Symmetric Key Security Implementation Using 2D Cellular Automata

Prof. P.S. Khot*[1], Rachana R. Kulkarni[2], Aishwarya V. Bhosale[3] , Nasreen Kachhi[4], Sonal Budhwani[5]

*[1]*Assistant Professor CSE, Shivaji University, Kolhapur , Maharashtra, India*

[2, 3, 4, 5]*BE-CSE, Shivaji University, Kolhapur , Maharashtra, India*

***Abstract*: Wireless sensor networks and cellular automata both are unconventional computing models. We can use cellular automaton based localized algorithms to solve various optimization problems of wireless sensor networks. In wireless communication, the requirement of security and privacy is the must. The usage of cryptography characteristics of cellular automata is still not much explored in WSN. Hence we present a symmetric key cryptography technique of block cipher using cellular automata rules applied to sensor data. Based on CA state transitions certain fundamental transformations are defined which are block ciphering functions of the proposed enciphering scheme. Different rule configurations are used to form group cellular automata that would be used for encryption and decryption. This algorithm can be used to send any confidential data that is captured by WSN for example in military application.**

***Keywords:* CA-cellular automata, symmetric key cryptography, WSN- wireless sensor network**

I. INTRODUCTION

A. WSN

Due to the advancement of sensor communication technology, wireless sensor networks have been used in many applications. [1] The sensors are the main components of a wireless sensor network. A sensor is a very low-cost small device that has limited battery power, short communication range, limited processing power and limited memory. A wireless sensor network (WSN) forms a distributed information processing system that gathers and processes different attributes of the network, for example, humidity, temperature, etc. A traditional wireless sensor network also includes single or multiple base stations that gather data from the sensors. Each sensor of a sensor network has a sensing radius and a communication radius. A sensor can sense or monitor the region that falls within its sensing radius and communicates with other sensors that are within its communication radius. The sensors with whom a sensor can communicate are called the neighbors of the sensor. A typical wireless sensor network consists of hundreds, or even thousands, of sensors[2]. These sensors are deployed in the monitored area and typically centralized controls are absent on these sensors. These nodes are also unattended due to typical applications of sensor networks, it is not possible to have a human operator to directly attend to individual sensors. The sensors use each other (multi-hop communication) to route the information that they sense to the base stations for further processing.

B. CELLULAR AUTOMATA

Cellular automata [1] is an infinite lattice of cells capable of storing one bit at a time. Each cell has a capability to transit into a new state depending upon its own state and that of its neighbor. Formally a cellular automaton is defined as three-tuple (S, T, N) where S is a finite and non-empty set of states, T is the finite and non-empty set of transition rules and N is the non-empty and finite set of neighborhood cells. 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. [4] The combinational logic is called the rule of the CA.

In case of 1-D, three neighborhoods, two states (0 and 1) CA, the number of all possible uniform rules is 28. These rules are enumerated using Wolfram's naming convention[5] from rule number 0 to rule number 255 and can be represented by a 3-variable Boolean function. Among the rules, rule 51, rule 60 and rule 102 are used in this paper to design the encryption algorithm. [2]

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

Table: Example of next state transition rule

The corresponding rules are called complemented rules.

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

Rule 60 : $Z_{t+1}(x) = Z_t(x) \oplus Z_t(x\text{-}1)$
Rule 150 : $Z_{t+1}(x)= Z_t(x\text{-}1) \oplus Z(x) \oplus Z(x+1)$
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 : $Z_{t+1}(x)= \overline{Z_t(x) \oplus Z_t(x\text{-}1)}$
Rule 90 : $Z_{t+1}(x)=Z_t(x\text{-}1) \oplus Zt(x+1)$
Rule 204 : $Z_{t+1}(x)= Z_t(x)$

A cellular automata [1] is an infinite collection of cells made of mono-stable multi-vibrators. Each cell transits into a new state depending upon transition function that maps each cell's present state into a new state based on its currents states of neighbors and that of its own. Here we can consider an example of two states (0 and 1) and 3 neighborhood one dimensional CA.

The first row displays three possible neighboring cell values at timestamp t. 2nd to 6th row gives the equivalent state of x th cell at timestamp t+1. Suppose we consider an array of n cells with degree n-1, and its cell value is a0, a1, a2,.., an-1, where

aj ={0,1}. Let us consider, Pt(X) and Pt+I(X) describe the CA state at t - th and (t+l) - th clock cycle. T is the characteristic matrix of CA, which contains rules of all cells. The characteristic matrix T is a n x n (for n cells) square matrix constructed according to the rule of each cell in a CA. The i-th row assigns a rule applicable to the i-th cell. If i-th cell's next state rely on a certain cell, then the latter's corresponding position in matrix T is set to '1', otherwise, it is set to '0'.

Mathematically, the next state transition can be represented as follows:

[Zt+1(x)]=[T]*[Zt(x)]

A total of 256 such rules can be formed for one dimensional, 3 neighborhood cellular automata with radius r=1[12]. The CA‟s can be of many types viz. Additive, non- additive, periodic boundary, null boundary, programmable CA[4], group CA etc.

Each sensor[1] node I within M, collects observed data ui from sensed data si under noisy environment given by,

Ui = si + ni

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[2] 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;

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

II. SYSTEM ARCHITECTURE

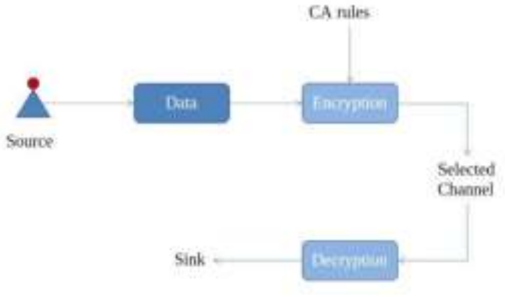


Fig : Architecture of system

The architecture of System :

- 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.

III. IMPLEMENTATION

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.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

Let us consider the decimal number 181 to be encrypted, Binary representation of 181 is,

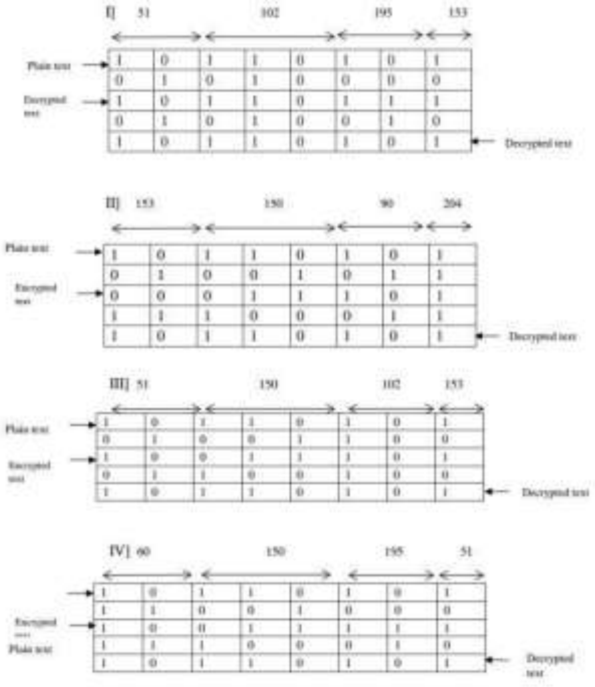
1	0	1	1	0	1	0	1

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

Combination 1:

1	0	1	1	0	1	0	1

51 102 195 153



1	0	1	1	0	1	0	1
0	1	0	1	0	0	0	0
1	0	1	1	0	1	1	1
0	1	0	1	0	0	1	0
1	0	1	1	0	1	0	1

1	0	1	1	0	1	0	1
0	1	0	0	1	0	1	1
0	0	0	1	1	1	0	1
1	1	1	0	0	0	1	1
1	0	1	1	0	1	0	1

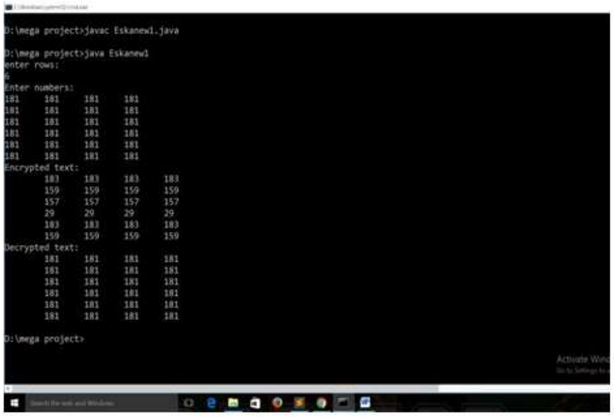
1	0	1	1	0	1	0	1
0	1	0	0	1	1	0	0
1	0	0	1	1	1	0	1
0	1	1	0	0	1	0	0
1	0	1	1	0	1	0	1

1	0	1	1	0	1	0	1
1	1	0	0	1	0	0	0
1	0	0	1	1	1	1	1
1	1	1	0	0	0	1	0
1	0	1	1	0	1	0	1

IV. ADVANTAGES OF OUR SCHEMA

- Using simple Cellular automata[2] 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
- 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.

Matrix form of encrypted and decrypted data is shown as follows:-

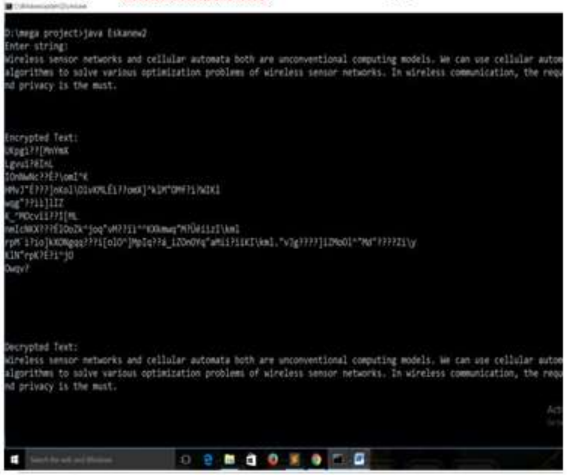


```
D:\mega project>javac Eskanew1.java

D:\mega project>java Eskanew1
enter rows:
6
Enter numbers:
181     181     181     181
181     181     181     181
181     181     181     181
181     181     181     181
181     181     181     181
181     181     181     181
Encrypted text:
        183     183     183     183
        159     159     159     159
        157     157     157     157
        29      29      29      29
        183     183     183     183
        159     159     159     159
Decrypted text:
        181     181     181     181
        181     181     181     181
        181     181     181     181
        181     181     181     181
        181     181     181     181
        181     181     181     181

D:\mega project>
```

String input data,encrypted form & decrypted form



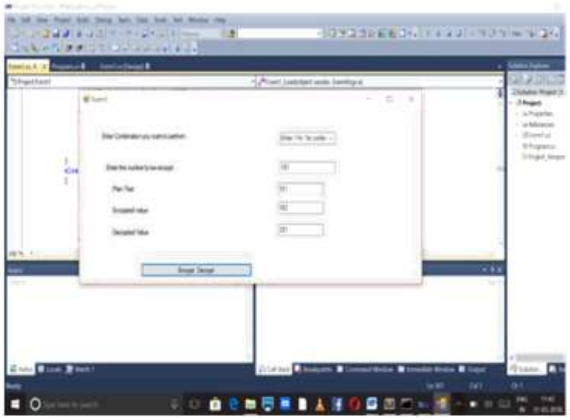
```
D:\mega project>java Eskanew2
Enter string:
Wireless sensor networks and cellular automata both are unconventional computing models. We can use cellular autom
algorithms to solve various optimization problems of wireless sensor networks. In wireless communication, the requ
nd privacy is the must.



Encrypted Text:
UKpgi??[MnYmK
Lgvul?ÉIxL
IOnNwNc??É?\omI^K
HMvJ"É???]nKol\OlvKMLÉi??omX]^klM"OMF?i?WIKl
wqg"??ii]1IZ
K_"MOcvii??I[ML
nmIcNKX???É1OoZk"joq"vM??ii""KXkmwq"M?ÛWiizI\kml
rpM`i?io]kXONgqq???i[olO^]MpIq??á_iZOnOYq"aMii?iiKI\kml."v1g????]iZMoOl^"Md"????Zi\y
KlN"rpK?É?i"jO
Owqv?



Decrypted Text:
Wireless sensor networks and cellular automata both are unconventional computing models. We can use cellular autom
algorithms to solve various optimization problems of wireless sensor networks. In wireless communication, the requ
nd privacy is the must.
```



Enter Combination you want to perform [illegible]

Enter the number to be encrypt 181

Plain Text 181

Encrypted value 102

Decrypted Value 181

V. FUTURE SCOPE

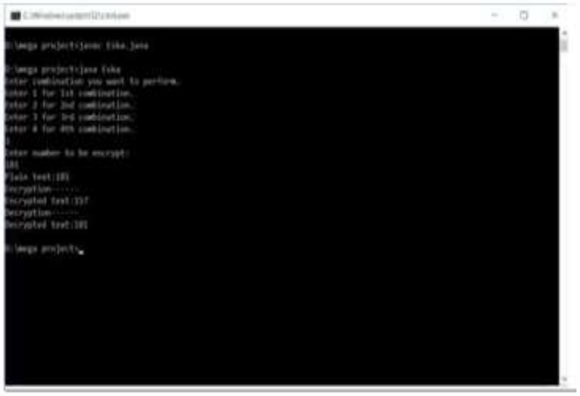
In a wireless sensor network scenario, the sensor data are encrypted using symmetric key block cipher encryption technique and transmits the encrypted data to the Base Station. The proposed methodology shows better performance in terms of implementation and generation of cipher text.[11]

The proposed methodology is resistant to brute force attack and linear cryptanalysis attacks. It also reduces the memory space in the Wireless Sensor Network.

This work might be extended in distributed clustering algorithms where data is encrypted using an asymmetric key. Different keys are used on the sender side and the receiver side for performing encryption and decryption.

In future this work can be extended for security in Underwater Wireless sensor networks (UWSN) where the UWSN is used to monitor the different aspects of seas, lakes etc. where the sensors are either static or dynamic in nature so the security's very important concern in UWSN and it is relatively very new filed of WSN many NAVAL base application demands UWSN

VI. RESULT



```
D:\mega project>javac fike.java

D:\mega project>java fike
Enter combination you want to perform.
Enter 1 for 1st combination.
Enter 2 for 2nd combination.
Enter 3 for 3rd combination.
Enter 4 for 4th combination.
1
Enter number to be encrypt:
181
Plain text:181
Encryption------
Encrypted text:157
Decryption------
Decrypted text:181

D:\mega project>
```

REFERENCES

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

[2]. S. Nandi, B. K. Kar, Pabitra Pal Chaudhuri, 'Theory and applications of cellular automata in cryptography", IEEE Transactions on Computers, 43(12), 1994, pp. 1346-1356.

[3]. Stephen Wolfram, A new kind of science, Wolfram Media Inc., ISBN: 1-57955-00S-S, 2002.

[4]. 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, India.

[5]. Petre Anghelescu, Programmable Cellular Automata Encryption Algorithm Implemented in Reconfigurable Hardware, International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems Vol. 2, No. 2.

[6]. 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.

[7]. 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.

[8]. Tygar, J.; SPINS: Security protocols for sensor networks. J. Wireless Nets. 8, 5 (Sept. 2002)

[9]. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and P. Anghelescu, E. Sofron, C. Rlncu, V. lana, "Programmable cellular 200S, vol. 2, pp. 351-354.

[10]. Debdeep Mukhppadhyay, "Design and analysis of cellular automata based cryptographic algorithms", Doctoral thesis, Indian Institute of Technology, Kharagpur, 2007.

[11]. E. Jamro, P. Russek, A. Dabrowska-Boruch, M. Wielgosz, "The implementation of the customized, parallel architecture for a fast word-match program", International Journal of Computer Systems Science and Engineering, Volume 26, Issue 4, pp. 285-292, 2011.

[12]. Menezes, P. Oorschot, and S. Vanstone. Handbook of applied cryptography, CRC Press, ISBN: 0-8493-8523-7, 1996