ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

ERROR CORRECTION USING GOLAY CODE IN WIRELESS SENSOR NETWORKS

P.AARTHI[1], S.ANUSIYA[2], S.JAYASHREE[3], R.KALAISELVI[4] A.POOJAA[5]

[1,2,3,4]STUDENT NAME[5]ASSISTANT PROFESSOR

[1,2,3,4] DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

[BHARATHIYA INSTITUTE OF ENGINEERING FOR WOMEN]

IEEE(april 2018)

Abstract-Wireless sensor network (WSN) have been widely used, most notably in real time traffic monitoring and military sensing and tracking. However, WSN application could suffer from threads and endanger the application 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 enhance efficiently a lightweight mutual authenticationprotocol for WSN application. Instead of tradition aspects of this protocol is that, for the purpose of data protection but with a low computation cost, the proposed key encryption function requires simple Exclusive (XOR) arithmetic operation. Here, perform error correction using GOLAY CODE. This process is implemented using XILINX software. The advantage of this system also allow legitimate users can freely change own passwords and the data leakage can be eliminated.

I.INTRODUCTION

Wireless sensor networks (WSNs) play an important role in information transmission and have a wide range of applications such as real-time traffic monitoring, building safety monitoring, military sensing and tracking, etc. They are composed of many little and low-cost sensor nodes with limited energy and computation ability to cooperatively monitor physical environmental intimation. It is well known that WSNs are hugely censurable and become a threat, thereby endangering the applications if the accurate security is not taken into working out. Because of it, how to secure WSNs has been becoming a challenging issue as it presents a resource-constrained environment.

User authentication is one of the most determinant security mechanisms to prevent the illicit or malicious entities from accessing the WSNs. In the past 10-15 years, various authentication schemes in WSNs have been proposed. Berenson et al. presented an authentication protocol where users can successfully authenticate with any suborder of sensors out of a set of n sensors. Berenson et al. further utilized public key cryptography (PKC) and elliptic curve cryptography (ECC) to design a new authentication mechanism. It is established on the self-certified key cryptosystem, which is an innovation of ECC. The advanced user authentication scheme proposed by Butun was based on the fact that it employed both the PKC and symmetric key cryptography schemes. This approach provides higher energy efficiency. Where the PKC- or ECC-based scheme suffers from a high computational cost for WSNs.

To minify the computational cost, Wong et al. proposed a dynamic password-based authentication scheme. Although this scheme only requires one-way hash functions and simple XOR operations, it is censurable to many attacks such as replay (rematch) attacks, forgery (bogus) attacks, and so on. The "two-factor user authentication," can be used to avoid multiple users with the same login-id and stolen-verifier attacks. However, Das's scheme has no ability to resist gateway node bypass attack and privileged-insider attack. There is no provision of users to change or update their passwords. Consider a wireless heterogeneous sensor network that consists of two types of devices, for example, low-resource devices and high-resource devices (Star gate), also known as the GW. The high-resource devices are tamper-resistant, but the low-resource devices are vulnerable to tampering. These devices are appropriately distributed in a confined area. To query the sensor data, a user must register with the GW node and get a smartcard. Upon registration, he/she can query the sensor data within the network in a secure manner. This scheme allows the user to choose and change his password frequently and An improved scheme presented is gives various advantages, including elimination of password leakage risk, capability of auto changeable password, and better efficiency and The use of the scheme in is considered for the (24,12) Golay code, This results in a decoder that is simpler than a Personal use is permitted, but traditional SEC decoder but that can also correct all double-adjacent errors and some triple-adjacent errors.

II. PROPOSED KEY GENERATION

In proposed key generation scheme, a new key generation function (KeyG), which is a main component for data encryption (protection), is introduced.

-The password and data leakage complication can be reduced by exploiting the Key Generation (KeyG) function and XOR arithmetic operation for cover-coding.

-The Key Generation (KeyG) function and algorithm can be represented as follows.

- The 32-bit message (Mg) and password (Pw) in binary (base 2) can be represented as

Msg= m0, m1, m2... m31

Pw = p0, p1, p2... p31.

-The 32-bit random number R is represented by

$$RX = RMSB \parallel RLSB$$

Where,

1) RX=Random number

2) RMSB and RLSB are denoted as 16 most significant bits (MSBs) and 16 least significant bits (LSBs), respectively.

3) $\parallel$ denotes the bitwise concatenation operation.

Now, let RMSB and RLSB be in hexadecimal (base 16), respectively.

RMSB = dt1 dt2 dt3 dt4

RLSB= ds1 ds2 ds3 ds4

- Each digit of RMSB and RLSB is used to indicate a*each* bit location in Message(Mg) and these each bits will concatenates to form a 16-bit output in hexadecimal (base 16) can be represented as

$$Mg-KeyG\ (RMSB,\ RLSB) = mdt1mdt2mdt3mdt4 \parallel mdt1+16mdt2+16mdt3+16mdt4+16 \parallel mds1mds2mds3mds4 \parallel mds1+16mds2+16mds3+16mds4+16=dv1dv2dv3dv4 \equiv RVX$$

Where, dv1 dv2 dv3 dv4 is the hexadecimal (base 16) notation.

-Pw−KeyG (RVX, RMSB) denotes the Key Generation output. And it performed over Password (Pw) using the previously generated RVX and RMSB.

-It is indicating a bit location in Password (Pw) and each bits will concatenates to form a 16-bit Key.

- The resulting of these Key can be represented as

$$Pw-KeyG(RVX,RMSB)= pdv1pdv2pdv3pdv4 \parallel pdv1+16pdv2+16pdv3+16pdv4+16 \parallel pdt1pdt2pdt3pdt4 \parallel pdt1+16pdt2+16pdt3+16pdt4+16 = hw1hw2hw3hw4 \equiv Key$$

Where,

-hw1 hw2 hw3 hw4 is the hexadecimal (base 16) notation.

- The key generation requires two steps. and it is represented by

$$Key = Pw-Mg-KeyG\ (RX).$$

A. Encoding Procedure of the Message

1) The 32-bit message (Mg) can be represented as

$$Msg = MMSB \parallel MLSB$$

Where ,

MMSB and MLSB are 16 MSBs and 16 LSBs. By utilizing these Key, we perform the XOR operation for cover coding MMSB and MLSB, respectively,

$$CCMgM=MgM \oplus Pw-Mg-KeyG(RX)$$

$$CCMgL = MgL \oplus Pw-Mg-KeyG(RX).$$

Consequently, the cover-coded message is

$$CCMg = CCMgMSB \parallel CCMgLSB.$$

TABLE I
MATHEMATICAL NOTATIONS

Notation	Description

Msg	Message
Urkey	User Client Password
RN	RandomNumber(Public)
RM	Random Number(private)
PW	Acess Password
ID	User Identity
TS	Time Stamp
CCPWx	Cover Coded Password
CCRMx	Cover Coded Random Number
||	Concatenation Operation
T	Reasonable Time

III.(24,12)EXTENDED GOLAY CODE

The extended binary Golay code G_{24} consists of a 12-dimensional linear subspace*W* of the space $V=F_2^{24}$ of 24-bit words such that any two distinct elements of *W* differ in at least 8 coordinates. *W* is called a linear code because it is a vector space. In all, *W* comprises 4096 = 2^{12} elements.The elements of *W* are called *code words*. They can also be described as subsets of a set of 24 elements, where addition is defined as taking the symmetric difference of the subsets.In the extended binary Golay code, all code words have Hamming weights of 0, 8, 12, 16, or 24. Code words of weight 8 are called octads and code words of weight 12 are called dodecads.Octads of the code G_{24} are elements of the S(5,8,24) Steiner system. There are 759 = 3×11×23 octads and 759 complements thereof. It follows that there are 2576 = 2^4×7×23 do decads.Two octads intersect (have 1's in common) in 0, 2, or 4 coordinates in the binary vector representation (these are the possible intersection sizes in the subset representation). An octad and a dodecad intersect at 2, 4, or 6 coordinates. Up to relabeling coordinates, *W* is unique.

Binary extended golay code is a linear code generated by the 12×24 matrix G24 $=[I_{12}|A]$, where I12 is the 12×12 identity matrix and A is the 12×12 matrix. Another generator matrix for G24 is$[A|I_{12}]$.The code G24 is self-dual. Thus its parity-check matrix is H = G^t_{24}.The code G24 has no codeword of weight 4, so the distance of G24 is d =8.The code G24 is an exactly three-error-correcting code.The weight of every codeword in G24 is a multiple of 4.All codewords in G24 have even weights. The perfect binary Golay code, G_{23}, has codewords of length 23 and is obtained from the extended binary Golay code by deleting one coordinate position.The binary Golay code, G_{23} is a perfect code.

The (24,12) extended Golay code is obtained by adding an overallparity check bit to the *(*23, 12*)* Golay code [16]. This code is a perfect code with a minimum distance of seven and has been widely studied [19]. The extended code has a minimum distance of eight, and therefore can correct 3-bit errors and detect 4-bit errors.,

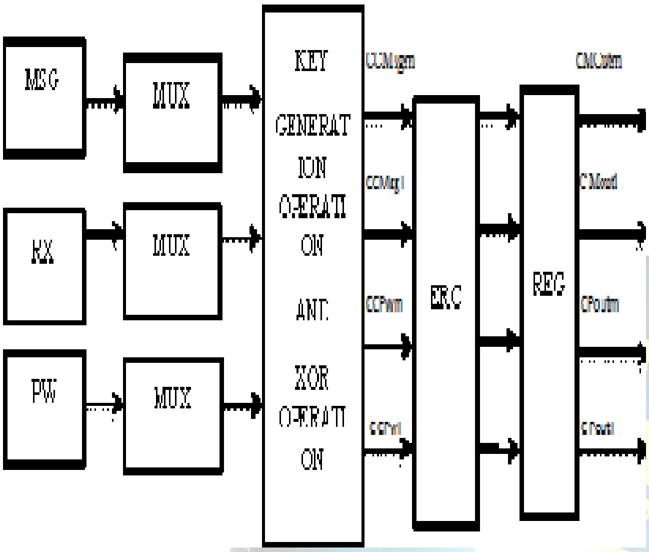

Fig.1.Mutual authentication hardware architecture

According to the mutual authentication protocol described, the proposed hardware architecture for KeyGen functions is shown in Fig. 1. In this figure, themessage Msgx, passwordPWx, and random number Rx serve as the input of KeyGen operation via 1_to_2 Mux modules.The output Keyxperforms the XOR operation with the outputsofMsgxand PWxvia 1_to_2 Mux modules to generate CCMsgM, CCMsgL, CCPWM,andCCPWL,FinallyCMOut1, CMOUT2,CMOUT3,CPOut1,CPOut2 andCPOut3 are generated the this hardware architecture.

IV.THE SIMULATION AND RESULT OF PROPOSED SYSTEM

TIMING UTILIZATION

DATA	EXISTING SYSTEM	PROPSED SYSTEM
Minimum Period	1.55ns	1.303ns
Min. Input Arrival Time Before Clock	2.047ns	2.047ns
Max. Output Required Time After Clock	1.289ns	0.575ns
Total Real Time To Xst Completion	16.00sec	13.00sec
Total CPU Time To Xst Completion	15.72sec	13.62sec

MEMORY AND FREQUENCYUSAGE

DATA	EXISTING SYSTEM	PROPOSED SYSTEM
Frequency	642.998MHZ	767.25MHZ
Memory	233340kilobytes	230076kilobytes

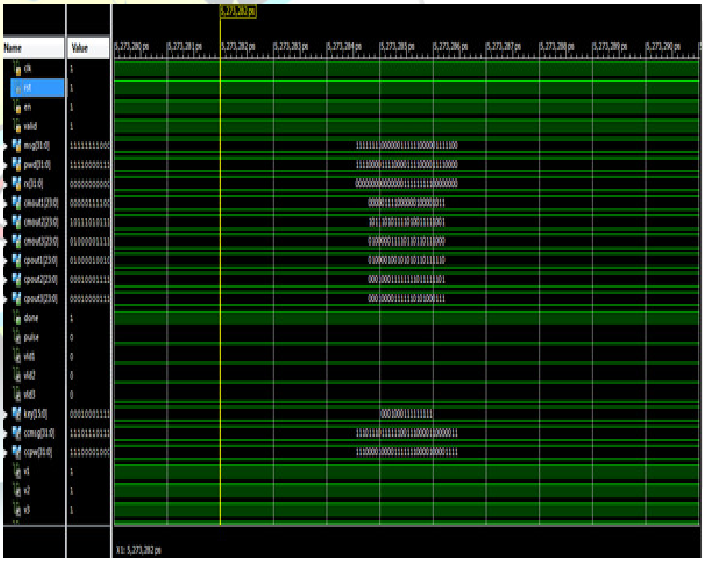

Fig 2. SIMULATION OF OUTPUT WAVEFORM

CONCLUSION

A lightweightmutual authentication protocol over WSNs has been developed in this paper. In comparison with other recent schemes, the proposed approach provides a low computational cost, while the secure data transmission is given. The corresponding architecture is also simulated using Verilog hardware description language to validate the functionality of the proposed architecture.

In addition, golaycode which provide additional security for data or message and also correction mechanism for error control.

REFERENCE

[1]Wei-Cheng Lin ,YU-Jung Huang,"Authentication protocol design and low cost key encryption function implementation for wireless sensor network", vol. 11, no. 4, december 2017

[2] H. Guo, K.-S.Low, and H.-A. Nguyen, "Optimizing the localization of awireless sensor network in real time based on a low-cost microcontroller,"IEEE Trans. Ind. Electron., vol. 58, no. 3, pp. 741–749, Mar. 2011.

[3] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. D. Xu, "A reconfigurable smartsensor interface for industrial WSN in IoT environment," IEEE Trans.Ind. Informat., vol. 10, no. 2, pp. 1417–1425, May 2014.

[4] D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and distributed reprogramming protocol for wireless sensor networks," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.

[5] Z. Benenson, F. Gartner, and D. Kesdogan, "User authentication in sensornetworks," in Proc. Workshop Sensor Netw., Lecture Notes Informat.Proc.Informatik, 2004, pp. 1–5.

[6] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authenticationin sensor networks," in Proc. Workshop REALWSN, 2005,pp. 20–21.

[7] C. Jiang, B. Li, and H. Xu, "An efficient scheme for user authenticationin wireless sensor networks," in Proc. 21st Int. Conf. AINAW, 2007,pp. 438–442.

[8] I. Butun, "Advanced two tier user authentication scheme for heterogeneous wireless sensor networks," in Proc. 2011 IEEE CCNC, Jan. 2011,pp. 169–171.

[9] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authenticationscheme for wireless sensor networks," in Proc. IEEE Int. Conf.SUTC, vol. 1, Jun. 2006, pp. 244–251.