International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Cellular Automata Based Secured Data Transmission Technique in Wireless Sensor Networks

Pradeep S. Khot, Udaykumar L. Naik

Abstract: ***In Wireless Sensor Network (WSN), CA to based mechanism is used to reduce various optimization problems (energy consumption, network life time, coverage, connectivity, security etc. with simple rules (algorithms). Due to this reason many researchers have concentrated on CA for improving the overall performance in WSN. Therefore, transmission of sensor data over wireless communication channel plays a crucial role using the cryptographic technique. The CA based crypto system is shows high quality of randomness of pattern. We can increase the quality of randomness by implementing the PCA(Programmable Cellular Automata).The sensor data must be encrypted by using Rule based symmetric key Encryption Algorithm(RSE). The proposed technique is based on the encryption algorithm & decryption algorithm by using dynamic cellular automata rules provides good security for sensor data in WSN.***

Keywords: CA-cellular automata, WSN- wireless sensor network, Cryptography, CA Rule.

I. INTRODUCTION

Wireless Sensor Networks:

Wireless sensor networks have been Sensor data must be encrypted before transmission used in many applications [1].The sensors are the main components of a wireless sensor network. A sensor is a very low-cost device which is very small in size, which also has very short communication range, limited processing power and limited memory. Coverage problem is the major challenge in a wireless sensor network (WSN) which needs to be addressed in WSN a set of sensors are deployed in a region of interest (ROI)[2].Security in wireless sensor network use of micro-mechanical system in WSN play very important role in the usability of wireless sensor networks[9]. This system play important role in extraction & analysis of raw data (e.q. temperature, humidity, pressure, seismic event, pressure etc.). Once this raw data is extracted data need to be protected from unauthorized access & need to send to the base(B.S.) through wireless channel sensors node.

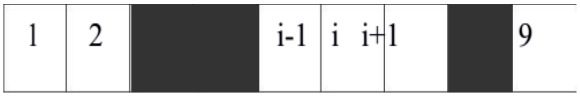
With the change in the rate of generation of data communication, the need of the security & privacy has become a very much need of the communication system. Data must be encrypted so other can't attack on it which is the requirement for communication privacy for communication privacy of the data[8]. Cellular Automata (CA) is one of the most engrossing fields for encrypting sensor data applied in Wireless Sensor Networks (WSN)[4].

Therefore, transmission of sensor data over wireless communication channel plays a crucial role using cryptography.

John Von Neumann proposed the cellular automata [1] ,where we can make use of symmetric key encryption for block cipher in order to provide security for the data transmitted through the sensors in the cellular automata[9].In symmetric one key is used this key is kept secret between sender and receiver. Sensor data is encrypted by using the given key of length of 128 bits [3]. By randomly selecting the rules among 256 different rules we can encrypt the given data. The simple structure of CA has attracted researchers from different fields of interests and has undergone rigorous theoretical and experimental analysis. CA represents a particular class of dynamical systems that enable to describe the evolution of complex systems with simple rules, without using partial differential equations. A CA consists of a regular uniform n- dimensional array of cells where every cell can take values either 0 or 1. Each cell evolves in each time step (discrete steps) depending on some combinational logic on itself and its neighbors. Such a CA is called three-neighborhood CA [5]. The combinational logic is called the rule of the CA. The next state function for a three-neighborhood CA cell can be expressed as follows:

Then,

$a_i(t+1)= f [a_i(t), ai+1(t), a_i(t)]$ where f denotes the local transition function known as a rule of the CA.



three neighbourhoods, two states (0 and 1) CA, the number of all possible uniform rules is 28. Rules are analysed using Wolfram's naming convention[5] from rule number 0 to rule number 255 and can be represented by funsitons. Among the rules, rule 51, rule 60 and rule 102 are used in this paper for encryption algorithm Each CA rule corresponds to a unique combinational logic.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Mr. Pradeep S. Khot*, Department of Computer Science & Engineering, Sanjay Ghodawat University, Atigre Kolhapur, Maharashtra (India)416118. Email: khot.ps@sginstitute.in
Prof. Dr. Udaykumar L. Naik, Department of Electronics & Communication Engineering, KLE"s Dr. M S Seshgiri College of Engineering, Belgavi Karnataka (India) 590008 Email: naikudayl@gmail.com

For example, using Veitch Karnaugh diagram, rule 60 specifies an evolution from the neighborhood configurations to the next state as:
Rule 60: $a_i(t+1)=a_i(t)\oplus a_i\text{-}1(t)$
That is, the next state of the ith is obtained by XORing the present states of the current cell and its left neighbor.

Table-I: State Transition Rule

Rule No.	111	110	101	100	011	010	001	000
51	0	0	1	1	0	0	1	1
60	0	0	1	1	1	1	0	0
102	0	1	1	0	0	1	1	0
150	1	0	0	1	0	1	1	0
153	1	0	0	1	1	0	0	1
195	1	1	0	0	0	0	1	1
90	0	1	0	1	1	0	1	0
204	1	1	0	0	1	1	0	0

Rule 51 : $Z_{t+1}(x)= Z_t (x)$

Rule 60 : $Z_{t+1}(x) = Z_t(x)\oplus Z_t(x-1)$

Rule 150: $Z_{t+1}(x)= Z_t(x-1)\oplus Z_t(x) \oplus Z_t(x+1)$

Rule 102: $Z_{t+1}(x)= Z_t(x+1)\oplus Z_t(x)$

Rule 153: $Z_{t+1}(x)= \overline{Z_t(x+1)\oplus Z_t(x)}$

Rule 195 :$Z_{t+1}(x)= \overline{Z_t(x)\oplus Z_t(x-1)}$

Rule 90: $Zt+1(x)=Zt(x-1)\oplus Z_t(x+1)$

Rule 204: $Zt+1(x)=Z_t(x)$

$[Z_t+n(x)]=[T]_n * [Z_t(x)]$
Rule 60 : $Z_{t+1}(x) = Z_t(x)\oplus Z_t(x-1)$

Rule 150: $Z_{t+1}(x)= Z_t(x-1)\oplus Z_t(x) \oplus Z_t(x+1)$

A total of 256 such rules can be formed for one dimensional, 3 neighbourhood cellular automata with radius r=1[12]. The CA can be categorize in to Additive CA, non-additive CA , periodic boundary CA , null boundary CA, programmable CA, group CA etc.
Where Zt+1(x) is the state of cell i at t+1.
A cellular automaton is called a group cellular automaton if it generates the initial configuration again after a certain number of repetitions by using a specific rule vector [9].
Mathematically,

$[Z_t+n(x)]=[T]n \times [Zt(x)]$,

[T]n=I (I is the identity matrix)
Where n is the order of the group.

There is a total of 256 such rule combinations [9] where 12 is the order of the group. We have used the combinations <11110000> where 1 denote rule 150 and „0" denotes rule 60. The order of the group is 12 for this combination [6].
Limitations of existing methodology:

- The existing system makes use of two different rules for encrypting data and sending the data from sensor nodes to base station through a secured channel.
- Since it makes use of only two rules for encrypting data, it is not secure.
- It can easily face the problem of Brute force attack. Hence, it cannot be used for sending the confidential data.
- In the existing system, the rule dynamic in nature.

Each sensor node I within M, collects observed data ui from sensed data S_i under noisy environment given by,

$$U_i = S_i + n_i$$

Where node i extracts the observed data ui under Additive White Gaussian Noise (AWGN) channel. Once each sensor node extracts the observed data ui, it transmits ui to Cluster head node of the cluster at each time stamp t. The cluster Head node stores the observed data ui in a matrix U [7].U is the matrix where the observed data ui is stored as a block of sensed data under a given time interval t given by; Cellular automata based rules specified with respect to the matrix representation of the input data in this apparocah it is very easy to recognize the input data & we can apply the different rules specified with the rule based encryption standard as given below format.

$$U = \begin{bmatrix} u_1^1 & u_1^2 & . & u_1^N \\ u_2^1 & u_2^2 & . & u_2^N \\ . & . & . & . \\ u_M^1 & u_M^1 & . & u_M^N \end{bmatrix}_{M\times N}$$

Where N is a block of data extracted by each sensor node i under time stamp t. Once this matrix U is obtained, a noise is added to each value uij. Then it is encrypted using group cellular automata rule vector. The non-complemented rules used are 150 and rule 60[8]. Logical expression for both the rules is described by equations respectively. These two rules are used for each 8-bit binary number obtained number from matrix U in the following fashion: <11110000> where „1" denotes rule 150 and 0" denotes rule 60.

- The proposed system consists of a source which is any sensor node deployed in a geographical region.
- The source that is Wireless Sensor Network collects the raw data from the region.
- The Wireless Sensor Network makes use of MEMS (Micro Mechanical System).
- The Micro Mechanical System extracts the raw data from the geographical region.
- This collected raw data is encrypted before it is sent through the channel.

- The data is encrypted using symmetric key block cipher cryptography technique.
- Different Cellular Automata rules are performed on data to encrypt the data

To make it more secure the proposal consists of a combination of 4 CA rule on a stream of 8 bits.

The stream of 8 bits is divided into a group of 2,3,2,1 bits respectively. Then the CA rules are applied to those groups of bits. We have formed 4 combinations of different CA rules. These 4 rules will change periodically after every 4 packets of data. [9] The encryption of given data consists of two iterations for every combination for the encrypted data will be formed Similarly, the decryption also combination of a rule & original data will be retrieved form this.

The combination of rules used in the proposed system are as follows:

i. 51 102 195 153

ii. 153 150 90 204

iii. 51 150 102 153

iv. 60 150 195 57

(Combination i: For 1st two bits apply rule 51, for next three bits apply rule 102, for next two bits apply rule 195 and remaining one bit apply rule 153 using null boundary CA principle.

Combination ii: For 1st two bits apply rule 153, for next three bits apply rule 150, for next two bits apply rule 90 and remaining one bit apply rule 204 using null boundary CA principle.

Combination iii: For 1st two bits apply rule 51, for next three bits apply rule 150, for next two bits apply rule 102 and remaining one bit apply rule 153 using null boundary CA principle.

Combination iv: For 1st two bits apply rule 60, for next three bits apply rule 150, for next two bits apply rule 195 and remaining one bit apply rule 51 using null boundary CA principle.)

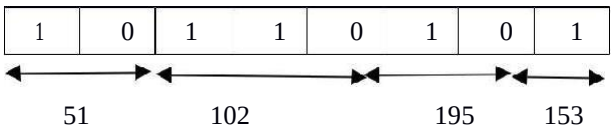
Let us consider the decimal number 181 to be encrypted,
Implementation:

Binary representation of 181 is,

1 0 1 1 0 1 0 1

After this the combination of rules are applied on this binary representation:

Combination 1:

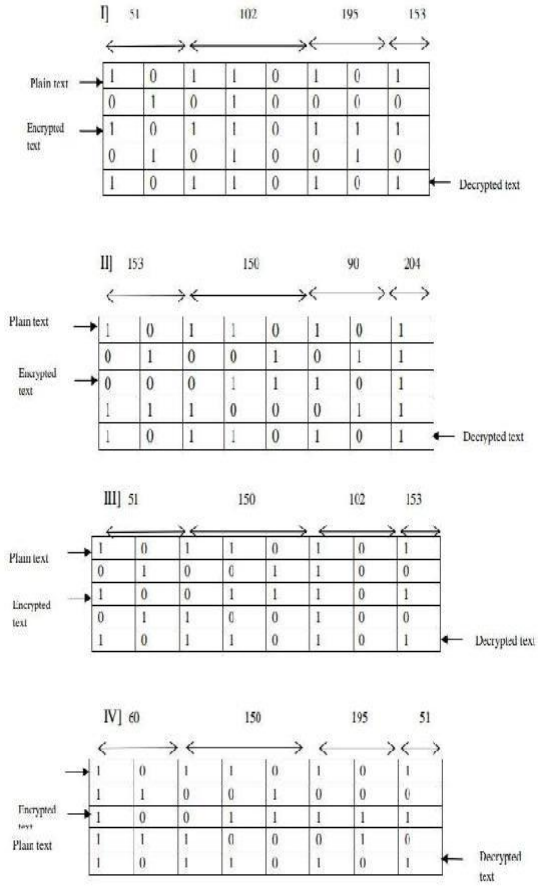


After applying this combination for 2 times

Advantages:

Using simple Cellular automata mathematical model to implement the complex system.

- The encryption and decryption is performed using simplest technique that is EXOR which generates highly secured encrypted data
- Sensor nodes require less memory. Hence, our proposed schema plays a more efficient role in terms of memory and computational complexities.
- The schema is resistant to various cryptanalysis attacks like Brute-force attack its variants.
- The schema is also resistant to linear cryptanalysis attacks
- Strong mathematical model in the field of wireless sensor networks security.



Algorithm for CA-RSE(Rule based symmetric key algorithm)

- Encryption Algorithm:-

Input: Raw data collected by the sensor nodes.

Output: Encrypted data

Step1: Get the raw data from the sensor node.

Step2: Convert the data into the 8-bit binary number.

Step3: Perform encryption using the following combinations CA rules: -

Combination1: For 1st two bits apply rule 51, for next three bits apply rule 102, for next two bits apply rule 195 and remaining one bit apply rule 153 using null boundary CA principle.

Combination2: For 1st two bits apply rule 153, for next three bits apply rule 150, for next two bits apply rule 90 and remaining one bit apply rule 204 using null boundary CA principle.

Combination3: For 1st two bits apply rule 51, for next three bits apply rule 150, for next two bits apply rule 102 and remaining one bit apply rule 153 using null boundary CA principle.

Combination4: For 1st two bits apply rule 60, for next three bits apply rule 150, for next two bits apply rule 195 and remaining one bit apply rule 51 using null boundary CA principle.

Step4: Convert the data into the decimal form and store the data.

Step5: Apply the steps 2 and 3 for each value of original data.

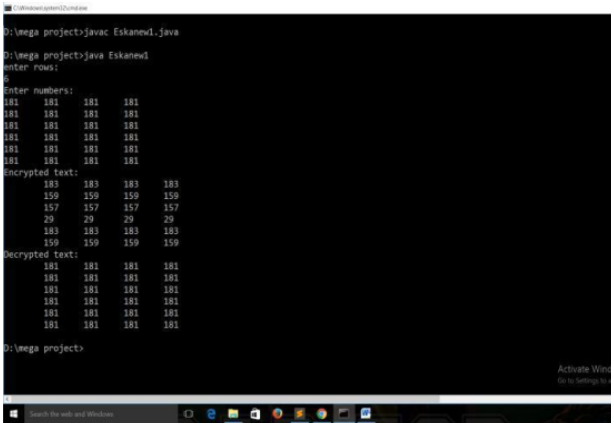
Step6: Send the encrypted data to the Base Station.

Decryption Algorithm
Input: Encrypted data from the Base Station.
Output: Decrypted data
Step1: Convert the data into the 8-bit binary number.

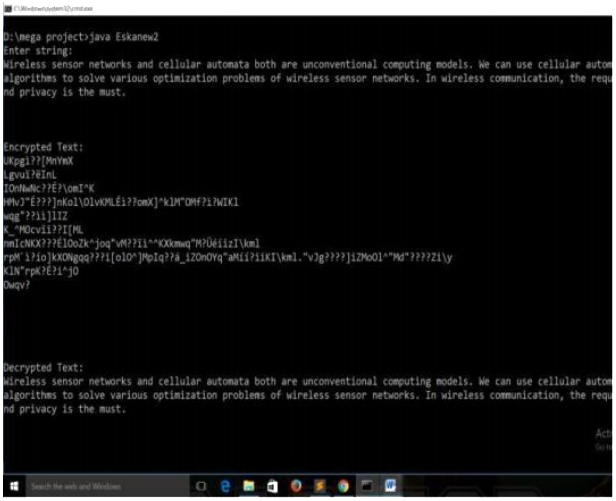
Step2: Perform decryption using the following combinations CA rules:-
Combination1: For 1st two bits apply rule 51, for next three bits apply rule 102, for next two bits apply rule 195 and remaining one bit apply rule 153 using null boundary CA principle.
Combination2: For 1st two bits apply rule 153, for next three bits apply rule 150, for next two bits apply rule 90 and remaining one bit apply rule 204 using null boundary CA principle.
Combination3: For 1st two bits apply rule 51, for next three bits apply rule 150, for next two bits apply rule 102 and remaining one bit apply rule 153 using null boundary CA principle.
Combination4: For 1st two bits apply rule 60, for next three bits apply rule 150, for next two bits apply rule 195 and remaining one bit apply rule 51 using null boundary CA principle.
Step4: Convert the data into the decimal form and store the data.
Step5: Apply the steps 2 and 3 for each value of encrypted data.
Step6: Output the decrypted data.

Results:
Matrix representation of numeric input data & encryption in matrix form. In the given matrix we have taken input as a decimal data represented in matrix form taken from[5]. In the wireless sensor network sensor dat is first encrypted in the head(node) master node. The given result shows how secrecy of the real time data is being preserved with respect to the given input data after applying the CA Rules in dynamic way. This type of cryptosystem shows very different kind of randomness by selecting the different CA rules which is gives more powerful results with respect to other older methods. In the first part of the result of encryption shown in matrix form, after decryption again original data received in matrix form.

Result 1: Where input is given in the Matrix format



Result 2: Where input is given as a text message and encrypted in the text format



II. CONCLUSION:

We have implemented CA based rule with dynamic approach where rules will be changed dynamically for encryption of the data also dynamic rules were applied for the decryption of the encrypted data. The result shows it is very difficult to predict the rules which are changing dynamically so Cellular Automata plays important role for secured data transmission in the wireless Sensor Network we have have shown with results.

REFERENCES:

1. John von Neumann, Theory of Self Reproducing Automata, edited and completed by Burks, AW. (Ed.), Univ. of Illinois press, London, 1966

2. Shalimur Choudhury, Cellular Automata and Wireless Networks, Springer International Publication 2017.
3. Satyabrata Roy, Subrata Nandi, Jayanti Dansana, Prasant Kumar Pattnaik Application of Cellular Automata in Symmetric Key Cryptography International Conference on Communication and Signal Processing April 3-5 2014,In Communication and Signal Processing, April 3-5, 2014, India.
4. Indrajit Banerjee, Sukanta Das, Hafizur Rahaman and Biplab K Sikdar, "C A Based Sensor Node Management Scheme: An Energy Efficient Approach"; in International Conference on Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007, pp: 2795-2798
5. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in CCS "02: Proceedings of the 9th ACM conference on Computer and communications security. ACM Press, 2002, pp. 41–47.
6. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J.; SPINS: Security protocols for sensor networks. J. Wireless Nets. 8, 5 (Sept. 2002) pp. 521–534.
7. L. Eschenauer and V. D. Gligor, "A keymanagement scheme for distributed sensor networks," in CCS "02: Proceedings of the 9th ACM conference on Computer and communications security. ACM Press, 2002, pp. 41–47.
8. P. Anghelescu, E. Sofron, C. Rlncu, V. lana, "Programmable cellular 200S, vol. 2, pp. 351-354.
9. Debdeep Mukhppadhyay, "Design and analysis of cellular automata based cryptographic algorithms", Doctoral thesis, Indian Institute of Technology, Kharagpur, 2007.

AUTHORS PROFILE

Pradeep Khot, received his B.E. degree in Computer Engineering from Mumbai University, Mumbai, India in 2007 and M. Tech. Degree in Computer Science and Engineering from SRM University, Chennai, Tamilnadu State, India in 2013. Pradeep Khot is currently pursuing the Ph.D. degree in Computer Science and Engineering with the Visvesvaraya Technological University (VTU) Belagavi, Karnataka State, India. With a broader scope of Cellular automata based in Wireless Sensor Networks, his main field of interest is Cellular automata, Wireless Sensor Networks, System Programming and Data analytics. He has presented papers in various National & International conferences.

Dr. Udaykumar Naik, is currently Professor, Electronics and communication Engineering department at KLE DRMSSCET, Belagavi, Karnataka, India.Prof. Udaykumar Naik received B.E. degree in Electronics and Communication Engineering, from the Karnataka University, Dharwar, India in 1988, M.Tech. degree in Digital Electronics and Advanced Communications, from National Institute of Technology-Karnataka (NIT-K), Surathkal, India, in 1996 and Ph.D. degree in Electronics Engineering, Shivaji University, Kolhapur, India, in 2014. His research interests include indoor wireless location technologies, Antenna design and wireless systems modeling and design. He is the author of 15 research papers in peer reviewed reputed international journals and conferences. He has over 25 years of teaching experience. Professor Udaykumar Naik is a Fellow of the Institution of Electronics and Telecommunications Engineers, New Delhi, India.