International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

Low Cost and Highly Efficient Authentication Protocol Design with Parallel Error Correcting Code

Agnes Shiny Rachel.N, M.Jaishree, B.Banu Selva Saraswathy, Subashree.K
Sri Krishna College of Technology

ABSTRACT

Wireless sensor networks (WSN) have been widely used, most notably in real-time traffic monitoring and military sensing and tracking. WSN applications could suffer from threats and endanger the applications if the suitable security issues are not taken into consideration. As a result, user authentication is an important concern to protect data access from unauthorized users. This paper presents a light weight mutual authentication protocol for WSN applications. Instead of the traditional use of hash function for data protection, in the proposed system a key encryption function is used, that only requires simple Ex-or arithmetic operations. Previously CRC16 was used which has high latency because of serial design. This is replaced by Golay code in the proposed system. Golay code not only detects the error but is also used to rectify errors.

KEYWORDS: Golay Code, mutual authentication, protocol, encryption.

INTRODUCTION

Omar Cheikhrouhou et.al in 2008 proposed a light weight user authentication scheme adapted to WSNs that provides mutual authentication and session-key agreement. The proposed scheme allows a user equipped with mobile device (typically PDA) to authenticate himself before gaining access to the WSN. The scheme is executed at two sides; the client side which controls the user's mobile device and the server side represented by the coordinator of the WSN. A security analysis of the scheme is presented and it proves its resilience against classical types of attacks. In addition, we have made a comparison between our scheme and the existing ones based on their security properties, and shown that our proposed scheme outperforms the existing ones in terms of confidentiality, integrity, mutual authentication and session key generation with a lightweight computation overhead. Securing Wireless Sensor Networks (WSNs) is a challenging task as it presents a hard environment with constrained resources. Therefore, security mechanisms designed for WSNs must be lightweight and efficient. One of the major important risks that faced WSNs is the illegal access of attackers to the data.

Designing a user authentication protocol for wireless sensor networks is a difficult task because wireless networks are susceptible to attacks and sensor node has limited energy, processing and storage resources. Wireless sensor networks (WSNs) are large scale, usually slow moving or Static. The nodes (motes) in such networks are designed to sense the environment and collect data. Proper authentication of users must be ensured before allowing the users to access data. However, we find that this issue has not been addressed adequately in comparison with the network and link layers protocols in WSNs. One of the reasons is that these schemes could not resist the insider attack and the related impersonation attack. Here the insider attack is defined as that any manager of the system purposely leaks the secret information leading to serious security weaknesses of an authentication protocol.

The presence of multiple obstacles on the real deployed geographical area may hinder the effective operations of large scale wireless sensor network in terms of significant disturbance in proper routing, increased delay in data transmission and increased energy consumptions. To overcome this problem, a novel pulse mode object localization algorithm and its VLSI implementation for designing the sensor node processor was proposed by J.Bag et.al in 2014. The algorithm supports distributed and energy efficient sleep scheduling with periodic synchronization and reconfigure the routing scheme that can be used to extend the life time of sensor network.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

The algorithm is made power efficient by using pulse mode operation. It is a high performance sensor node processor with an overall power consumption of 0.012 mW in active mode with a dynamic current of 1.27 mA at the working frequency of 1,536 MHz

Memories that operate in harsh environments, like for example space, suffer a significant number of errors. Pedro Reviriego.,et.al in 2014 has put forth a double adjacent error correcting parallel decoder for the extended Golay code. The error correction codes (ECCs) are routinely used to ensure that those errors do not cause data corruption. A number of recent works have proposed advanced ECCs, such orthogonal Latin squares or difference set codes that can be decoded with relatively low delay. A compromise solution has been recently explored for Bose–Chaudhary–Hocquenghem codes. The idea is to implement a fast parallel decoder to correct the most common error patterns (single and double adjacent) and use a slower serial decoder for the rest of the patterns. An Efficient and Robust User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card proposed by Tanmoy Maitra et.al discusses that the scheme is secure against all possible attacks disapproving the method put forth by Das et.al. After deployment of sensor nodes, they communicate to other neighbouring nodes within their communication range to form clusters. After that, one cluster head or gateway node is selected by base station or sensor nodes for each cluster on the basis of energy, signal strength, degree, capability, mobility etc. All the sensor nodes sense raw data from environment and send to their nearest cluster head by single-hop or multi-hop communication. Cluster heads gather the raw data and send to nearest base station or sink node by multi-hop or single-hop communication.

EXISTING METHOD:

Wireless sensor network play an important role in information transmission and have a wide variety of applications such as real-time traffic monitoring, building safety monitoring, military sensing and tracking, and so on. They are composed of many tiny and low-cost sensor nodes with limited energy and computation ability to cooperatively monitor physical environmental information. A new key generation function, which is a main component for data encryption, is proposed. The password and data leakage risk can be reduced by exploiting the Key Generation function and XOR arithmetic operation for cover coding. User authentication is one of the most crucial security mechanisms to prevent the illegal or malicious entities from accessing the WSNs. Public key cryptography (PKC) and elliptic curve cryptography (ECC) to design a new authentication mechanism. A distributed entity authentication architecture was introduced. It is established on the self-certified key cryptosystem, which is a modification of ECC. The advanced user authentication scheme was based on the fact that it employed both the PKC and symmetric key cryptography schemes. This approach provides higher energy efficiency as compared to the existing PKC-based schemes, whereas the PKC- or ECC-based scheme suffers from a high computational cost for WSNs.To alleviate the computational cost, a dynamic password-based authentication scheme requires one-way hash functions and simple XOR operations, it is vulnerable to many attacks such as re-play attacks, forgery attacks, and so on.

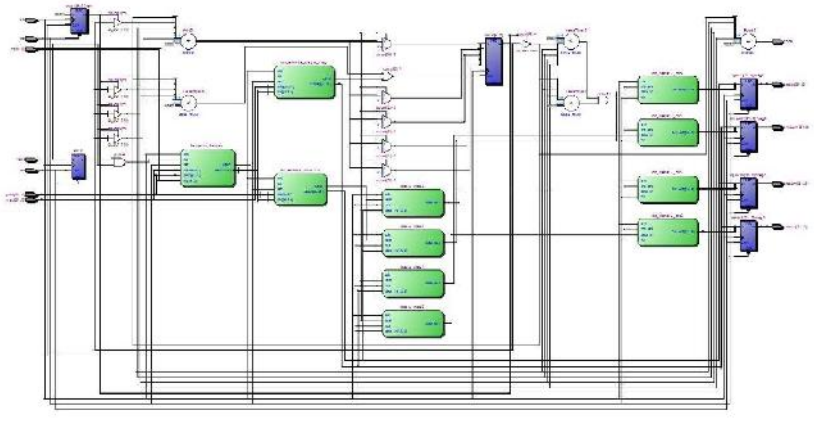

Fig 1: Schematic Diagram of the existing system

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

Message, password and Random number are the three inputs. Each input is 32 bits. Random number is further is divided into 16 bits, this 16 bits is again divided into 4bits respectively, Where RxM and RxL are denoted as 16 (MSBs) and 16 -least significant bits (LSBs) respectively, Denotes the bitwise concatenation operation. Now, let RxM and RxL be

RxM = dt1 dt2 dt3 dt4

RxL = ds1 ds2 ds3 ds4

Combining RxM, RxL and Message we can generate Random Value (RV).By using Password, Random value and RxM we can able to generate key. If we Exor the MsgM and key, we will get CCMsgM. If we Exor the CCMsgM and key then we will get original message that was send by the sender. Due to generation of key the message can't be hacked by other person. The message is confidential by generation of Key. Cycling Redundancy Check (CRC16) has been used which will detect the error alone.

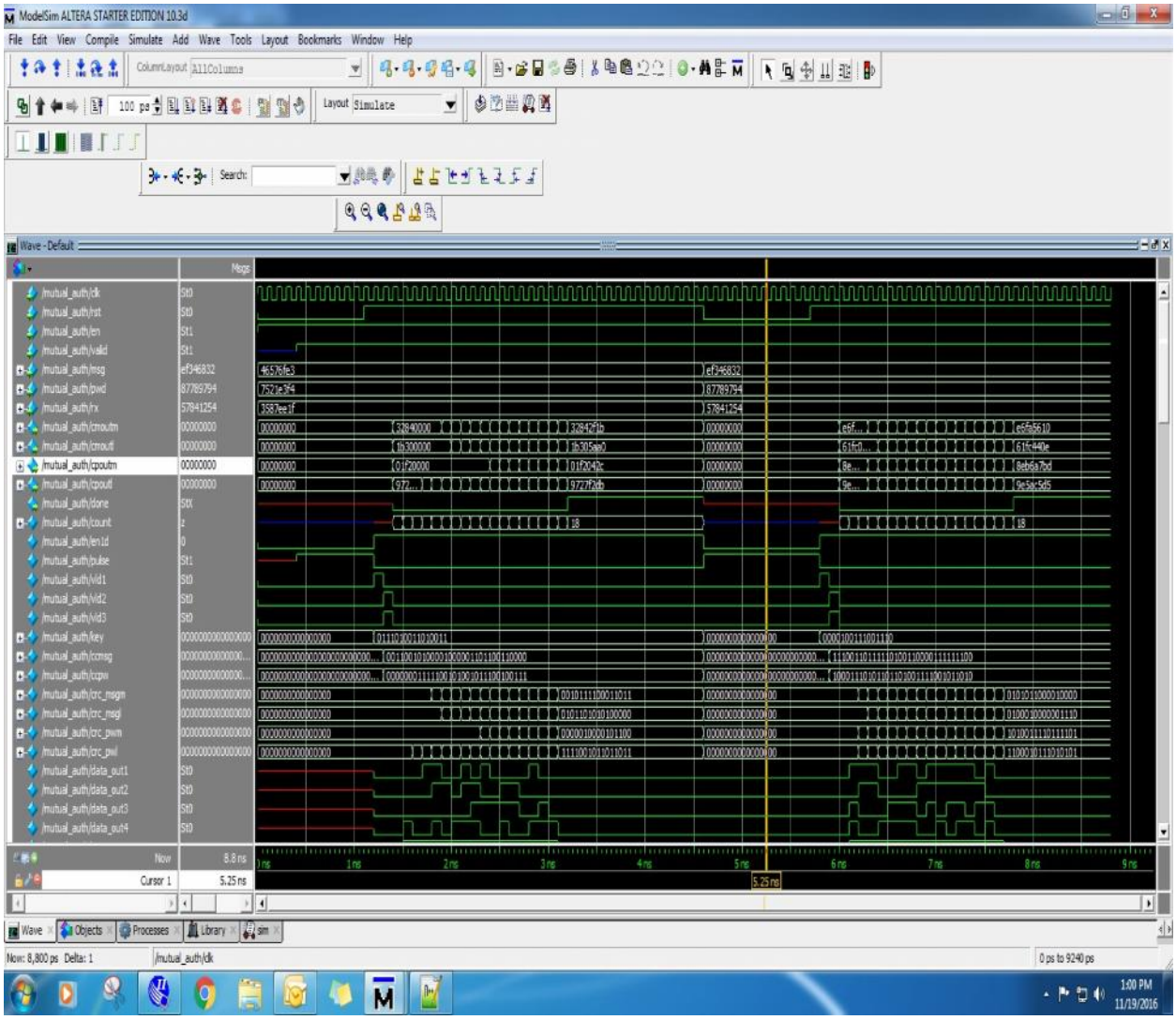

Fig 2:Output of the existing system

It is inferred from the above output that throughput is minimum of 589.0909091Mbps and at the same time delay is maximum of 22ns. The input can be of either binary or hexa-decimal. But it is more convenient to give hexadecimal as input. The random value will be generated by performing ex-or operation between

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

message and the key. The original message can be retrieved by ex-oring the key with the generated random value. The output will be displayed only after the DONE signal has been provided. Cycling Redundancy Check (CRC16) has been used which will detect the error alone.

Table 1: Tested Parameters for the Existing Method

FREQUENCY(MHz)	LATENCY(ns)	THROUGHPUT(Mbps)
402	22	589.0909091

PROPOSED METHOD

The proposed key encryption function only requires simple exclusive-OR (XOR) arithmetic operations. By replacing CRC16 block (Error Detecting Code: can only detect errors) which will have high latency because of serial design with Parallel Golay Code (Error Correcting Code: can detect & correct errors).We can retrieve the original data with the help of Golay code.

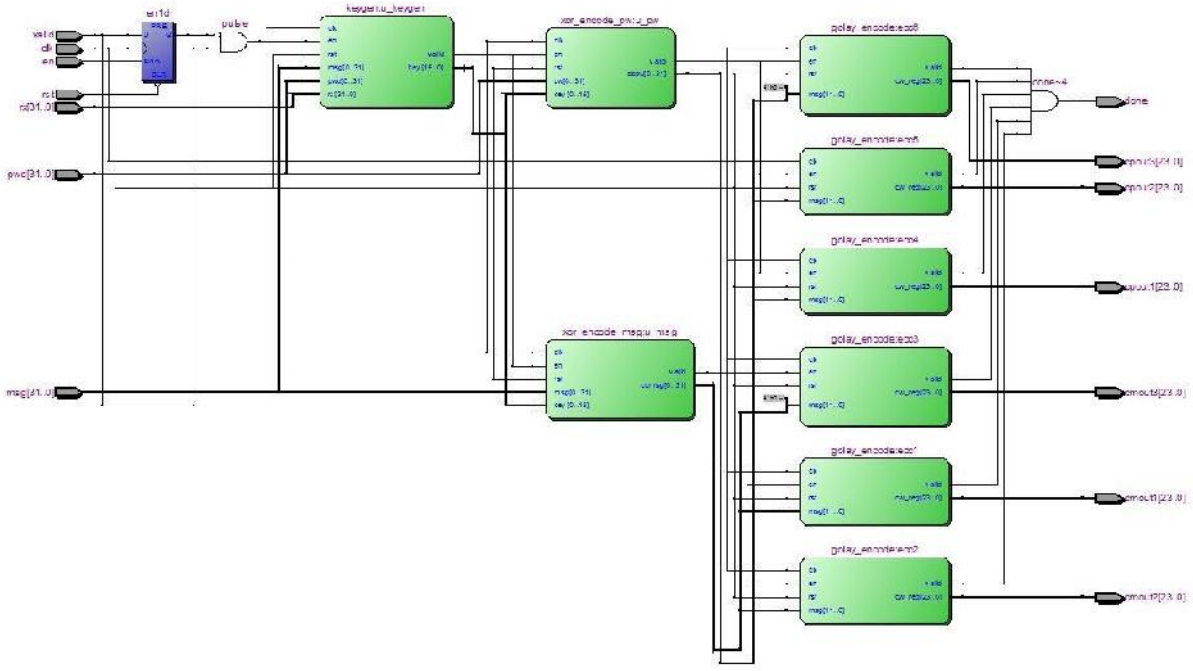

Fig 3: Proposed Block Diagram

In this system the throughput is maximum of 4000 and at the same time delay is minimum of 4ns from the output of the proposed system. The input can be of either binary or hexa-decimal. But it is more convenient to give hexa-decimal as input. The random valve will be generated by performing ex-or operation between message and the key. The original message can be retrieved by ex-oring the key with the generated random value. The output will be displayed only after the DONE signal has been provided. Cycling Redundancy Check (CRC16) has been eliminated in this system. In order to detect and rectify the error in the system, Golay code has been used. The input can be provided without any delay because of low latency.

Table 2: Tested Parameters for the Proposed Method

FREQUENCY(MHz)	LATENCY(ns)	THROUGHPUT(Mbps)
500	4	4000

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

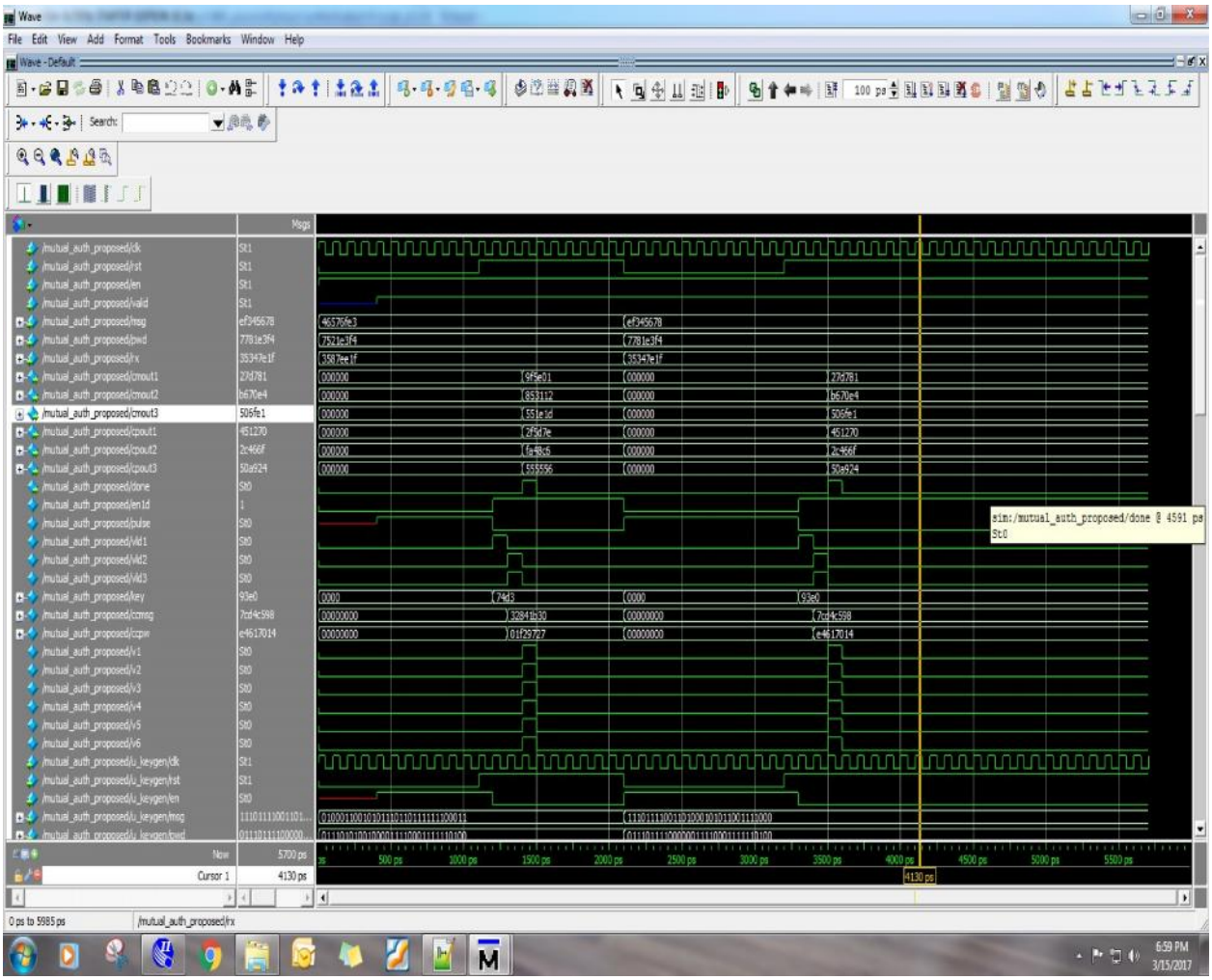

Fig 4: Output of the proposed system

CONCLUSION

By using the wireless sensor network the data is sent in a much secured manner. The data is encrypted and hence a key is generated which is known only to the end user so that no one can hack it. The end user receives the key along with the parity bit using cyclic redundant check-16(CRC-16) and Golay codes for error detection and error correction.

REFERENCES

[1] J.Bag ‘”Design and VLSI implementation of power efficient processor for object localization in large WSN”, Ad-Hoc and sensor wireless networks, Vol 4, February 2013.
[2] Z. Benenson, F. Gartner, and D. Kesdogan, “User authentication in sensor networks,” in Proc. Workshop Sensor Networks., Lecture Notes Information. Proc. Informatik, 2004, pp. 1–5.
[3] J. Bu, S. Chan, C. Chen, D. He “SDRP: A secure and distributed reprogramming protocol for wireless sensor networks,” IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.
[4] V. ÇagrıGüngör, G. P. Hancke, “Special section on ˘ industrial wireless sensor network,” IEEE Trans. Ind. Information., vol. 10, no. 1, pp. 762–764, Feb. 2014.
[5] Q. Chi,Z. Pang,L. D. Xu,H. Yan, C. Zhang“A reconfigurable smart sensor interface for industrial WSN in IoT environment,” IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1417–1425, May 2014.
[6] H. Guo, K.-S. Low, and H.-A. Nguyen, “Optimizing the localization of a wireless sensor network in real time based on a low-cost microcontroller,” IEEE Trans. Ind. Electron., vol. 58, no. 3, pp. 741–749, Mar. 2011.

[7]Omar Cheikhrouhou, AnisKoubasa, Manel Boujelben, Mohammed Abid,"A lightweight user authentication scheme for wireless sensor networks",National Conference on Electronics,Vol 18,No 3,2010.

[8] Pedro Reviriego, Shanshan liu,Liyi Xiao and Juan Antonio Maestro, "An Efficinet single and Double Adjacent error correcting Parallel decoder for the Extended Golay code", IEE Transactions on very large scale integration systems,Vol 24,No 4,April 2015

[9]Tanmoy Maitra,Ruhul Amin,Debasis Giri and P.D.Srivastava, "An efficient and Robust user authentication scheme for Hierarchial Wireless sensor networks without Tamper proof Smart card", International Journal of Network Security,Vol 18,No 3 ,2014