ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A Study of Wireless Communication Using Multiple Algorithm

R.Karthikeyan[1] K.G.S.Venkatesan[2]

[1]Asst. Professor Dept of CSE, Bharath University, Chennai, Tamil Nadu, India

[2]Asst. Professor Dept of CSE, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: Information security is an imperative issue in information transmission through any sort of system. In our task we proposed a coordinated cross breed encryption calculation in remote eg.zigbee correspondence to improve the information security. This plan is in view of Triple DES, RSA and MD5.Triple DES calculation (variation of DES) is utilized for encryption, which is more secure in correlation to DES. RSA is utilized to scramble the key of triple DES. Message digest Algorithm MD5 is received in this component to check the trustworthiness of the message. Three noteworthy security standards, for example, verification, secrecy and trustworthiness are accomplished together utilizing this plan.

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

I. INTRODUCTION

Zigbee is a specification for a suite of high level communication protocols using small, low-power digital radios based on an IEEE 802 standard for personal area networks. Zigbee devices are often used in mesh network form to transmit data over longer distances, passing data through intermediate devices to reach more distant ones[1]. 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. Wireless networks are generally susceptible to attacks and security is clearly very important. Although zigbee 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[2,].

Zigbee is a very low-cost, very low-power-consumption; two way wireless communication standard hat is being developed by the Zigbee Alliance, an independent nonprofit organization. Zigbee is targeted at radio frequency (RF) applications that require low data rate, long battery life, and secure networking. Zigbee has a very wide application area that covers consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games, etc.

II. PROPOSED SYSTEM

To increase the security level this proposed scheme overcomes the limitation of "Hybrid encryption algorithm proposed. The proposed enhanced scheme includes Triple DES, RSA and MD5.Triple DES (Variant of DES) strengthens the security of zigbee 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[3]. Use of message digest algorithm in combination of cryptographic algorithm provides strength in security of data transmitted by zigbee. Here we specify different modules of envision system.

III. PROCESSING STEP OF HEA

A)Key Generation Module

This module includes MD5 algorithm and Bit discarding process. *B. MD5 algorithm*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

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.

B)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'[4]. This MD' is use as the encryption key in triple DES for data encryption.

C) 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)[5], 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
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[6].

D) 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[2]. In Public key algorithm public-private key pair is used for encryption & decryption.

E) Integrity Verifier Module
This module performs the integrity verification of the received message. Checking of integrity is the important security service[3]. 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[5].A.Bit MD' is encrypted by RSA Algorithm with receiver Public key BPK and produce Cipher Text of Key (CK) shown in figure .1

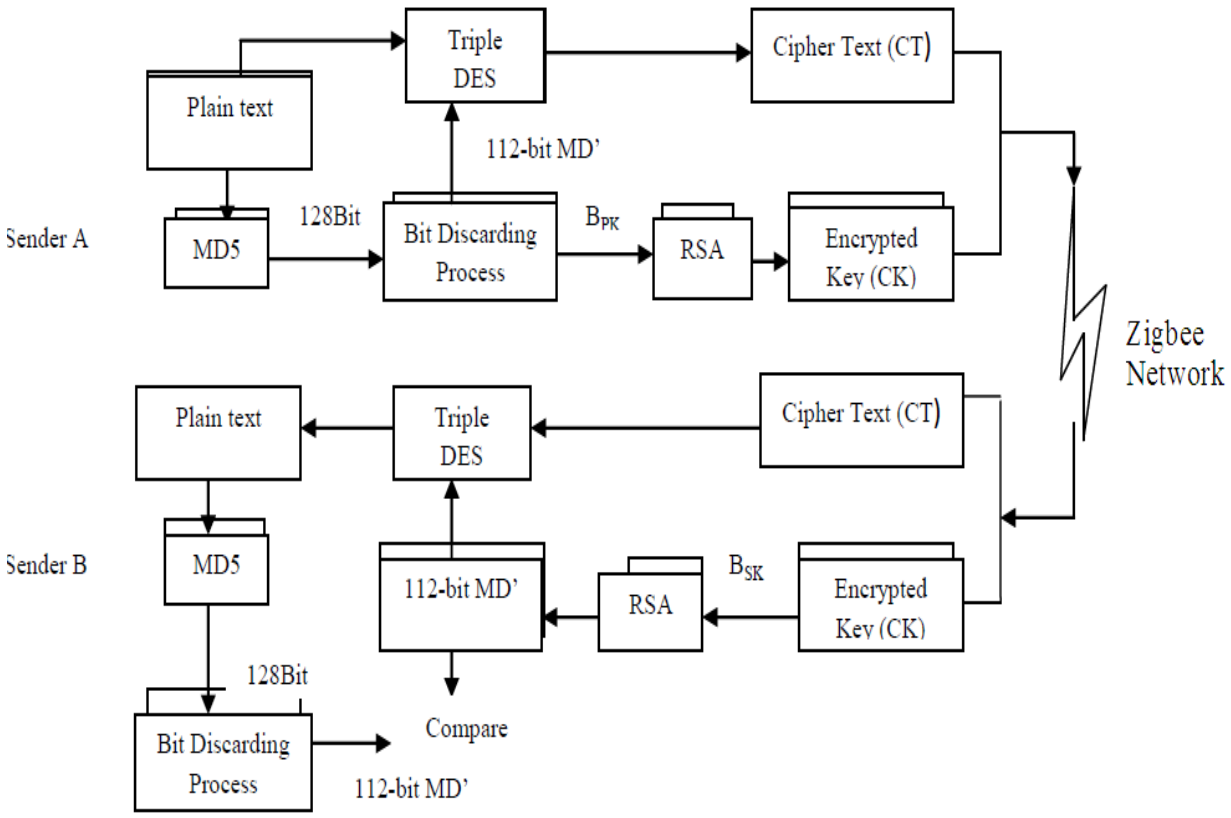

FIGURE.1 Proposed hybrid scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

IV. 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.

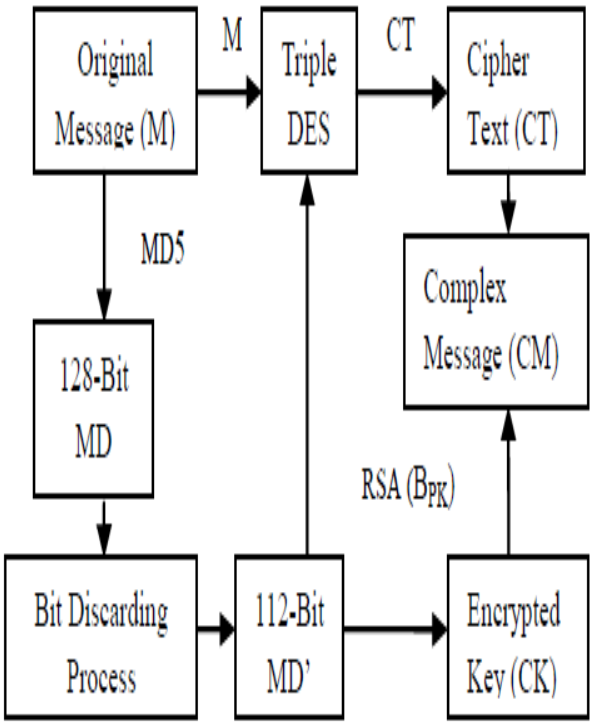

Figure 2: Encryption Process

SENDER SIDE ENCRYPTION ALGARITHM

1. Take text message M as input
2. compute MD
MD5(M)=MD

3. BDP(MD)=MD'
4. MD'=K
5. Ek (M) =CT
CT= Ek 1(d K2(Ek1(M)))
6. go to step 4
7. Encrypt key K with RSA
Ebpk (K) =CK
8. CK+CT=CM

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

9. Send CM to receiver

V. 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'.

Receiver Side Decryption Algorithm

1. RECEIVE CM
2. Dbsk (CK) =K=MD'
3. Dk (CT) =M
Dk1 (Ek2 (D k1(CT)))=M

VI. 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.

VII. EMPIRICAL RESULTS

We apply our methodology to various size of sample plain text file which the sender wants to transmit through zigbee technology and set up the experimental results such as size of text file to be encrypt, size of cipher text file (output) 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

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

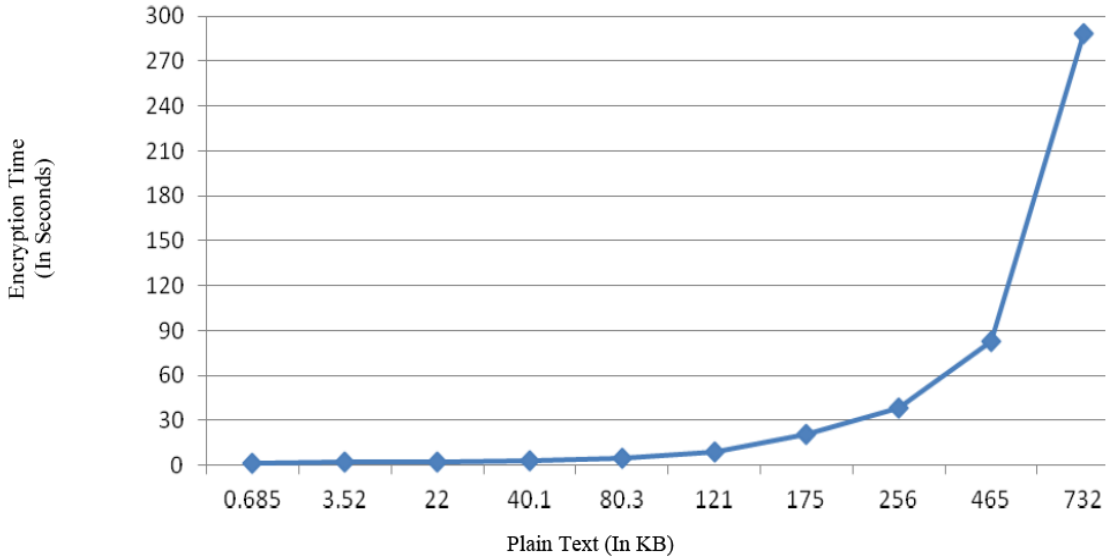

Fig 4: Encryption time for various size of plain text file

VIII. CONCLUSION

Since data transmission through zigbee 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 zigbee data transmission. This scheme provides integration of Triple DES, RSA and MD5 together to achieve the high level of data security in zigbee transmission.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Starting with the concept proposed which is the integration of most popular cryptographic algorithm. We introduce an idea of integrity verification of data received by receiver. By applying cryptographic algorithm such as triple DES, RSA and MD5 together, we succeed in secure data transmission through zigbee 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. The results shown in Table 2 proved that this property is achieved by this proposed system, but it is possible that the conclusions are cautious.

IX. FUTURE WORKS

This proposed work would be inspiring for advance research such as secure zigbee transmission of PDF file, video file, image file, etc. . 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.

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] Kalaiselvi V.S., Prabhu K., Ramesh M., Venkatesan V., "The association of serum osteocalcin with the bone mineral density in post menopausal women",Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(5) (2013) pp.814-816.

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

[4] Jayalakshmi T., Krishnamoorthy P., Kumar G.R., Sivamani P., "The microbiological quality of fruit containing soft drinks from Chennai", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 3(6) (2011) pp. 626-630.

[5] 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".*

[6] Kulanthaivel L., Srinivasan P., Shanmugam V., Periyasamy B.M., "Therapeutic efficacy of kaempferol against AFB1 induced experimental hepatocarcinogenesis with reference to lipid peroxidation, antioxidants and biotransformation enzymes", Biomedicine and Preventive Nutrition, ISSN : 2210-5239, 2(4) (2012) pp.252-259.

[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] Rekha C.V., Aranganna P., Shahed H., "Oral health status of children with autistic disorder in Chennai", European Archives of Paediatric Dentistry, ISSN : 1818-6300, 13(3) (2012) pp.126-131.

[9] 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.

[10] Sundararajan M., "Optical instrument for correlative analysis of human ECG and breathing signal", International Journal of Biomedical Engineering and Technology, ISSN : 0976 - 2965, 6(4) (2011) pp.350-362.

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

[12] Jemima Daniel,Language Teaching in the Digital Age,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 11029-11031, Vol. 3, Issue 4, April 2014.

[13] Jemima Daniel,Importance of Group Discussions,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 9081-9084,Vol. 3, Issue 2, February 2014.

[14] Jemima Daniel,The Playboy of the Western World' As a Tragi-Comedy, International Journal of Innovative Research in Science,Engineering and Technology,ISSN: 2319-8753,pp 10379-10381,Vol. 3, Issue 3, March 2014.

[15] Jemima Daniel,Techniques Used in Teaching English, International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 8791-8793,Vol. 3, Issue 1, January 2014.

[16] M. Santhi & Dr. A. Mukunthan,A Detailed Study of Different Stages of Sleep and Its Disorders – Medical Physics,International Journal of Innovative Research in Science, Engineering and Technology ,ISSN: 2319-8753, pg 5205-5212 , Vol. 2, Issue 10, October 2013.

[17] M.NAGESHWARI, Dr.A.MUKUNTHAN , C.RATHIKA THAYA KUMARI,A Study of Surface Ozone Measurement at Vadasery, Kanyakumari District,International Journal of Computer & Organization Trends (IJCOT),ISSN: 2319-8753, pp 160-165,Vol. 1, Issue 2, December 2012.