum of seven active slave devices and one master device. All communication within a piconet goes through the piconet master. The clock of the piconet master and frequency hopping information are used to synchronize the piconet slaves with the master. Two or more piconets together form a scatternet, which can be used to eliminate Bluetooth range restrictions. Scatternet environment requires that different piconets must have a common device, so-called scatternet member, to relay data between the piconets. Figure 1 illustrates Bluetooth topology, when ACL or SCO/eSCO links are used.

When ACL links are used (see Figure 1a), the scatternet member is the slave for both piconets. Device A is the master for piconet 1, and devices B, C, D and E are equal slaves for that piconet. Device F is the master for piconet 2, and devices E, G and H are equal slaves for that piconet. Piconets 1 and 2 together form a scatternet. Piconets 1 and 2 are not synchronized with each other and the scatternet member must multiplex between these two piconets. When SCO or eSCO links are used (see Figure 1b), the scatternet member must be slave for piconet 1 and master for piconet 2. If, for example, master A's clock runs at slightly slower rate than the clock of the common device E, master A's timeslots are drifting slowly to the right. To avoid an eventual overlap of timeslots, the common device E must periodically delay the exchange of voice packets by a pair of timeslots.

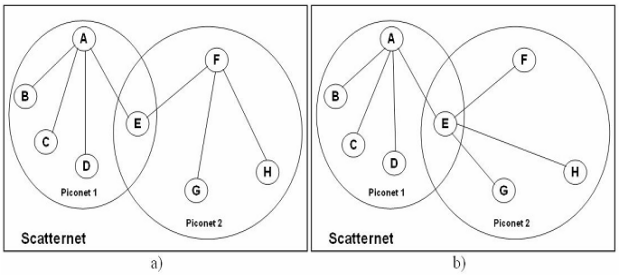


Figure 1. a) Bluetooth topology when ACL links are used.
b) Bluetooth topology when SCO

Only the master device is allowed to delay the exchange of voice packets for SCO or eSCO links. Device A is the master for piconet 1, and devices B, C, D and E are equal slaves for that piconet. Device E is the master for piconet 2, and devices F, G and H are equal slaves for that piconet. Piconets 1 and 2 together form a scatternet.

2.2 Special characteristics of Bluetooth medium

Bluetooth is a wireless RF communication system using mainly omnidirectional antennas. Communication with other Bluetooth devices is possible within the range and no direct line-of-sight between the communicating Bluetooth devices is required. This capability makes Bluetooth communication much easier to use than the traditional cable-based communication or very short range direct line-of-sight infrared communication, but on the other hand it also makes eavesdropping much easier
.
There are three different Bluetooth device classes: class 1, class 2 and class 3. Maximum transmit powers for class 1, class 2 and class 3 devices are 100 mW (20 dBm, i.e. 20 decibels relative to one milliwatt), 2.5 mW (4 dBm), and 1 mW (0 dBm) respectively. According to the Bluetooth specification [Blu04a], the reference sensitivity level of a Bluetooth device has to be -70 dBm or better. The range of Bluetooth devices depends on the class of devices at both ends, the sensitivity levels at both ends, and the level of obstacles. The quantity n is so- called PL (Path Loss) exponent that can be adjusted to account for the amount of clutter in the path between the transmitter and the receiver. The level of obstacles can be roughly divided into four categories: none (a free space without clutter in the transmit-receive path; n=2.0), light (a lightly cluttered path such as an office environment with moveable walls; n=2.5), moderate (a moderately cluttered path such as an

office environment with fixed walls; n=3.0), or heavy (a heavily cluttered path in which the density of the materials used in building's construction is very high; n=4.0). The most common case is a moderate level of obstacles, which is why the Bluetooth specification promises that the Bluetooth device range is from 10 meters (class 3 device) to 100 meters (class 1 device) indoors when the level of obstacles is moderate.

Several assumptions must be made before proceeding with the range calculations. First, let us assume that Bluetooth transmitter's (TX) power is either 0 dBm (class 3 device) or 20 dBm (class 1 device). Second, let us also assume that Bluetooth receiver's (RX) sensitivity level is either -70 dBm (standard sensitivity level) or -80 dBm (enhanced sensitivity level). Third, let us assume that Bluetooth transmit and receive antennas each have a gain of 0 dBi (decibels relative to an isotropic source). The most common TX power for Bluetooth devices is 0 dBm (1 mW). Table 1 presents the range of Bluetooth devices with these prerequisites by using the (PL 40)/(10n) formula d=10 , where d is the range of Bluetooth devices, PL is the Path Loss value, and n is the PL exponent.

Level of obstacles:	n:	TX power (dBm):	RX sensitivity (dBm):	PL:	Range (m):
None	2.0	0	-70	70	32
None	2.0	0	-80	80	100
None	2.0	20	-70	90	316
None	2.0	20	-80	100	1000
Light	2.5	0	-70	70	16
Light	2.5	0	-80	80	40
Light	2.5	20	-70	90	100
Light	2.5	20	-80	100	251
Moderate	3.0	0	-70	70	*10*
Moderate	3.0	0	-80	80	*22*
Moderate	3.0	20	-70	90	*46*
Moderate	3.0	20	-80	100	*100*
Heavy	4.0	0	-70	70	6
Heavy	4.0	0	-80	80	10
Heavy	4.0	20	-70	90	18
Heavy	4.0	20	-80	100	32

Table 1. The range of Bluetooth devices

Bluetooth devices can form ad-hoc networks of several devices in which no fixed infrastructure is needed. This can be very useful, for example, in meetings where all participants have their Bluetooth compatible laptops which can share files with each other without a traditional cable-based interconnection network. On the other hand, security issues in ad-hoc networks are much more complex than those of more traditional wired or Centralized wireless networks.

The design goals for Bluetooth technology have been simplicity, compatibility, inexpensive and compact microchips, fast data transfer, globality, secure communication, and low power consumption. Simplicity means that a Bluetooth device must be as easy as possible to use for a user. Compatibility means manufacturer-independent interoperability between different Bluetooth devices, and it also means backward-compatibility with older Bluetooth versions (see Section 2.1). Bluetooth microchips are also very compact (roughly 5 mm × 5 mm of size) and cheap (roughly 2.50 dollars per microchip [Blu06d, Tan06]). The latest public version of Bluetooth specification, Bluetooth 2.0+EDR, supports data rates up to 3 Mb/s. The future version of Bluetooth specification (Seattle) is expected to provide data rates up to 480 Mb/s. Globality means that Bluetooth can be used all over the world using the same free ISM-band. Bluetooth has built-in security measures at the link level to provide the secure communication for the piconet. Bluetooth microchips have also low power consumption and therefore they are widely used in many different kinds of mobile devices

Bluetooth protocol stack is illustrated in Figure 2. Protocols below HCI (Host Controller Interface) are built-in to the Bluetooth microchip and protocols above HCI are located as a part of the host device's software package. HCI is needed between the hardware and software protocols. The purpose of HCI is to enable manufacturer-independent combining of Bluetooth chips (Host Controller) and the actual host device. HCI takes care of security communication between the host and Bluetooth module.

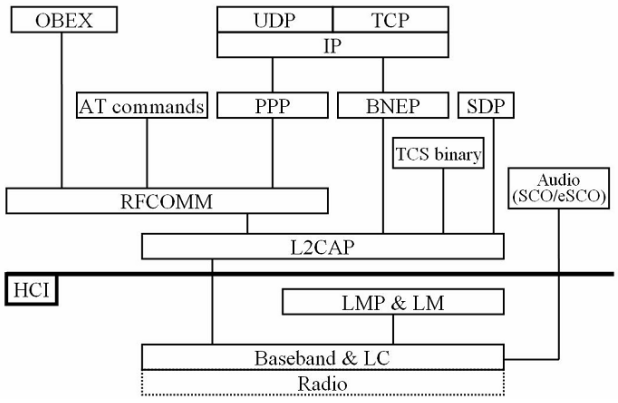


Figure 2. Bluetooth protocol stack

Baseband and LMP (Link Manager Protocol) together enable the physical RF connection. LC (Link Controller) is a state machine that defines the current state of Bluetooth device. Bluetooth device can be, for example, in low-power mode for saving batteries, in the connected state for normal piconet operation, or in the paging state for master to bring new slaves to the piconet. LC has pseudorandom number generation capability, the methods for managing security keys, and capability for

providing the needed mathematical operations for authentication and encryption.

LM (Link Manager) acts as a liaison between the application and the LC on the local device, and it also communicates with the remote LM via PDUs (Protocol Data Units) using the LMP, i.e. the LM communicates with three different entities during a Bluetooth session: the local host through HCI, the local LC (local operations), and the remote LM (link configuration, link information, and link management operations). The PDU is acknowledged at the Baseband level, but it is acted upon by the LM. The local LM usually resides on the Bluetooth module as a complete host-module implementation. The remote LM can be defined as the LM at the other end of the Bluetooth link. LM has also several commands for handling security issues.

SCO and eSCO links are used for transferring realtime two-way voice (see Section 2.1). They are established directly from the Baseband level, so overhead of upper layer protocols is not causing any delays for realtime two-way voice connections.L2CAP (Logical Link Control and Adaptation Protocol) is a software module that normally resides on the host. It fits upper layer protocols to the Baseband, i.e. it acts as a conduit for data on the ACL link between Baseband and host applications. L2CAP also offers CO (Connection-Oriented; from master to one slave and from slave to master) and CL (Connection-Less; from master to multiple slaves) services, and it is defined only for ACL links. Lower layer protocols do not have to know how layers above L2CAP work and vice versa. L2CAP can initiate security procedures when a CO or a CL channel connection attempt is made.

SDP (Service Discovery Protocol) is used to find the services of Bluetooth devices in the range. RFCOMM (Radio Frequency Communication) emulates serial ports over L2CAP, and therefore it is possible to use existing serial port applications via Bluetooth. OBEX (Object Exchange Protocol) [Inf03] is used to exchange objects, such as calendar notes, business cards and data files, between devices by using the client-server model.

TCS (Telephony Control protocol Specification) binary defines the call control signalling for the establishment/release of speech and data calls between Bluetooth devices. It also provides functionality for exchanging signalling information that is unrelated to ongoing calls. Many AT commands are also supported for transmitting control signals for telephony control.

BNEP (Bluetooth Network Encapsulation Protocol) is used to provide networking capabilities for Bluetooth devices. It allows that IP (Internet Protocol) packets can be carried in the payload of L2CAP packets. IP is a network layer protocol in the TCP/IP (Transmission Control Protocol / Internet Protocol) protocol suite. It contains both addressing information and some control information to enable routing of packets. TCP is one of the transport layer core protocols used in the TCP/IP protocol suite. It provides reliable transmission of data in IP network. UDP (User Datagram Protocol) is also one of the transport layer core protocols used in the TCP/IP protocol suite. It provides unreliable transmission of data in IP network, i.e. it does not provide reliability, flow-control, or error-recovery functions to IP. PPP (Point- to-Point Protocol) can also be used to provide TCP/IP networking capabilities for Bluetooth devices, but it is slower, i.e. it works over RFCOMM while BNEP works directly over L2CAP, and therefore it is rarely used anymore.

3. Bluetooth Security

This section provides Bluetooth specifications to illustrate their limitations and provide a foundation for some of the security recommendations A high-level example of the scope of the security for the Bluetooth radio path is depicted in Figure 3. In this example, Bluetooth security is provided only between the mobile phone and the laptop computer, while IEEE 802.11 security protects the wireless local area network link between the laptop and the IEEE 802.11 AP. However, the communications on the wired network are not protected by Bluetooth or IEEE 802.11 security capabilities. End-to-end security is not possible without using higher-layer security solutions in addition to the security features included in the Bluetooth specification and IEEE 802.11 standards.

The following are the three basic security services specified in the Bluetooth standard:

Authentication: verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.

Confidentiality: preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.

Authorization: allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

The three security services offered by Bluetooth and details about the modes of security are described below. Bluetooth does not address other security services such as audit and non-repudiation; if such services are needed, they must be provided through additional means.

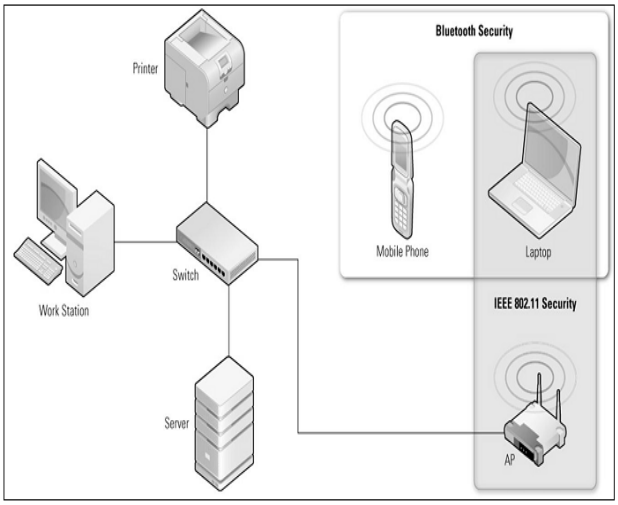


Figure 3 Bluetooth Air-Interface Security

3.1 Authentication

The Bluetooth device authentication procedure is in the form of a challenge-response scheme. Each device interacting in an authentication procedure is referred to as either the claimant or the verifier. The claimant is the device attempting to prove its identity, and the verifier is the device validating the identity of the claimant. The challenge-response protocol validates devices by verifying the knowledge of a secret key—the Bluetooth link key. The challenge-response verification scheme is depicted in
Figure 4.

The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant. The claimant uses the E_1 algorithm to compute an authentication response using his unique 48-bit Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E output are used for authentication purposes. The remaining 96 bits of the 128-bit output are known as the Authenticated Ciphering Offset (ACO) value, which will be used later to create the Bluetooth encryption key. The claimant returns the most significant 32 bits of the E_1 output as the computed response, SRES, to the verifier. The verifier compares the SRES from the claimant with the value that it computed. If the two 32-bit values are equal, the authentication is considered successful. If the two 32-bit values are not equal, the authentication has failed**.** Performing these steps once accomplishes one-way authentication. The Bluetooth standard allows both one-way and mutual authentication to be performed. For mutual authentication, the above process is repeated with the verifier and claimant switching roles.

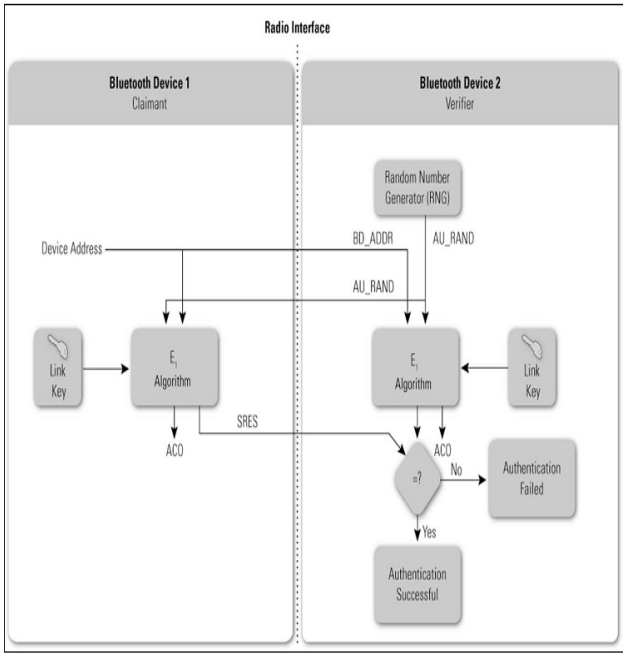


Figure 4 Bluetooth Authentication

3.2 Confidentiality

In addition to the Security Modes, Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:
Encryption Mode 1—No encryption is performed on any traffic.
Encryption Mode 2—Individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.
Encryption Mode 3—All traffic is encrypted using an encryption key based on the master link key.
Encryption Modes 2 and 3 use the same encryption mechanism.

4. DESCRIPTION OF SAFER+ ALGORITHM

The SAFER+ (Secure And Fast Encryption Routine) algorithm is based on the existing SAFER family of ciphers, which comprises the ciphers SAFER K-64, SAFER K-128, SAFER SK-128. All algorithms are byte-oriented block encryption algorithms, which are characterized by the following two properties. First, they use a non-orthodox linear transformation, which, is called Pseudo-Hadamard-Transformation (PHT) for the desired

diffusion, and second, they use additive constant factors (Bias vectors) in the scheduling for weak keys avoidance.

It consists of two main units: the encryption data path and the key-scheduling unit. The key-scheduling unit allows on-the-fly computation of the round keys. To reduce the silicon area, we used eight loops of a key scheduling single-round implementation. In the proposed design, round keys are applied in parallel in the encryption data path. The full Safer+ algorithm execution requires eight loops of the single round. We chose the single-round hardware implementation solution because, with this minimum silicon area, we could achieve the required throughput. The encryption data path's first component is an *input register*, which combines the *plaintext* and the *feedback data* produced in the previous round. The input register feeds the Safer+ single round

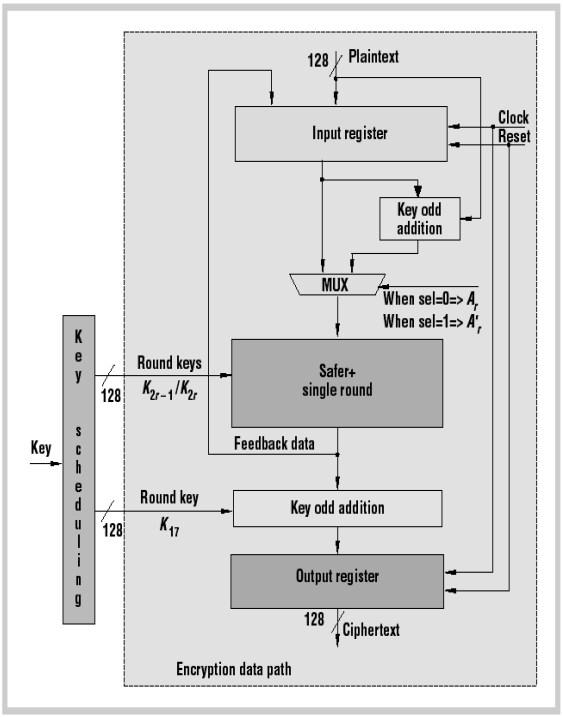


Figure.5 Safer + Implementation

.

4.1 SAFER + Single round

A Safer+ single round has four subunits:

- The mixed XOR/addition subunit, which combines data with the appropriate round sub key *K*2*r*–1.
- The non-linear layer (use of the non-linear functions *e* and *l*). The *e* function is implemented as $y = 45^x$ in GF(257), except that 45128 = 0. The *l* function is implemented as $y = \log45(x)$ in GF(257), except that log45(0) = 128.
- The mixed addition/XOR subunit, which combines data with the round sub key *K*2*r*
- The four linear Pseudo-Hadamard Transformation layers, connected through an "Armenian Shuffle" permutation.

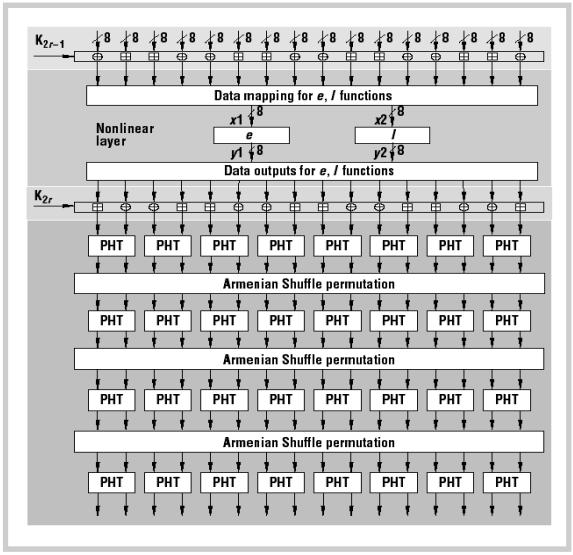


Figure 6. SAFER single round

The implementation of the non-linear layer using a *data-mapping* component that produces the X1 and X2 bytes is done. These bytes are the input of the non-linear functions *e* and *l*. During one round, we execute *e* and *l* eight times. This design significantly reduces the required silicon area. Each function is implemented using 256 bytes of ROM. After the SAFER+ single round in the encryption data path is a mixed XOR/addition (or *key odd addition*) component.

4.2 PHT Implementation

The design of PHT element is shown in Fig.5: The PHT Implementation Multiplication by 2 can be achieved by one bit left wired shift.

Out1=2 in1+in2

(1)

Out2=in1+in2 (2)

the four linear PHT layers connected through the permutations. The permutation boxes show how input byte indices are mapped into the output byte indices. Thus, position 0 (leftmost) is mapped on position 8; position 1 is mapped on position 11, etc.

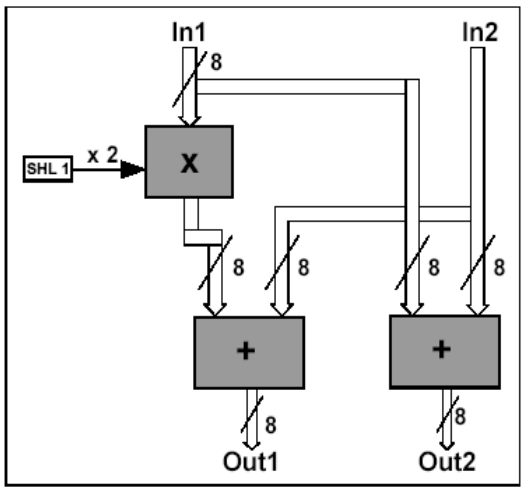


Figure.7 PHT Implementation

5. Simulation Results for SAFER+ Algorithm

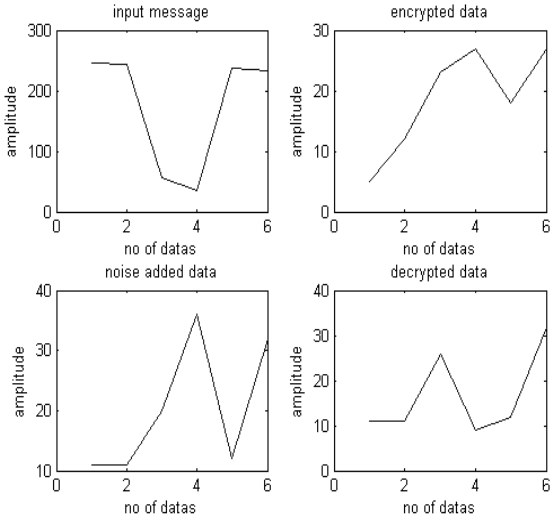


Figure 8 Matlab Simulation

Figure 8 shows the matlab simulation for the SAFER+ algorithm. Whenever noise is added to the encrypted data, the data get corrupted and the original data cannot be retrieved. This shows that Bluetooth attack is possible for the SAFER+ algorithm.

6. Triple DES Algorithm

Triple DES is based on the DES algorithm; it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. To this end the National Institute of Standards

and Technology (NIST), the Advanced Encryption Standard (AES) as a replacement for DES. The procedure for encryption is exactly the same as regular DES, but it is

Figure 9 Architecture of TDES

repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key.

6.1 Modes of operation

6.1.1 Triple ECB (Electronic Code Book)

This variant of Triple DES works exactly the same way as the ECB mode of DES. This is the most commonly used mode of operation.

6.1.2 Triple CBC (Cipher Block Chaining)

This method is very similar to the standard DES CBC mode. As with Triple ECB, the effective key length is 168 bits and keys are used in the same manner, as described above, but the chaining features of CBC mode are also employed.

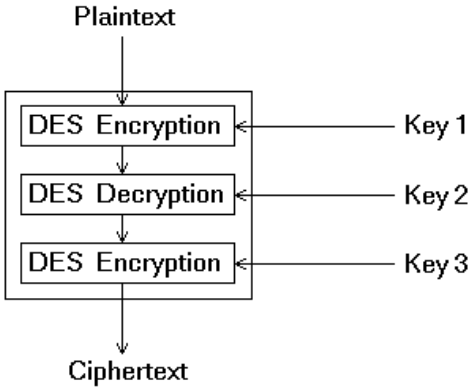
The first 64-bit key acts as the Initialization Vector to DES. 34Triple ECB is then executed for a single 64-bit block of plaintext. The resulting ciphertext is then XORed with the next plaintext block to be encrypted, and the procedure is repeated. This method adds an extra layer of security to Triple DES and is therefore more secure than Triple ECB, although it is not used as widely as Triple ECB.

The most widely used conventional encryption algorithms: the Data Encryption Standard (DES). Although numerous conventional encryption algorithm have been developed since the introduction of DES, it remains the most important such algorithm. Further, the detail study of DES provides an understanding of the principles used in other conventional encryption algorithms.

6.2 Simplified DES

The simplified DES(S-DES) encryption algorithm takes an 8-bit block of plain text and 10-bit key as input and produces an 8-bit block of cipher-text as output. The S-DES algorithm takes an 8-bit block of cipher text and the

same 10-bit key used to produce that cipher text as input and produces the original 8-bit block of plain text.



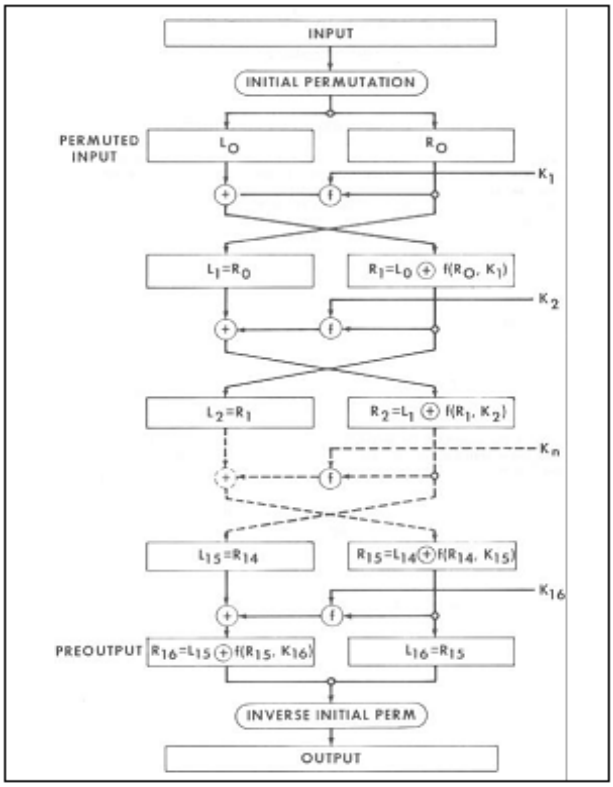


Figure 10 Enciphering computation

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key . Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1} . The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described.

Enciphering

A sketch of the enciphering computation is given in Figure 10. The 64 bits of the input block to be enciphered are first subjected to the following permutation, called the initial permutation IP:

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

That is the permuted input has bit 58 of the input as its first bit, bit 50 as its second bit, and so on with bit 7 as its last bit. The permuted input block is then the input to a complex key-dependent computation described below. The output of that computation, called the preoutput, is then subjected to the following permutation which is the inverse of the initial permutation:

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

That is, the output of the algorithm has bit 40 of the preoutput block as its first bit, bit 8 as its second bit, and so on, until bit 25 of the preoutput block is the last bit of the output.

Let the 64 bits of the input block to an iteration consist of a 32 bit block L followed by a 32 bit block R. Using the notation defined in the introduction, the input block is then LR. Let K be a block of 48 bits chosen from the 64-bit key. Then the output L'R' of an iteration with input LR is defined by:

L'= R (1)

R' = L f(R,K)

Where denotes bit-by-bit addition modulo 2.

As remarked before, the input of the first iteration of the calculation is the permuted input block. If L'R' is the output of the 16th iteration then R'L' is the preoutput block. At each iteration a different block K of key bits is chosen from the 64-bit key designated by KEY.

Deciphering

The permutation IP applied to the preoutput block is the inverse of the initial permutation IP applied to the input. Further, from (1) it follows that:

R = L'

L=R' f (L', K) (2)

Figure 11 shows the simulation result of the Triple DES algorithm. When the noise is added to the encrypted data, the data did not affected and the original data are retrieved. Hence the Triple DES has better security than the SAFER+ algorithm.

7. Simulation Result for Triple DES Algorithm

Figure 11 shows the matlab simulation for the triple DES algorithm. Whenever noise is added to the encrypted data, the data was not corrupted and the original data can be retrieved. This shows that Bluetooth attack is not possible for the triple DES algorithm.

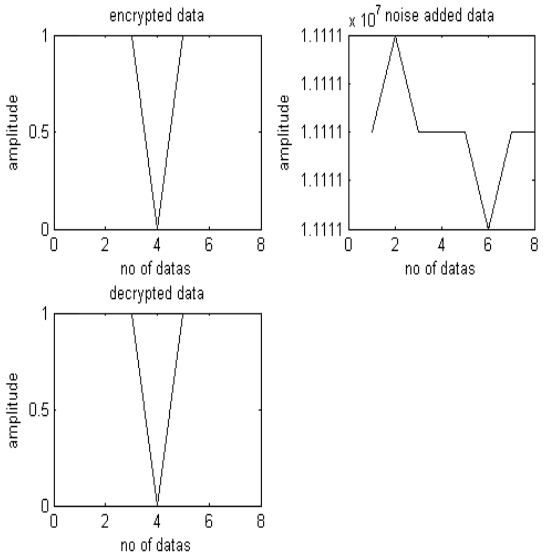


Figure 11 Matlab simulation

8. Conclusion

In this paper, comparison of the SAFER+ encryption algorithm and Triple DES algorithm for Bluetooth security systems are presented. The whole design was captured entirely in matlab. The efficiency of the algorithm was evaluated by the addition of noise to the encrypted data and the output was seen to be obtained without any incorrectness which justifies the level of security. On comparison, Triple DES algorithm proved to be better for implementation in Bluetooth devices than the SAFER+ algorithm.

9. References

[1] Paraskevas kitos, Nicolas sklavos, Kyriakos Papadomanolakis and Odysseas Koufopavlou university of patras, Greece," Hardware Implementation of Bluetooth Security" *IEEE CS and IEEE Communications Society* - January to March 2003. pp. 21 to 29.

[2] N. Sklavos et al., "Random Number Generator Architecture and VLSI Implementation," *Proc. IEEE Int'l Symp. Circuits&Systems* (ISCAS 02), IEEE Circuits and Systems Soc. Press, Piscataway, N.J., 2002, pp.854–857.

[3] J.L. Massey and R. Rueppel, "LinearCiphers and Random Sequence Generators with Multiple Clocks," *Advances in Cryptology:Proc. Eurocrypt 84*, Lecture Notes in Computer Science, vol. 209, Springer- Verlag, Berlin, 1984, pp. 74–87.

[4] P. Chandrakasan, S. Sheng, and R.W.Brodersen, "Low Power CMOS DigitalDesign," *IEEE J. Solid-State Circuits*, vol.27, no. 4, Apr. 1992, pp. 473–484

[5] J. L. Massey, "On the Optimality of SAFER+ Diffusion", *Second Advanced Encryption Standard Candidate Conference (AES2)*, Rome, Italy, March 22-23 online available at

http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm.

[6]AlfonsoDeGregorio. Cryptographic Key ReliableLifetimes: Bounding the Risk of Key Exposure in the Presence of Faults. In Fault Diagnosis and Tolerance in Cryptography, volume 4236 of LNCS, pages 144–158. Springer, 2006.

[7] ARC Electronics (n.d.). DSSS and FHSS - Spread Spectrum modem. Retrieved March 24, 2004 from, Web site:http://www.arcelect.com/DSSS_FHSS-spead_spectrum.htm

[8] Bhagwat, P. (2000, July 31). Bluetooth Technology Overview. Retrieved March 24, 2004 from AT&T Labs, Networking Research Group Web site: http://www.ietf.org/proceedings/00jul/SLIDES/ipobt-tech/sld001.htm

[9] Vainio, J. (2000, May 25). Bluetooth Security. Retrieved March 24, 2004 from Helsinki University of Technology, Department of Computer Science and Engineering Web site: *http://www.niksula.cs.hut.fi/~jiitv/bluesec.html#chap2.1*

[10] Hall, J. (20003, August 21). Brush up on Bluetooth. Retrieved March 24, 2004 from, SANS Web site: *http://www.sans.org/rr/papers/68/1222.pdf*

[11] Gehrmann, C. (2002, April 4). Bluetooth Security Whitepaper. Retrieved March 24, 2004 from , Bluetooth SIG Security Expert Group Web site: http://www.bluetooth.com/upload/24Security_Paper.PDF

[12] Karygiannis, T. & Owens, L. (n.d.). Wireless Network Security 802.11, Bluetooth™ and Handheld Devices. Retrieved March 24, 2004 from, National Institute of Standards Technology Web site: http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf

[13] Tim Grembowski, Roar Lien, Kris Gaj, Nghi Nguyen, Peter Bellows, Jaroslav Flidr, Tom Lehman, and Brian Schott, "Comparative analysis of the hardware implementations of hash functions SHA-1 and SHA-512", Proceedings of fifth International Conference on Information Security (ISC 2002), LNCS, Vol. 2433, Springer-Verlag, Sao Paulo, Brazil, September 30-October 2, 2002.

[14] Diez J. M., Bojanic S., Stanimirovic Lj., Carreras C., Nieto-Taladriz O., "Hash algorithm for cryptographic protocols: FPGA implementation", Telecommunications forum (TELFOR 2002), Proceedings of 10 November 26-28, Belgrade, Yugoslavia, 2002.

[15] Infrared Data Association: IrDA specifications. Infrared Data Association, technical specifications, 1993-2005. http://www.irda.org (4.11.2005)

[16] NIST: Advanced Encryption Standard (AES) The Federal Information Processing Standards Publication 197. NIST, November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (20.9.2006)

[17] NIST: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. NIST, May 2004. http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf (19.9.2006)

[18] NIST: Data Encryption Standard (DES) The Federal Information Processing Standards Publication 46-3. NIST, October 1999. *http://www.cerberussystems*.com/INFOSEC/stds/fip46-3.htm (19.9.2006)

[19] Whitehouse O.: RedFang, Bluetooth Discovery Tool. SecuriTeam, homepage, 2003.http://www.securiteam.com/tools/5JP0I1FAAE.html (2.11.2005)

[20] A. Laurie and B.Laurie. serious flaws in blue tooth security lead to disclosure of personal data. *http://bluestumbler.com*.

[21] Brent A.Miller And Chatschik Bisdikian "Bluetooth revealed" – low price edition

[22] Network security (second edition) by Kaufman-Perlman-Speciner

[23] The 10th ACM conference on computer and communications security, Washington, dc, USA, October-27-31, 2003.

[24] Stallings W.: Cryptography and Network Security Principles and Prac 3rd Edition, Upper Saddle River, New Jersey, Prentice Hall, 2003.

[25] Jennifer Bray and Charles F Sturman," Bluetooth" –Low price edition.

[26] *http://www.bluetooth.com*

[27] *http://www.ericsson.com/3g/*

D.Sharmila is presently working as Associate Professor, Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam. She received B.E.(ECE) and M.E. (Applied Electronics) from Kongu Engineering College, Perundurai. She is now pursuing Phd in Wireless Security. She has 12.5 years of teaching experience and has guided several UG and PG projects. She is a life member of ISTE and Associate member of IE. Her area of interests are Wireless Security, Low power VLSI, Adhoc networks. She has published 6 research papers in International Conferences and 18 papers in National Conferences

Dr.R. Neelaveni is presently working as a Assistant Professor, Department of EEE, PSG College of Technology, Coimbatore. She has a Bachelor's degree in ECE, a Master's degree in Applied Electronics and PhD in Biomedical Instrumentation. She has 19 years of teaching experience and has guided many UG and PG projects. Her research and teaching interests includes Applied Electronics, Analog VLSI, Computer Networks, and Biomedical Engineering. She is a Life member of Indian Society for Technical Education (ISTE).She has published several research papers in national Journals and Conferences.