International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

An Input Based Random Number Generator

Prashant Kumar Yadav, Surjeet Kumar

Abstract: ***The this research article, a neoteric technique is introduced to generate four digit random number for authenticating a user as well as increasing the security of wireless and wired networks by using input based random number generator. An input based random number generator uses number conversion technique and some logical operations. Though the degree of randomness of generated number will not become very high but this hypothesis will increase the security in different areas of computer and sensor network.***

Keywords **: *Random number generator; security; PRNG; TRNG.***

I. INTRODUCTION

The traditional computer network isa network of computers and sensors nodes combined with some type of processing unit and a transceiver module, which may be wired or wireless. The sensors are those devices which have the capability to sense or measure some digital data or analog data, depending upon the type of sensor. Such devices are called sensor nodes; the size and dimensions of a sensor node areas small as these can be easily deployable without putting it in front of human eyes. The applications ofwireless as well as wired sensor networks can be of different kind which includes surveillance system for civilians as well as military people, weather forecasting, detection of any biological system, industrial diagnostics, etc. [1]. Because the sensor networks are rapidly growing day by day and play very crucial role in order to secure our privacy, hence the security of these nodes and data generated by these node must be ensured [2]. Because sensor networks may interact with some personal and sensitive information and operate in very far from us geographically, it is imperative that the security concerns be addressed for securing both the sensor nodes and sensor information [3].In this article a novel structure of Input Based random number generator (IBRNG) is introduced to increase security of wireless sensor networks. Because of inherent resource and computing constraints, security of sensor networks poses different challenges in comparison to our traditional computer network security.

Manuscript published on November 30, 2019.
*Correspondence Author
Prashant Kumar Yadav,Dept. of Computer Science & Engineering Uma Nath Singh Institute of Engineering and Technology Veer Bahadur Singh, Purvanchal University, Jaunpur E-Mail: prashant.yadaw@gmail.com
Surjeet Kumar,Dept. of Computer Applications Uma Nath Singh Institute of Engineering and Technology Veer Bahadur Singh, Purvanchal University, Jaunpur

In the recent days, the security field of computer and sensor network attracts researchers to do something for betterment of the security of computer and sensor network. Thus, the knowledge about this current field of research will provide a great advantage to researchers. Different methods are proposed for increasing security in these networks. Random numbers are much useful for different purposes, such as encrypting and decrypting sensitive information, the analysis of statistical data and for picking up random samples from a very large data set [4]. The most valuable applications of random numbers is in cryptography.

The main role of this research article is to authenticate user as well as increasing security of computer and sensor nodes and network by using input based random number generator to encrypt or decrypt sensitive data. The remaining sections of this research paper are organized as follows:

Section II describes a review of concrned works. Section III presents a freshperspective to increase security in computer network by using an input based random number generator to encrypt or decrypt data or for user authentication and information. Section IV concludes the paper and its uses.

II. RELATED WORK

Basically pins or passwords are generated using one of random number generation techniques. Some of them are as follows:

1. PRNG: It stands for Pseudo-random number generators (PRNGs), are predefined procedures that are capable to deliberately generate long numbers with excellent random properties but sometimes the sequence may repeat [5]. The random numbers generated by such algorithms is generally determined by a fixed number called seed [6]**.** Linear congruential generator (LCG)is the most common PRNG.LCG uses the recurrence to generate numbers which is:

$$X_{n+1} = (ax_n + b) \bmod m$$

where X is the sequence of pseudo-random values
m is modulus , a is multiplier
b is increment, X_n is the seed or initial value.

2. TRNG: The phrase TRNG stands for True Random Number Generator. This is also known as hardware random number generator. It uses physical process, i.e. some specific hardware, to generate random numbers rather than any specific algorithm [7]. Physically, a true random number can be generated with the help of four physical entities i.e. quantum, noise, FRO (free running oscillator) and chaos [8][9]. These entities are used to create some specific true random number generators named as:

(i). Quantum Random Number Generators (QRNG).
(ii). Noise based Random Number Generator (NRNG).
(iii). Free Running Oscillator Random Number Generators (FRORNG).
(iv). Chaos Random Number Generators (CRNG).

The chaos random number generator technique is the most objectionable method for generating random number because this technique uses conceptual mixing of randomness and chaos [7][10]. Some authors have thinking that if a system is hard to describe then it will behave in a random fashion.

All the above techniques generate random numbers according to the measurement of their physical entities, but in our proposed work, we will generate random numbers according to user given input sequence of numbers [9]. Our proposed work is described in the following section.

III. PROPOSED WORK

Following is the procedure used for generating four digit pin number, depending upon the user given input data:

1. User Data Input.
2. Data Processing.
3. Number Generation.

1. User Data Input:

In our proposed system, four types of data sets will be used for four digit number generation. Those data sets are,

(i). Current date, month, and year as, DD:MM:YY.

(ii). Last six digit of card number as $C_1C_2C_3C_4C_5C_6$.

(iii).Current hour, minute and second as, HH:MM:SS.

(iv). User given six digit random number as $U_1U_2U_3U_4U_5U_6$.

2. Data Processing:

The data processing steps involves a set of logical operations on user given input. Those logical operations are as follows:

2.1 On first data set, DDMMYY-

- Convert $(DD)_{10}=(BDD)_2$ where BDD stands for binary equivalent DD (Date).
- Convert $(MM)_{10}=(BMM)_2$
- Convert $(YY)_{10}=(BYY)_2$

Now, perform logical operation on BDD, BMM and BYY as:

BR_1R_2 = (BDD && BMM) || BYY.....eq.(1)

Where BR_1R_2 stands for binary result which will be calculated from above Eq.(1) and further converted into equivalent decimal. Now we will split BR_1R_2 into two equal length binary number as BR_1 and BR_2. Again we will perform the following operation:

$BD_1=BR_1 \oplus BR_2$.

$(BD_1)_2=(D_1)_{10}$.....**eq.(2)**

2.2 On second data set, $C_1C_2C_3C_4C_5C_6$ ----

- Convert $(C_1C_2)_{10}=(BC_1C_2)_2$ where BC_1C_2 stands for binary equivalent C_1C_2.
- Convert $(C_3C_4)_{10}=(BC_3C_4)_2$
- Convert $(C_5C_6)_{10}=(BC_5C_6)_2$

Now, perform logical operation on BC_1C_2 ,BC_3C_4 and BC_5C_6 as:

BR_3R_4 = (BC_1C_2&&BC_3C_4)||BC_5C_6.....**eq.(3)**

Where BR_3R_4 stands for binary result which will be calculated from above Eq.(3) and further converted into equivalent decimal. Now we will split BR_3R_4into two equal length binary number as BR_3 and BR_4. Again we will perform the following operations:

$BD_2=BR_3 \oplus R_4$.

$(BD_2)_2=(D_2)_{10}$.....**eq.(4)**

2.3 On third data set HHMMSS

- Convert $(HH)_{10}=(BHH)_2$ where BHH stands for binary equivalent HH.
- Convert $(MM)_{10}=(BMM)_2$
- Convert $(SS)_{10}=(BSS)_2$

Now, perform logical operation on BHH, BMM and BSS as:

BR_5R_6 = (BHH&&BMM)||BSS.....**eq.(5)**

Where BR_5R_6 stands for binary result which will be calculated from above Eq.(5) and further converted into equivalent decimal. Now we will split BR_5R_6into two equal length binary number as BR_5 and BR_6. Again we will perform the following operations:

$BD_3=BR_5 \oplus R_6$.

$(BD_3)_2=(D_3)_{10}$.....**eq.(6)**

2.4 On fourth data set, $U_1U_2U_3U_4U_5U_6$ ----

- Convert $(U_1U_2)_{10}=(BU_1U_2)_2$ where BU_1U_2 stands for binary equivalent U_1U_2.
- Convert $(U_3U_4)_{10}=(BU_3U_4)_2$
- Convert $(U_5U_6)_{10}=(BU_5U_6)_2$

Now, perform logical operation on BU_1U_2 ,BU_3U_4 and BU_5U_6 as:

BR_7R_8 = (BU_1U_2&&BU_3U_4)||BU_5U_6.....**eq.(7)**

Where BR_7R_8 stands for binary result which will be calculated from above Eq.(7) and further converted into equivalent decimal. Now we will split BR_7R_8into two equal length binary number as BR_7 and BR_8. Again we will perform the following operations:

$BD_4=BR_7 \oplus R_8$.

$(BD_4)_2=(D_4)_{10}$.....**eq.(8)**

3. Number Generation:

In the number generation step, we take input from the output of Eq.(2), Eq.(4), Eq.(6) and Eq.(8), defined in data processing step. By combining the results of above equations we will get our desired random number i.e. four digit pin:

Eq.(2)	Eq.(4)	Eq.(6)	Eq.(8)
D_1	D_2	D_3	D_4

The Following figure (1) depicts the working process of above defined sequences.

IV. CONCLUSION

The basic goal of this research article is to enhance the security of wireless sensor network as well as wired network by introducing input based random number generator to encrypt the data packets as well as information. Input based random number generation is a modified theory in comparison withtraditional random number generation. It provides a method which binds the conceptswith data structures and some logical operations. The authentication key generation process involves three levels of processing. First level includes data conversion of predefineddata and user given data, from decimal number into binary number, second level performssome logical operations such as XOR and OR,

on those data sets and third level convertsthe resulting binary data into decimal numbers to get the desired pin. The given RNGmethod is much fast with good statistical property and hence can be used for both userauthentication and data encryption in short amount of time.

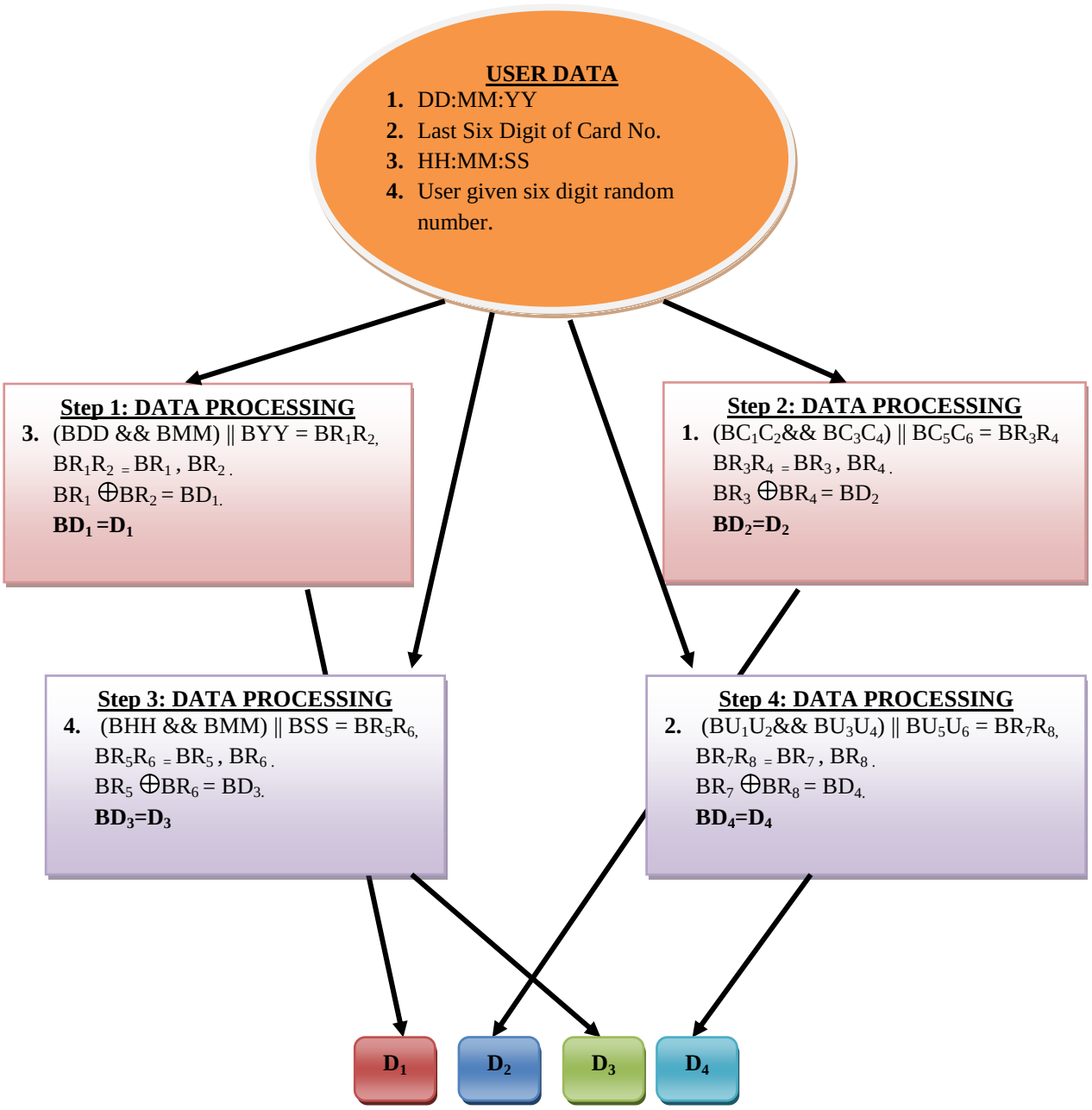

Figure 1: Work flow of sequences used for random number generation

REFERENCES

1. William Bains, "*Random number generation and creativity",* Rufus Scientific, 37 The Moor, Melbourn, Royston, Herts SG8 6ED, United Kingdom, 2008.
2. Florian Neugebauer , Ilia Polian , John P. Hayes, "*S-Box-Based Random Number Generation for Stochastic Computing*", Microprocessors and Microsystems, 2018.
3. Alexei Sibidanov, *"A revision of the subtract-with-borrow random number generators",* Computer Physics Communications, Elsevier, University of Victoria, Victoria, BC, Canada V8W 3P6, 2017.
4. Wu X, Li S. "*A new digital true random number generator based on delay chain feedback loop*", Proc. of IEEE Inter. Symp. on Circuits and Systems (ISCAS), Baltimore, USA, 2017.
5. Young-Seob Jeong, Kyojoong Oh, Chung-Ki Cho, Ho-Jin Choi "*Pseudo Random Number Generation Using LSTMs and Irrational Numbers",* IEEE International Conference on Big Data and Smart Computing, 2018.
6. Pareschi F, Setti G, Rovatti R. "*A fast chaos-based true random number generator for cryptographic applications*", Proc. of 26th Eur. Solid-State Circuit Conf., Montreux, Switzerland, 2006.
7. Guido Di Patrizio Stanchieri, Andrea De Marcellis, Elia Palange Marco Faccio, "*A True Random Number Generator Architecture Based on a ReducedNumber of FPGA Primitives",* International Journal of Electronics and Communications, 2019.
8. S. Gangwar, Prashant K. Yadav, "*Information Security: New Cryptographic Approach*",International Journal of Computational Intelligence Research, 2017.
9. Wieczorek PZ, Golofit K. Dual metastability *"time-competitive true random number generator",* IEEE Trans. on Circuits and Systems I , 2014.

AUTHORS FROFILE

Prashant Kumar Yadav is an Assistant Professor in the department of Computer Science and Engineering, Veer Bahadur Singh Purvanchal University, Jaunpur. He has received his B.Tech. degree in Information Technology from Veer Bahadur Singh Purvanchal University, Jaunpur and M.Tech. in computer Science and Engineering from Gautam Buddha Technical University, Lucknow, Uttar Pradesh, India. He has published five research papers in the field of security. His research interest mainly focuses on Cryptography and steganography, automata theory and network security.

Surjeet Kumar is an Assistant Professor in the department of Computer Applications, Veer Bahadur Singh Purvanchal University, Jaunpur. He has received his M.Sc. degree in computer science from Marathwada University, Aurangabad, Maharastra and Ph.D. from Sri Venkateshwara University, Gajraula, Uttar Pradesh, India. His major research interests are data mining, Cryptography and network security and knowledge discovery. He has published more than twenty seven research articles in international reputed journals and conferences. He has authored a book on Internet and Java Programming.