ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Security Enhanced Standard for Zigbee Network

Kantem Vanitha
MTech Student
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

A.Swathi
Assistant Professor
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

ABSTRACT: ***The security protocols used in ZIGBEE relies on an advanced encryption standard-counter mode (AES-CTR) algorithm to encrypt data before transmission. This algorithm is very robust, but it is time consuming. For some industrial and medical applications, it does not meet the real-time requirement. When the AES is used in counter mode CTR, it becomes like a stream cipher that aims to generate pseudorandom bits. Also, to encrypt data, the latter are combined with the plaintext using the XOR operation. New fast stream ciphers were proposed for the e-Stream project, but these ciphers have shown some weakness. On the other hand, ciphers based on chaotic functions seem to be more promising. Detailed analyses have shown that chaotic functions have very good cryptographic properties and can be used to construct high speed and strong stream ciphers. In this paper, a new robust and fast chaotic encryption algorithm RFCA is presented. This consists of a chaotic cipher composed of two perturbed maps piecewise linear chaotic map. This algorithm is, in particular, adequate for data encryption in ZigBee networks where robustness and real time are both essential. A comparison between our algorithm (RFCA), the AES-CTR and the simplified AES.***

Index Terms: ***AES Encryption, computer languages, pipeline processing, reconfigurable architectures.***

INTRODUCTION:

This paper addresses the need of finding patterns in a sequence of rows. We see this often in Complex Event Processing where business processes are driven from sequence of events, in Security applications where detection of unusual behavior definable with regular expressions is needed, in Financial applications where detecting stock patterns is critical, Fraud Detection applications, and for RFID processing where tracking of valid paths for RFID tags is needed. This paper proposes new SQL functionality for finding patterns in sequences of rows. Patterns are defined using familiar syntax of Regular Expressions (RE). RE variables span sub-sequences of rows and are defined using conditions on individual rows and their aggregates. New pattern recognition clause, the MATCH_RECOGNIZE clause, can be applied either to a table expression or can be used in a window definition. In the former case we provide two modes of matching: one that issues a single row for each match of the pattern or one that issues all rows that matched it. In both cases, we can perform and emit calculations on the pattern variables. In the latter case, a win-dow size is defined using a pattern, and then standard processing on the window of rows can take place.

Existing System:

Data Encryption Standard previously predominant algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small. There are also some analytical results which demonstrate theoretical weaknesses in the cipher. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology. The existing modes of operation in the literature (ECB, CBC, OFB, CTR, CFB, DES, Triple DES), CTR mode is widely used and it is well suited to operate on a

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

multiprocessor machine where blocks can be encrypted in parallel.

EXISTING SYSTEM ALGORITHM:

- Triple DES Algorithm

EXISTING SYSTEM DRAWBACKS:

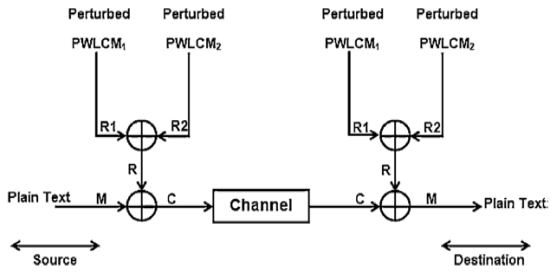
- It is required more Memory space.
- More time required.
- Easily hack the architecture.

Proposed System:

We present our proposed chaotic algorithm RFCA. A good encryption algorithm should be robust against all kinds of cryptanalytic, brute-force, and statistical attacks. In this section, the performance of the RFCA scheme is analyzed and compared with the eSream final candidates, the simplified AES, and the AES-CTR. As the image encryption is more difficult from text encryption due to some intrinsic properties of images such as bulky data capacity and high redundancy.

PROPOSED SYSTEM BLOCK DIAGRAM:

PROPOSED RFCA SCHEME:



PROPOSED SYSTEM ALGORITHM:

- AES Algorithm
- New Robust and Fast Chaotic Encryption Algorithm (RFCA**)**

PROPOSED SYSTEM ADVANTAGES:

- More secured

It is required less Memory space

Chaotic cryptographic

Chaos functions have mainly used to develop mathematical models of non linear systems. They have attracted the attention of many mathematicians owing to their extremely sensitive nature to initial conditions and their immense applicability to modeling complex problems of daily life. Chaotic functions which were first studied in the 1960's show numerous interesting properties. The sequences produced by such functions [9] has very good random and complexity. These functions have an extreme sensitiveness to initial conditions. For example, if the initial start value of a chaoticfunction is modified 10-20, iterative numbers produced after some iterations are completely different from each other. This extreme sensitivity to initial conditions and some other interesting properties, such as pseudo-randomness, ergodicity, wide spectrum and good correlation, grant chaotic functions as a promising alternative for the conventional cryptographic algorithms.

Dynamical degradation

Digital chaotic generators have been proposed such as the traditional continuous chaotic maps. But they are discretized in 2N finite space, and many researchers have found that they don’t have good statistical properties and they present dynamical degradation. Such degradation threatens security of designed chaotic ciphers. Because of the sensitivity of chaotic systems, the quantization errors which are introduced into iterations will make pseudo orbits in finite precision entirely different from the theoretical ones even after a short number of iterations.

Chaotic generator The chaotic stream cipher is based on chaotic map as PRNG to encrypt the plaintext bit by bit. The produced chaotic random sequences are combined with the plaintext using XOR operation. There are very tight relationships between pseudo-random sequence and good cryptography. Consequently, the higher randomicity the chaotic sequence is, the stronger the encryption robustness will be. Therefore, to replace the RC4 and AES-CTR in the considered wireless networks, we need a high performance chaotic generator which can produce random series having a noise-like shape. And it must be very fast to meet the real time requirement of industrial control

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONFIGURABLE ELEMENTS

The FPGA has three major elements: Configurable logic blocks, input/output blocks and interconnects. The CLBs provide the functional elements for constructing user's logic. The IOBs provide the interface between the package pins and internal signal lines. The programmable interconnect resources provide routing paths to connect the inputs and outputs of the CLBs and IOBs into the appropriate networks. The field-programmable Gate Array provide the benefits of custom MOS VLSI, while avoiding the initial cost, time delay, and inherent risk of a conventional masked gate array. The FPGAs are customized by loading configuration data into the internal memory cells. Complex programmable logic Devices and Field programmable Gate Array are becoming a critical part of every system design. There are many different FPGAs with different architectures/ processes. There are four main categories of FPGAs currently and sea-of-gates .In all of these FPGAs the interconnections and how they are programmed vary.

TECHNOLOGIES

Currently there are four technologies in use. They are: static RAM cells, anti-fuse, EPROM transistors, and EEPROM transistors. Depending upon the applications, one FPGA technology may have features desirable for that application.

1.Static RAM Technology

In the Static RAM EPGA programmable connections are made using pass-transmission, transmission gates, or multiplexers that are controlled by SRAM cells. This technology allows fast in-circuit reconfiguration. The major disadvantage is the size of the chip required by the RAM technology and that the chip configuration needs to be loaded to the chip from some external source (usually external non-volatile memory chip). The FPGA can either actively read its configuration data out of external serial or byte-parallel PROM (master mode), or the configuration data can be written into the FPGA (slave and peripheral mode). The FPGA can be programmed an unlimited number of times.

1.Anti-Fuse Technology

An anti-fuse resides in a high-impedance state; and can be programmed in to low impedance or "fused" state. This technology can be used to make program once devices that are less expensive than the RAM technology.

2.EPROM Technology

This method is the same as used in the EPROM memories. The programming is stored without external storage of configuration. EPROM based programmable chip cannot be re-programmed in circuit and need to be cleared with UV erasing.

3.EEPROM Technology

This method is the same as used in the EEPROM memories. The programming is stored without external storage of configuration. EEPROM based programmable chips can be electrically erased but generally cannot be re-programmed in-circuit FUSE-One-time programmable.

CONCLUSION:

A new encryption method has been proposed for Wi-Fi and ZigBee networks. It relies on a new chaotic generator formed by the combination of two perturbed PWLCM map. The proposed generator has the role of a stream cipher that produces random sequences which resembles stochastic noise. This sequence is combined with the plaintext to form the encrypted data. The proposed encryption algorithm has very good properties and succeeds all the statistical tests. We have shown also that the proposed method gives better results than the AESCTR in terms of many measures and tests like: correlation, UACI, NPCR, and NIST statistical tests. Therefore, this encryption method is very secure and it has a high encryption speed. Additionally, it is easily realized, it has a very large key range and it needs a low memory capacity. So, it meets the requirements of industrial control and it can replace the traditional encryption methods used in Wi-Fi and ZigBee networks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

[1] S. Charkravarthy and Q. Jiang, Stream Data Processing: A Quality of Service Perspective. New York: Springer-Verlag, Apr. 2009.

[2] D. Gyllstrom, J. Agrawal, Y. Diao, and N. Immerman, "On supporting Kleene closure over event streams," inProc. IEEE 24th Int. Conf. Data Eng., Apr. 2008, pp. 1391–1393.

[3] F. Zemke, A. Witkowski, and M. Cherniak, "Pattern matching in sequences of rows," American National Standards Institute, Washington, DC, Tech. Rep. ANSI NCITS H2-2006-nnn, Mar. 2007.

[4] M. R. Mendes, P. Bizarro, and P. Marques, "A performance study of event processing systems," inPerformance Evaluation and Benchmark-ing, vol. 5895. New York: Springer-Verlag, 2009, pp. 221–236.

[5] OPRA. (2011, Jan. 19). Updated Traffic Projections 2011 & 2012, Chicago, IL [Online]. Available: http://www.opradata.com/specs/upd_ traffic_proj_11_12.pdf

[6] R. Mueller, J. Teubner, and G. Alonso, "Streams over wires—A query compiler for FPGAs," inProc. Int. Conf. Very Large Data Bases,vol.Aug. 2009, pp. 229–240.

[7] L. Woods, J. Teubner, and G. Alonso, "Complex event detection at wire speed with FPGAs," inProc. Int. Conf. Very Large Data Bases,vol.3. Sep. 2010, pp. 660–669.

[8] H. Inoue, T. Takenaka, and M. Motomura, "20 Gb/s C-based complex event processing," inProc. IEEE Int. Conf. Field Program. Logic Appl., Sep. 2011, pp. 97–102.

[9] R. Sidhu and V. Prasanna, "Fast regular expression matching using FPGAs," inProc. IEEE Symp. Field-Program. Custom Comput. Mach., Apr. 2001, pp. 227–238.

[10] B. Johnson, Algorithmic Trading and DMA: An Introduction to Direct Access Trading Strategies. Myeloma, U.K.: Myeloma Press, Feb. 2010.