INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ENGINEERING RESEARCH AND DEVELOPMENT (IJCSERD)

ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online)
Volume 4, Number 2, April- June (2014), pp: 60-65
© PRJ Publication, http://www.prjpublication.com/

IJCSERD

© PRJ PUBLICATION

SECURE ZIGBEE PROTOCOL USING RSA CRYPTOGRAPHIC ALGORITHM

J. Sivaiah[1], M.S.V.Vara Prasad[2], K.Krishna Murthy[3]

[1]Department of B.S & H,Vignans Lara Institute of Technology & Science,
Vignan College of Engineering and Technology, Vadllamudi

[2,3]Department of Electronics, P.G. Center,
P. B. Siddhartha College of Arts & Science, Vijayawada

ABSTRACT

We propose a novel wireless access monitoring and control system based on Zigbee technology that provides the possibility of various routes and selects the shortest possible path to interact with the systems. Zigbee wireless technology eliminates the connection of wires from system to system i.e. wireless home automation systems. The technology can effectively play as an economic interactive interface in various electronic, electrical and power devices. In this work to uniquely modify it with the implementation of RSA cryptographic algorithms. It is also comparatively better than its closest counterparts like integer factorization systems, discrete or logarithm systems and ECC. The present work reports advantageous features. During the transmission of the signal if one path is obstructed automatically the nearest path is selected for interaction. The implementation of RSA Cryptographic Zigbee protocol provides maximum security to the data transmission. The time required for hacking the data is more compared to encryption and decryption during the transmission of data. In brief, the implementation of RSA with Zigbee provides multipath data transmission with good secured cryptographic system. It can also be applied to the real market for home networking systems.

Key words: RSA With Zigbee Protocol, PC Based Wireless Technology, Data Transmission, Cryptography, Data, Path.

INTRODUCTION

Did you ever walk into an empty house where the temperature was at a comfortable level and your dinner was hot and waiting for you, and the TV was on your favorite channel ? If you felt this to be a homely welcome to you then you probably knew that this dream was expensive and unrealistic for the common middle class. Currently available technology allows this to be done with timers and/or expensive computers with messy cable connections.

This is currently done on a very limited basis, for the rich and disabled. We would like to present our scope on home automation, which is cheaper, wireless and convenient to use.
Imagine controlling your household appliances with your PC (Personal Computer). Today this dream can be realized with Zigbee wireless Technology **[1-9].** Zigbee is a new technology, which has at its centre the goal of eliminating wired connections between computers. Instead of connecting with wires, every appliance has small transmitters or receivers **[12-19]**.

The home automation systems provide mutual interoperability between various electronic, electrical, and power devices as well as interactive interface for people to control their operation. These features are very helpful to optimize and to economize energy consumption whereby saved energy during some few years could make more money than home automation systems implementation cost [5]. These technologies make peoples' lives also easier, especially for elderly persons and persons with disabilities. These systems exist of course, but there are many non-interoperable, expensive, and often wired systems. Wiring complicates implementation of the home automation in buildings which are already built, especially in historical ones. Therefore, my dissertation will be a system which comes out with a product based on PC and Zigbee wireless technology which could effectively communicate **[20-23]** with each other to control home devices/appliances.

OVERVIEW OF RSA ALGORITHM

RSA is one of the most popular and successful public key cryptography algorithms. The algorithm has been implemented in many commercial applications. It is named after its inventors Ronald L. Rivest, Adi Shamir, and Leonard Adleman. They invented this algorithm in the year 1977. They utilized the fact that when prime numbers are chosen as modulus, operations behave "conveniently". They found that if we use a prime for the modulus, then raising a number to the power (prime - 1) is 1.

It is based on a very simple number-theoretical idea, and yet it has been able to resist all cryptanalytic attacks. The idea is a clever use of the fact that, while it is easy to multiply two large primes, it is extremely difficult to factorize their product. Thus, the product can be publicized and used as the encryption key. The primes themselves cannot be recovered from the product and are used for decryption. There is no formal proof whatsoever that factorization is intractable or is intractable in the special case needed for RSA, and that factorization is needed for the cryptanalysis of the RSA.

RSA algorithm simply capitalizes on the fact that there is no efficient way to factor very large integers. The security of the whole algorithm relies on that fact. If someone comes up with an easy way of factoring a large number, then that's the end of the RSA algorithm. Then any message encrypted with the RSA algorithm **[13-15]** is no more secure. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key **[10-13]**and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet **[17-23]**.

The private key is used to decrypt text that has been encrypted with the public key **[10-13]**. Thus, while sending a message, it is easy to find out the public key (but not the private key) from a central administrator and the message is encrypted using the public key. While receiving it, the message is decrypted with the private key.

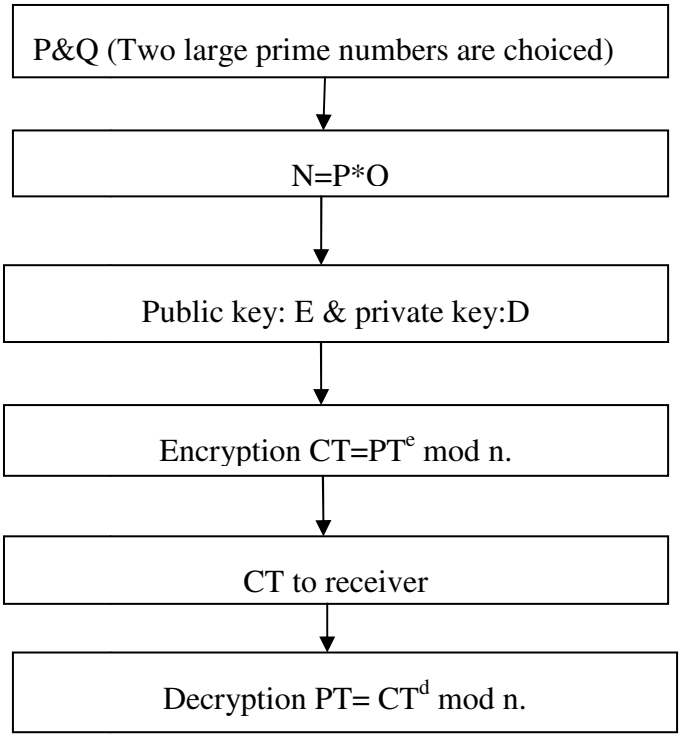
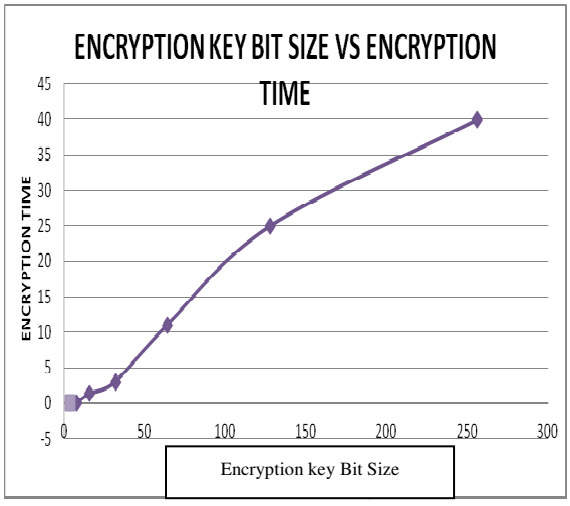


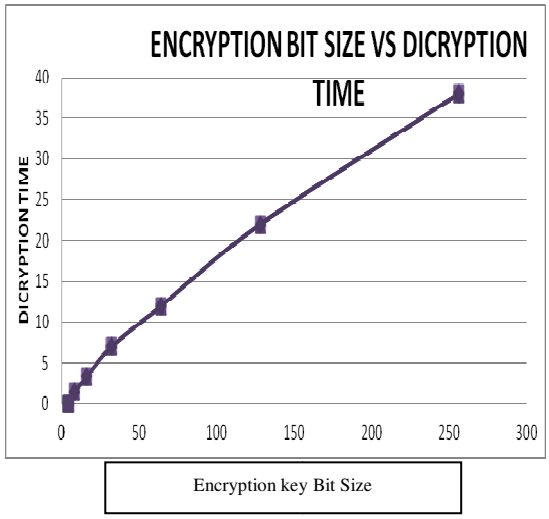
Fig 4.1: RSA algorithm

RESULTS

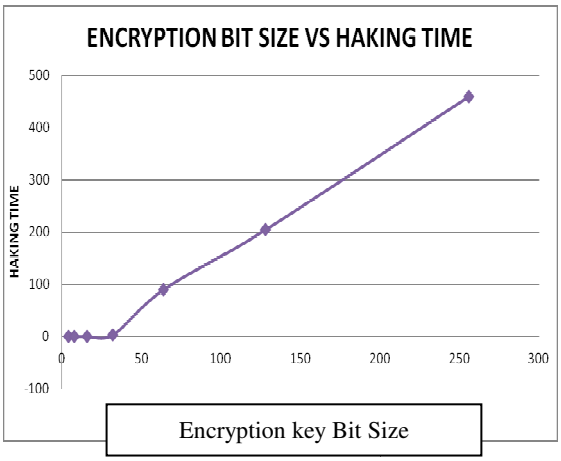
The simulation (SIMULINK 7.9) results are tabulated Corresponding graphs are plotted for Encryption Time, Decryption Time and Hacking time with respect to Encryption key Bit Size



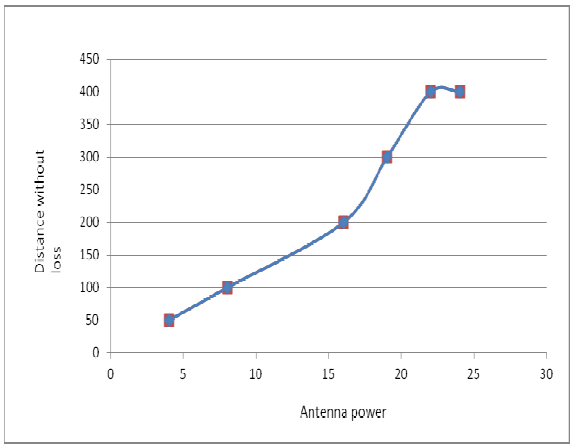
Graph.1. Encryption key Bit Size Vs Encryption Time



Graph.2 Encryption key Bit Size Vs Decryption Time



Graph.3. Encryption key Bit Size Vs Range Decryption Time



Graph.4. Antenna Input Power Vs (without loss)

ANALYSIS

In encryption, the key bit size increases, encrypted time increases and also increases the Decrypted time. In between, the data thefting time i.e. hacking time is more. So before hacking the information the data is more secured.

In Zigbee transceivers, the given input power of antenna increases and the distance covered without loss of the data is increased up to 19 mw. Beyond that the power increases the data without loss covers which a distance limited to 4 m.

RSA cryptographic systems have proven to be effective and more manageable than BLAKE systems in a large number of scenarios. Implementers today are faced with a choice between three types of public-key systems: integer factorization systems, discrete logarithm systems, and ECC. Each of these systems is capable of providing confidentiality, authentication, data integrity and non repudiation. Of the three, however, the RSA offers significant efficiency savings due to its added strength-per-bit. These savings are advantageous in many applications, particularly when computational power, bandwidth, or storage space limitation and encryption time, decryption times are less with more hacking time.

In the cryptographic systems, we are having single path. If we use Zigbee protocol, we will have Multi paths. So in this implementation of RSA with Zigbee, we have Multipath data transmission that takes place in the secured cryptographic systems.

CONCLUSIONS

The implementation of RSA with Zigbee protocol provides maximum security. In PC based wireless technology, the data could be effectively communicated to the respective system in a single route. If this route is failed, there is no data transmission. If PC based Zigbee protocol is used, it can select itself the other possible shortest route. No data loss occurs due to multi routed Zigbee system. In RSA cryptographic systems using Zigbee protocol, data transmission through Encryption and Decryption, time is very less, when compared to the Hacking time for a longer bit size. In RSA cryptographic Zigbee protocol, the range varies with antenna power with out loss of the Encrypted data.

REFERENCES

[1] ZigBee Alliance, ZigBee Specification, ZigBee Document 053474r06 Version 1.0, April 2004.

[2] J. Choi, B. Ahn, Y. Cha, and T. Kuc, "Remote-controlled Home Robot Server with Zigbee Sensor Network," SCIE - ICASE International Joint Conference, pp. 3739-3743, October 2006.

[3] I. Poole, "What exactly is ZigBee?," Communications Engineer, vol. 2,no. 4, pp. 44-45, August 2004.

[4] N. Baker, "Bluetooth strengths and weaknesses for industrial applications," IEE Computing & Control Engineering, pp. 21-25, April 2006.

[5] A. Wheeler, "Commercial applications of wireless sensor networks using, ZigBee," IEEE Communications Magazine, pp. 70-77, April 2007.

[6] L. Zheng, "ZigBee wireless sensor network in industrial Applications",SICE-ICASE International Joint Conference, pp. 1067-1070, October 2006.

[7] J. Jonn and S. Gong, "ZigBee-re ady modules for sensor networking,"Proceedings of Workshop on Real-World Wireless Sensor Networks,Stockholm, Sweden, pp. 103-104, June 2005.

[8] D. Egan, "The emergence of ZigBee in building automation and industrial control," Computing & Control Engineering Journal, vol. 16,no. 2, pp. 14-19, June 2005.

[9] A. Jurisic and A.J. Menezes, "Elliptic curves and cryptography", Dr. Dobb's Journal, pages 26-35, April 1997.

[10] ANSI X9.62, "Public key cryptography for the financial services industry - the Elliptic Curve Digital Signature Algorithm (ECDSA)", draft, 1997.

[11] W. Diffie and M.E. Hellman, "New directions in cryptography", IEEE Transactions in Information Theory, volume IT-22, pages 644-654, November 1976.

[12] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", Advances in Cryptology - Proceedings of CRYPTO'84, Springer Verlag Lecture Notes in Computer Science 196, pages 10-18, 1985.

[13] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, volume 21, pages 120-126, February 1978.

[14] C.P. Schnorr, "Efficient signature generation by smart cards", Journal of Cryptology, volume 4, pages 161-174, 1991.

[15] H.C. Williams, "A modification of the RSA public-key encryption procedure", IEEE Transactions on Information Theory, volume IT- 26, pages 726-729, 1980.

[16] W. P. Kluge, "A fully integrated 2.4-GHz IEEE 802.15.4-compliant transceiver for ZigBeeTM applications", IEEE Journal of Solid-State Circuits, vol. 41, no. 12, pp. 2767-2775, December 2006.

[17] N. Kokkos, A. Floros, N. Tatlas, and J. Mourjopoulos, "A paradigm for wireless digital audio home entertainment," Audio Engineering Society 120th Convention, Paris, May 2006.

[18] T.B. Zahariadis and A.K. Sakintzis, "Introduction to special feature on wireless home networks," ACM Mobile Computing and Communications Review, vol. 7, no. 2, April 2003.

[19] S. Conner and R. Gryder, "Building a wireless world with mesh networking technology," Technology@Intel Magazine, November 2003.

[20] Il-Kyu H Wang ,Jin-Wook Baek "Wireless acess Monitoring And Control System Based On Digital Door Lock" IEEE Transactions on consumer electronics , vol 53, no. 4, pp. 1724-30, Nov-2007.

[21] K. Sangani, "Home automation – It's no place like home," Engineering & Technology, vol. 1, no. 9, pp. 46-48, December 2006.

[22] T. Ciardiello, "Wireless communications for industrial control and monitoring," computing and Control Engineering, vol. 16, no. 2, pp. 12-13, April 2005.

[23] V.S. Miller, "Use of elliptic curves in cryptography", Advances in Cryptology - Proceedings of CRYPTO'85, Springer Verlag Lecture Notes in Computer Science 218, pages 417-426, 1986.