An Integrated Scheme based on Triple DES, RSA and MD5 to Enhance the Security in Bluetooth Communication

Trishna Panse
Department of Information Technology
Institute of Engineering & Technology,
DAVV, Indore, India

V. Kapoor
Department of Information Technology
Institute of Engineering & Technology,
DAVV, Indore, India

ABSTRACT

Data security is an important issue in data transmission through any type of network whether it is LAN, WAN, MAN or PAN. We are concentrating on PAN that is personal area network. Bluetooth is an example of this type of network. To provide the security in Bluetooth communication currently used encryption algorithm is a 128 bit symmetric stream cipher but symmetric cipher may be broken under certain condition. Another popularly used encryption algorithm for Bluetooth security are Data Encryption Standard (DES) and Ron Rivest, Adi Shamir and leonard adleman (RSA) Algorithm. However DES is vulnerable to possible attacks. To overcome these limitations and increase the security in Bluetooth communication here we propose an integrated cryptographic scheme. This scheme is based on Triple DES, RSA and MD5.Triple DES algorithm (variant of DES) is used for encryption, which is more secure in comparison to DES. RSA is used to encrypt the key of triple DES. Message digest Algorithm MD5 is adopted in this mechanism to verify the integrity of the message. Three major security principles such as authentication, confidentiality and integrity are achieved together using this scheme.

General Terms

Bluetooth security, Encryption, Authentication, Data transmission.

Keywords

Bit Discarding process, MD5, RSA, Triple DES, BDP, Integrity Verifier.

1. INTRODUCTION

Bluetooth is a type of wireless adhoc network. It is also known as Personal area network with IEEE 802.15 standard. Bluetooth technology has many features like low cost, low complexity, low power consumption, adhoc in nature. The amount of data to be transmitted is Bluetooth version dependent. Whenever we talk about data transmission through any type of network whether it is LAN, WAN, MAN or PAN the important aspect is how we provide confidentiality in transmitted data. The encryption algorithm that is currently used in Bluetooth is the E0 stream cipher [1]. Although Bluetooth have their own security mechanism but still there are serious security risks because it is more vulnerable to security threats as compare to infrastructure based system. Data leaking is one of the major security risk associated with Bluetooth transmission.

2. RELATED RESEARCH WORK

2.1 Wuling Ren, Zhejiang Gongshang, 2010[1] proposed the solution to the short comings; 128-bit E0 stream ciphers in some cases can be cracked, Low credibility of PIN, High probability of non-link key cheat, Address Spoofing present in existing security system of Bluetooth. They proposed a hybrid system based on DES and RSA. DES is a symmetric key cryptographic algorithm and RSA is an asymmetric key cryptographic algorithm. In which public and private key pair is used. Here DES use symmetric key and the size of the key is 56-bit only that is more vulnerable to attacks like brute force attack, man-in-middle attack etc.

2.2 Li juan Chen Bin, Li Kun, 2009[3] proposed the solution to the limitations of the E0 stream cipher that is used in Bluetooth System, the proposed system uses DES algorithm. The problem with this approach is distribution of encryption key used in DES. In which both communication parties agree on one shared secret key that is known as symmetric key. But the problem arises that how one party exchange this secret key with other party because it is possible that opponent can intercept the key during transmission of symmetric key. The another problem is again the small size of the key that is highly vulnerable to brute force attack.

2.3 Dave Singel'ee, Bart Preneel, 2004[4] published an article that gives an overview of key agreement protocols used in Bluetooth communication security and weakness of Bluetooth transmission. This paper gives an outline about generation of keys that are used to implement security in Bluetooth communication like encryption key generation, link key generation, unit key generation, initialization key generation and combination key generation. This paper also describes mutual authentication process. See also [7].

2.4 Markus Jakobsson and Susanne Vitzel [5] they give an article that explains three major security vulnerabilities in Bluetooth standard. These are eavesdropping and impersonation of key that is exchanged by two victim devices. Man–in-middle attack is also possible on the keys. Second vulnerability is location attack in which the geographical location of victim device can be identified by attacker. The third vulnerability is attack on cipher that means it shows how an attacker can break the security in cipher that means attacker can guess the content of registers. Also show another attack with time and memory complexity. This article also gives details of Bluetooth specification that includes device modes, addressing and specify how initialization and link keys can be established.

2.5 Jun-Zhao,Douglas Howie, Antti and Jaakko Sauvola[6] They gives an article about the security issues of Bluetooth standard and introduced security frame work which includes both link level and service level security schemes. At link level key management, authentication and encryption schemes are defined. Flexible security architecture is implemented at service level security. In the security frame work security modes can be defined for each Bluetooth device. This article gives an analysis of potential risks, attacks against the vulnerabilities like DOS, man-in–middle attack[2], spoofing, session hijacking, eavesdropping etc. and proposed countermeasures to improve Bluetooth security. See also [8,9].

3. PROPOSED SYSTEM

To increase the security level this proposed scheme overcomes the limitation of "Hybrid encryption algorithm proposed by Wuling Ren et. al" (mentioned in section 2.1) [1]. The proposed enhanced scheme includes Triple DES, RSA and MD5.Triple DES (Variant of DES) strengthens the security of Bluetooth transmission. Reason behind for selecting triple DES rather than Double DES is that in double DES algorithm the key used for encryption and decryption is suspected to meet-in-middle attack. RSA is used to solve the key distribution problem and in addition to this, MD5 to verify the integrity of the message. Use of message digest algorithm in combination of cryptographic algorithm provides strength in security of data transmitted by Bluetooth. Here we specify different modules of envision system.

3.1 Key Generation Module

This module includes MD5 algorithm and Bit discarding process.

3.1.1 MD5 algorithm

It is a message digest algorithm. Message-Digest refers to hash transformation or the fingerprint of the message. Plaintext gives as input to the MD5 algorithm and gets the message digest of 128-bit.

3.1.2 Bit discarding process (BDP)

The output of MD5 is send to the bit discarding process. In this process every 8th bit of MD5 output is discarded and get the 112-bit which is called as MD'. This MD' is use as the encryption key in triple DES for data encryption.

3.2 Data Encryption using Triple DES

The triple DES Algorithm with 2-keys is a symmetric, group cipher algorithm. It operates on 64-bit plaintext blocks and uses 112-bit keys (2*56), what makes it practically immune to brute force attacks and man-in-middle attack that are possible in DES and double DES. It can be denoted in the form of equation as shown below[2]

$$C = E_{K1}\left(D_{K2}\left(E_{K1}(P)\right)\right)$$

The plain text is encrypted using triple DES with the help of MD' as symmetric key that is achieved from proposed bit discarding process and produce the cipher text CT.

3.3 Key Encryption using RSA

RSA algorithm is the public key cryptographic algorithm. It can be used for data encryption, also can be used for digital signature algorithms. In Public key algorithm public-private key pair is used for encryption & decryption.

3.4 Integrity Verifier Module

This module performs the integrity verification of the received message. Checking of integrity is the important security service. In Integrated Encryption Scheme sender is A, the receiver is B. A's public key is AP, and Secret key is AS, B,s public key is BP and Secret key is BS.(We assuming that the two sides of communication know each RSA public key AP and BP). RSA algorithm overcomes difficulty of key distribution/agreement.112 Bit MD' is encrypted by RSA Algorithm with receiver Public key BPK and produce Cipher Text of Key (CK) as shown in figure 1.

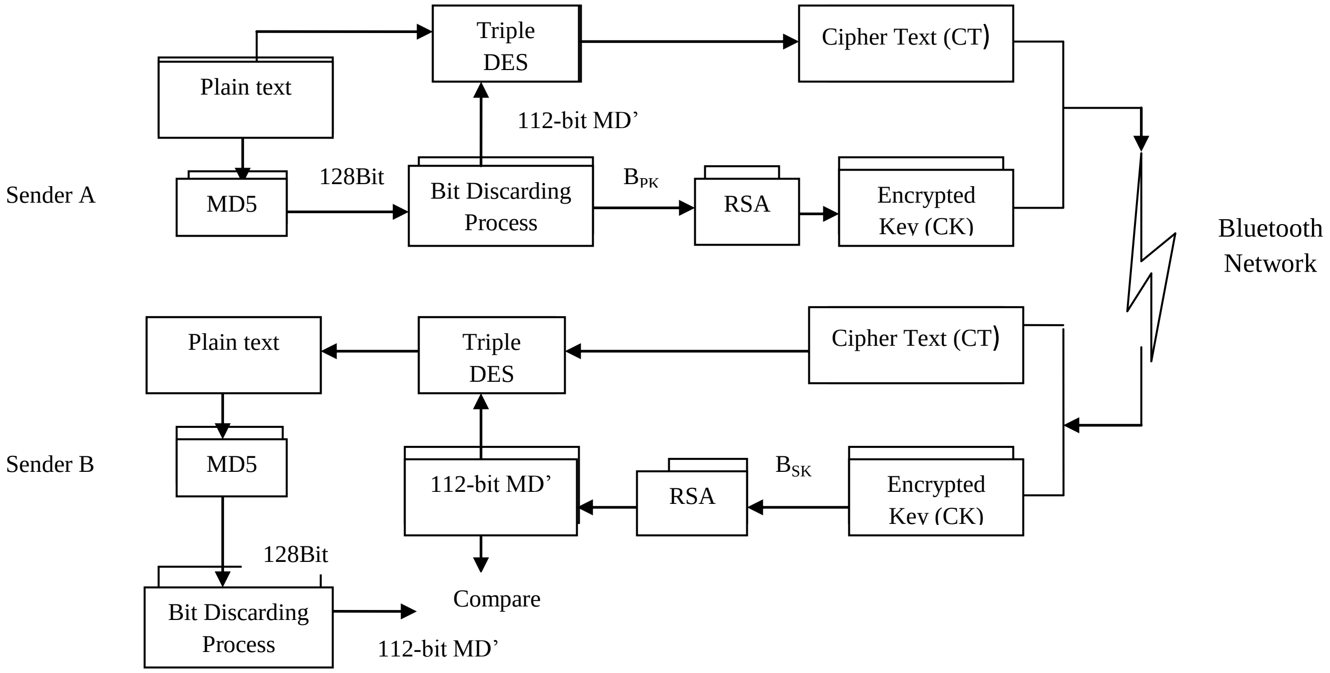

Figure 1: Proposed Hybrid Scheme

4. RESEARCH METHODOLOGY

This research methodology includes following processes.

4.1 Encryption Process

1. MD5 algorithm computes 128 Bit MD5.
2. Reduce 128-bit message digest to 112 bits by discarding every number that is a multiple of 8-bit used for parity. This output is called as MD'.
3. Triple DES algorithm encrypts the Original Message (M) with help of MD' as symmetric key used in triple DES, and then produce a cipher text (CT).
4. The MD' Encrypted by RSA Algorithm with receiver Public key BPK and produce Cipher Text of Key(CK).
5. Combine a Cipher Text (CT) and Cipher text of Key (CK), produces a Complex Message (CM).Complex Message (CM) is sent to the Receiver B.

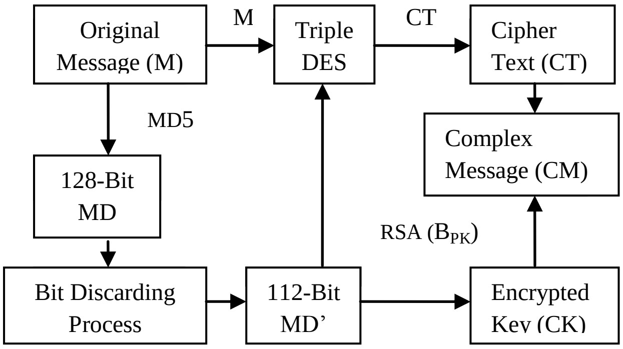

Figure 2: Encryption Process

A) Sender Side Encryption Algorithm

1. Take Text Message M as input
2. *compute MD*
   $MD5(M) = MD$
3. $BDP(MD) = MD'$
4. $MD' = K$
5. $E_K(M) = CT$
   $CT = E_{K1}\left(D_{K2}\left(E_{K1}(M)\right)\right)$
6. Go to Step 4
7. Encrypt Key K with RSA
   $E_{BPK}(K) = CK$
8. $CK + CT = CM$
9. Send CM to Receiver

4.2 Decryption Process

1. The receiver B received cipher text CT into two parts, one is cipher text of key CK from the RSA algorithm encryption, and the other is cipher text CT from the triple DES algorithm encryption.
2. The receiver B decrypts cipher text of key CK by their own private key BSK, and retrieve the key K, then decrypt the cipher text CT to the original M by key K that is MD'.

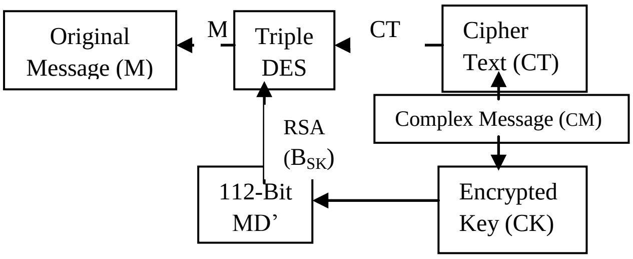

Figure 3: Decryption Process

B) Receiver Side Decryption Algorithm

1. *Receive CM*
2. $D_{BSK}(CK) = K = MD'$
3. $D_K(CT) = M$
   $D_{K1}\left(E_{K2}\left(D_{K1}(CT)\right)\right) = M$

4.3 Verification Process

1. Calculate MD5 of Original Message (M).
2. 128-Bit message digest is converted into MD' using Bit discarding process.
3. Cipher Text of Key (CK) decrypts by RSA Algorithm with help of Receiver Secrete Key BSK and produce a key and it's also a MD'.
4. Compare both MD'.

A) Integrity Verification Algorithm

1. $MD5(M) = MD$
2. $BDP(MD) = K = MD'$
3. Compare step 2 and decrypted key from decryption algorithm i.e. both MD'
4. If found equal
5. then accept
   Else:
   reject message

To implement this methodology we have used various security classes like cipher class, key generator class etc.of JAVA programming language. In implementation we have used start time variable before encryption process and end time variable after encryption process has been completed to calculate time taken by encryption process of a particular plain text file.

5. EMPIRICAL RESULTS

We apply our methodology to various size of sample plain text file which the sender wants to transmit through Bluetooth technology and set up the experimental results such as size of text file to be encrypt, size of cipher text file (output file) and time taken by plain text file in encryption. Table1 provided encryption time for various size of plain text file. In order to measure the effect of change in plain text files in getting the encryption time. We analyzed that as the size of text file increased the encryption time had also increased.

Table 1. Plain Text file size with Encryption Time

File Name	Plain Text (In Kilobyte)	Encryption Time (In Seconds)
Data Set 1	0.685	1.516
Data Set 2	3.52	1.875
Data Set 3	22	2.156
Data Set 4	40.1	2.867
Data Set 5	80.3	4.86
Data Set 6	121	9.11
Data Set 7	175	20.515
Data Set 8	256	38.062
Data Set 9	465	82.438
Data Set 10	732	288.157

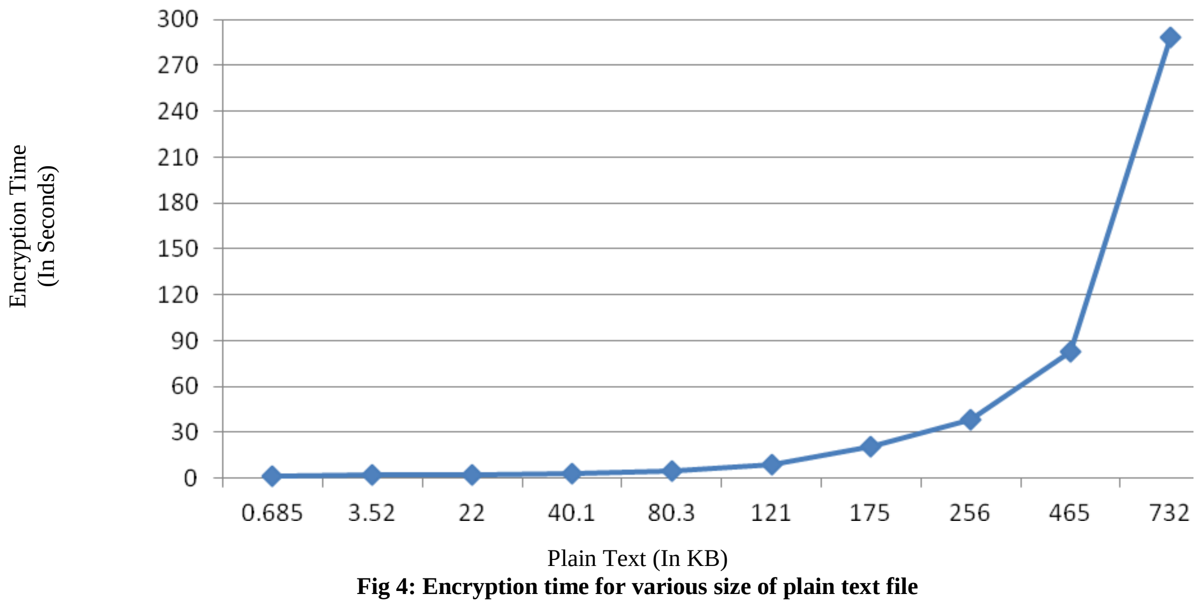

Fig 4: Encryption time for various size of plain text file

At the certain level the time of encryption would grow exponentially because of increasing in plain text as shown in fig 4. Table 2 provided time taken by various sizes of plain text file and size of corresponding cipher text. Our analysis has shown that integration of both symmetric and asymmetric key cryptography produce output like cipher text size is small or compact as compare to plain text size. This is the advantage of using both the techniques together, which we have achieved from experimental results. We analyzed that as the file size of plain text is small the size of cipher text is approximately equal up to some extend and when the file size is greater than 100 KB the size of cipher text is decreased a lot.

Table 2. Performance analysis of Plain Text size and corresponding Cipher Text size with Encryption time

File Name	Plain Text (In KB)	Encryption Time (In Seconds)	Cipher Text (In KB)
Data Set 1	3.52	1.875	3.47
Data Set 2	22	2.156	21.1
Data Set 3	40.1	2.867	40.1
Data Set 4	80.3	4.86	80.3
Data Set 5	121	9.11	120
Data Set 6	175	20.515	118
Data Set 7	256	38.062	115
Data Set 8	465	82.438	155
Data Set 9	732	288.157	121
Data Set 10	1045	492.719	193

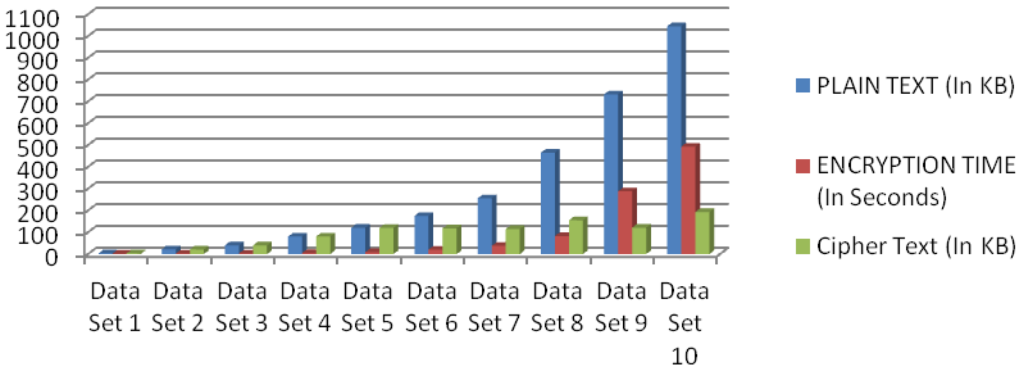

Fig 5: Analysis of plain text size and cipher text size with Encryption time

9. COMPARISON OF BLUETOOTH SECURITY SYSTEMS

This Section gives a comparison of different Bluetooth security systems in terms of keys and suggests countermeasures against disadvantages of security system.

Table 1. Comparison of Various Security Systems

Bluetooth Security System	Security Mechanism	Types and Size of key	Advantage	Limitations	Countermeasure
Existing System[8,9]	-E0 stream cipher -challenge response technique	Link Key,128-bit [1,10]	Low complexity due to absence of cryptographic technique	-.Low credibility of PIN -Address spoofing -Non-link key cheat because same key is used for different parties[1]	-Increase the PIN code length.[6] -Need user authentication and application level security -Use some other advanced scheme in place of cipher[6].
System proposed by- **Li juan Chen Bin, Li Kun[3]**	Use single DES algorithm	Symmetric Key, 56-bit	Fast Encryption /Decryption[2]	-Key distribution problem -More Vulnerable to attack because of small key size	-Use asymmetric cryptographic algorithm -Use Public and Private key pair.
System proposed by- **Wuling Ren, Zhejiang Gongshang[1]**	Use DES and RSA algorithm	Symmetric and Asymmetric key, 56-bit Symmetric key	Key distribution Problem solved	- Brute force attack is possible on small key size(56-bit only) - No any process proposed for verifying the integrity of message	-Increase the size of the key like 112 bit and 168 bit key. -Proposed a system that include integrity check also.
Proposed system	Use Triple DES (with 2-keys), RSA, MD5	Symmetric and Asymmetric key, 112-bit Symmetric key	-Key distribution problem solved -Brute force attack problem is somehow solved because key size is increased	Only text file is encrypted.	-use some advanced technique for encryption of file other than text for example PDF file, Image file etc.

10. CONCLUSION AND FUTURE WORK

Since data transmission through Bluetooth is largely used now days, it is rarely focused on the issue of integrity and confidentiality of received data. Our main objective in this paper is to demonstrate how data can be encrypted and integrity of data can be verified. This scheme is particularly applied in Bluetooth data transmission. This scheme provides integration of Triple DES, RSA and MD5 together to achieve the high level of data security in Bluetooth transmission.

Starting with the concept proposed by Wuling Ren, Zhiqian Miao[1] which is the integration of most popular cryptographic algorithm. We introduce an idea of integrity verification of data received by receiver. In addition to this the proposed system uses triple DES algorithm instead of DES algorithm to provide higher security because the key size in this algorithm is relatively large so it is difficult for attacker to break the key. By applying cryptographic algorithm such as triple DES, RSA and MD5 together, we succeed in secure data transmission through Bluetooth communication and generating the encrypted text called as cipher text and decrypting the cipher text to get the same plain text sent by sender.

Our result shows time taken by different size of plain text file in encryption process. The output of this encryption process is stored as cipher text in a text file. The key used in Triple DES algorithm is also stored in an encrypted format. We have analyzed the experimental data from large number of tests carried out, we examined that as the file size of plain text is greater than 100KB corresponding cipher text is decreased a lot and as we know that the property of combination of both type of cryptographic algorithm is that the size of cipher text is compact in comparison to plain text size. The results shown in section 8 Table 2 proved that this property is achieved by this proposed system, but it is possible that the conclusions are cautious. This proposed work would be inspiring for advance research such as secure Bluetooth transmission of PDF file, video file, image file, etc. with watermarking technique; this may perhaps our future research topic.

11. REFERENCES

[1] Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering, Zhejiang Gongshang University, "*A Hybrid Encryption Algorithm Based on DES and RSA" in Bluetooth Communication* Second International Conference on Modeling, Simulation and Visualization Methods, 2010.

[2] Atul Kahate,Cryptography and Network Security Second Edition.

[3] Li Juan, Chen Bin, Li Kun, Electronic Engineering College, Naval University of Engineering Wuhan, China, "Study on the Improvement of Encryption Algorithm of Bluetooth", 2009 International Conference on Networking and Digital Society.

[4] Dave Singel'ee, Bart Preneel, "Security Overview of Bluetooth", COSIC Internal Report June 2004.

[5] Markus Jakobsson and Susanne Vitzel, Lucent Technologies – Bell Labs, Information Science Research Center, Murray Hill, USA , "Security Weakness in Bluetooth".

[6] Jun-Zhao Sun, Douglas Howie, Antti Koivisto and Jaakko Sauvola, Media Team, Machine Vision and Media Processing unit, InfoTech Oulu, University of Oulu, Finland, "Design Implementation and Evaluation of Bluetooth Security".

[7] Trishna Panse, Vivek Kapoor, Prashant Panse, "A Review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission" International Journal of Information and Communication Technology Research, Volume 2 Number 3, March 2012. Available online: http://www.esjournals.org

[8] Trishna Panse, Vivek Kapoor, "A Review paper on Architechture and Security system of Bluetooth Transmission" International Journal of Advanced Research in Computer Science, Volume 3, No. 1, Jan-Feb 2012. Available online: www.ijarcs.info

[9] Trishna Panse, Vivek Kapoor, "A Review on Security Mechanism of Bluetooth Communication", International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012.

[10] Paraskevas Kitsos, Nicolas Sklavos,Kyriakos Papadomanolakis, and Odysseas Koufopavlou, "Hardware Implementation of Bluetooth Security",*University of Patras, Greece.*