Markovian Process and Novel Secure Algorithm for Big Data in Two-Hop Wireless Networks

K. Thiagarajan,
Department of Mathematics,
PSNA College of Engineering and Technology,
Dindigul, India.

A. Veeraiah,
Department of Mathematics,
K. L. N College Engineering and Technology,
Madurai, India.

K. Saranya,
Department of Information Technology,
PSNA College of Engineering and Technology,
Dindigul, India.

B. Sudha,
Department of Mathematics
SRM University,
Chennai, India.

***Abstract*—This paper checks the correctness of our novel algorithm for secure, reliable and flexible transmission of big data in two-hop wireless networks using cooperative jamming scheme of attacker location unknown through Markovian process. Big data has to transmit in two-hop from source-to-relay and relay-to-destination node by deploying security in physical layer. Based on our novel algorithm, the nodes of the network can be identifiable, the probability value of the data absorbing nodes namely capture node C, non-capture node NC, eavesdropper node E, in each level depends upon the present level to the next level, the probability of transition between two nodes is same at all times in a given time slot to ensure more secure transmission of big data. In this paper, maximum probability for capture nodes is considered to justify the efficient transmission of big data through Markovian process.**

***Keywords*—big data; two-hop transmission; security in physical layer; cooperative jamming; energy balance; Markov process**

I. INTRODUCTION

Wireless networks have become an indispensable part of our daily life, used in many applications where the amount of data is very massive and is called big data [2]. Security is a critical issue in wireless applications of big data, when people rely heavily on wireless networks for transmission of important/private information. Therefore, the ability to share secret information reliably in the presence of eavesdroppers is extremely important in the environment of big data [8]. Cryptographically enforced security is not sufficient to provide everlasting security in handling huge data size due to increased attacks by capturing its keys [10]. So security in physical layer is used to retain the everlasting security in big data as it prevents eavesdroppers and malicious nodes from capturing the data [11].

The term big data is high volume, variety, velocity and veracity. The amount of data increases faster and quicker in big data. According to a report published by IBM in 2012 [4], 90 percent of the data in the world was generated in the previous two years. As a consequence, the concept of the big data has emerged as a widely recognized trend, which is currently attracting much attention from government, industry, and academia [3]. It is essential to have data transfer mechanism, two-hop transmission from source-to-relay and relay-to-destination node plays a vital role in secure and energy efficient transmission of big data.

Cooperative communication helps in exploiting spatial diversity to enhance the quality of wireless links. The characteristics of cooperative networks are shown in Fig. 1. Security can be improved by cooperative networks by having the information content minimum to the eavesdropper nodes of the expected destination and having maximum to the relay node of the expected destination [6]. The recently proposed cooperative network technique is cooperative jamming to improve physical layer security in the presence of eavesdroppers [5]. In wireless communication, occurrence of interference is considered redundant. This fetches the work of

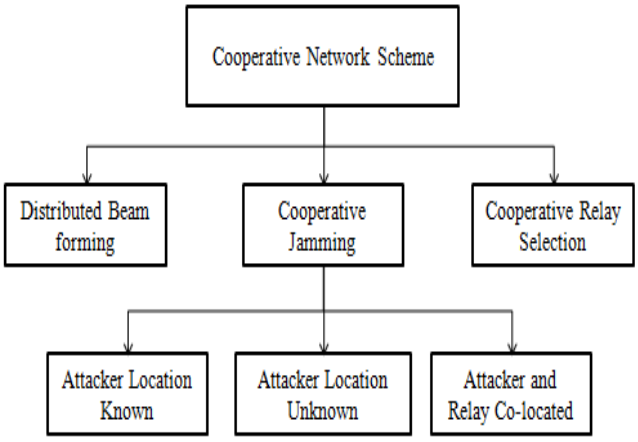


Fig. 1. Classification of cooperative network scheme

cooperative jamming for flexible and efficient wireless network technique to confuse the eavesdroppers and making the source message uncertain by generating friendly jamming signal to the eavesdroppers. In this, if the data has to be transmitted from source S to destination D, jamming signal will be emitted by the relay nodes to have the secure communication and to prevent the eavesdroppers of location

unknown from capturing the data. In our novel algorithm, cooperative jamming scheme is considered [9].

The remainder of this paper is organized as follows. Section II highlights the overview of novel secure algorithm [9]. Section III discuss about the Markovian implementation on the proposed algorithm. We conclude our paper by experimental result verification for the proposed algorithm.

II. Overview of Novel Secure Algorithm

The Fig. 2 shows the overview diagram for the novel secure transmission algorithm which is clearly explained in our previous paper [9], in which we want to select the data transmitting region which is of side length l followed by segmenting the selected region of equal size. Then we have to determine the probability value for each node which is detailed in our paper [9]. Based on probability value for capture node we want to classify the transmission as secure data transmission and unsecure data transmission. If it is secure data, transmit the data in two-hop. If it is unsecure data transmission, transmit the data in two-hop by adopting cooperative jamming technique to prevent eavesdroppers from capturing the data. The jammers should be of distance r away from the intended destination. We assume that only one end-to-end transmission can be conducted in one time slot.

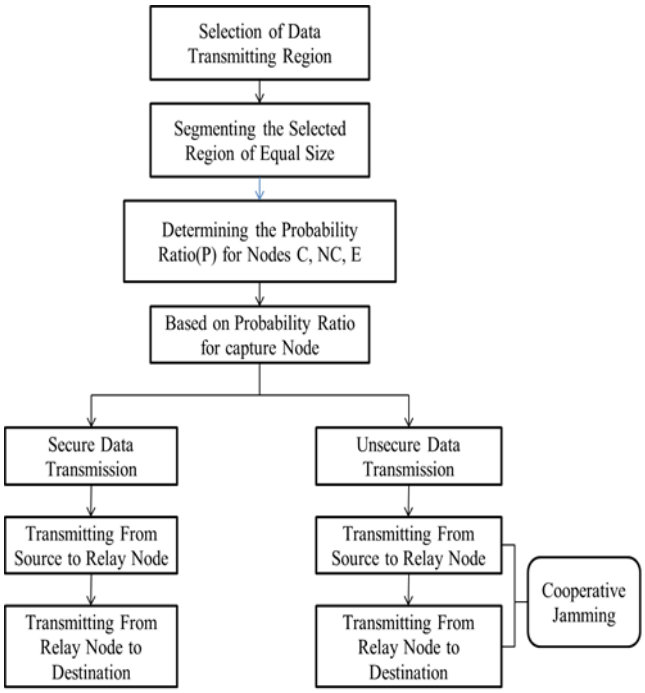


Fig. 2. Overview of proposed algorithm

III. Discussion of Markovian Process on Proposed Algorithm

A. Markov Model

Markovian model is a model of representing different resident states of a system, and the transitions between the different states [7]. Similarly in the algorithm which is proposed in [9] have different states of the system namely source, capture, non-capture, eavesdropper, ideal and destination nodes for having transition between different states to have secure transmission of big data.

B. Stochastic Process

Let S be a sample space of a stochastic experiment. A stochastic process is a mapping X which assigns to every outcome s ϵ S a real valued function of time x (t, s) (i.e) X (s) = x (t, s). The family or ensemble of all such time functions is denoted by X (t, s) and is called a stochastic process [7]. The novel secure transmission algorithm which we have proposed in [9] satisfies with the stochastic process in which the behavior of the system varies randomly with time and space for each end-to-end transmission of big data.

C. Markov Process

Markov process is the simplest generalization of independent processes which allow the outcome at any instant to depend only on the outcome that precedes it and not on the earlier ones [7]. As per our algorithm, a stochastic process X(t) is said to be a Markov process if for any $t_1 < t_2 < t_3 <\ldots\ldots< t_n$

$$P[X(t_n) \leq x_n \mid X(t_{n-1}) = x_{n-1}, X(t_{n-2}) = x_{n-2}, \ldots\ldots X(t_1) = x_1]$$

$$= P [X(t_n) \leq x_n \mid X(t_{n-1}) = x_{n-1}]$$

(i.e.) the conditional distribution of X (t_n) for given values of X (t_1), X (t_2), …,X(t_{n-1}) depends only on present state X(t_{n-1}).

D. Markov Chains

Based on our algorithm in [1], let X (t) be a Markov process with states X (t_r) = X_r , $t_0 < t_1 < \ldots.. < t_n$. If for all n,

$$P [X_n = a_n \mid X_{n-1} = a_{n-1}, X_{n-2} = a_{n-2}. \ldots., X_0 = a_0]$$

$$= P \{X_n = a_n \mid X_{n-1} = a_{n-1}]$$

then the sequence of random variables {Xn} is called a Markov chain, n=0,1,2… Here a_1, a_2…a_n are called the states of Markov chain [7].

E. Transition Probabilities

P $\{X_m = a_i\} = P_i (m)$ represents the probability that at time $t=t_m$, the system occupies the state a_i, P $[X_n = a_j \mid X_m = a_i] = P_{ij}(m, n)$ represent the probability that system goes into state a_j at $t=t_n$ given that it was in state ai at $t=t_m$. The numbers $P_{ij}(m,n)$ represent the transition probabilities of the Markov chain from state a_i at time tm to a_j at time t_n [7].

F. Markov Transition Diagram

The state of transmitting the data transition probabilities from i^{th} state to the j^{th} state by an arc labeled as P_{ij} is the representation of Markov state transition diagram is shown in Fig. 3.

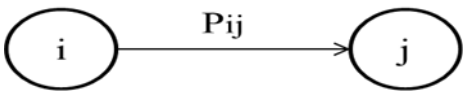


Fig. 3. Model transition diagram

G. Markov Transition Matrix

$$P = \begin{matrix} \\ 1 \\ 2 \\ \cdots \\ m \end{matrix} \begin{matrix} \begin{matrix} 1 & 2 & \cdots & n \end{matrix} \\ \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{bmatrix} \end{matrix}$$

The square matrix represents the number of states in rows and columns [7]. The rows are represents the nodes from which the data is transmitting. The columns are representing the nodes to which the data is received. The sum of the probability in each row must equals to 1.

IV. Experimental Result Verification

Discrete time and space Markov chain is used to verify our novel secure transmission algorithm. As in our previous work [9] and with the reference from [1, 12] secure transmission of big data through binary probability evaluation value in Table I. Based on that result we are going to verify using Markov process.

TABLE I. Binary Evaluation to Verify the Transmission

C	NC	E	Transmission
0	0	0	No Action
0	0	1	Unsecure
0	1	0	Unsecure
0	1	1	Unsecure
1	0	0	Secure
1	0	1	Secure/Unsecure
1	1	0	Secure/Unsecure
1	1	1	Secure/Unsecure

The verification process is based on minimum probability is for the non-capture and eavesdropper nodes. The maximum probability is for the capture node to prove the secure transmission of big data. If the probability is Maximum for the malicious nodes it can be prevented to capture the big data by cooperative jamming [9].

A. Case I

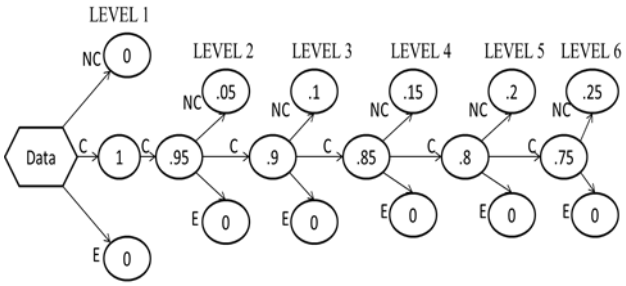
With eavesdroppers E=0, sum of the values for capture node C, non-capture node NC is 1. The verification result to this case is discussed in Markov Principle as transition table in Table II, transition diagram in Fig. 4 and by transition matrix.

a) Probability Values Distribution Table

TABLE II. Transition Table (Case I)

C	NC	E
1	0	0
0.95	0.05	0
0.9	0.1	0
0.85	0.15	0
0.8	0.2	0
0.75	0.25	0
……N-1, N		

b) Markov Transition Diagram



…… LEVEL N-1, LEVEL N

Fig. 4. Transition diagram (case I)

c) Markov Transition Matrix

LEVEL 1

$$\begin{matrix} \\ C \\ NC \\ E \end{matrix} \begin{matrix} \begin{matrix} C & NC & E \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

LEVEL2

$$\begin{matrix} \\ C \\ NC \\ E \end{matrix} \begin{matrix} \begin{matrix} C & NC & E \end{matrix} \\ \begin{bmatrix} 0.95 & 0.05 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

LEVEL 3

$$\begin{matrix} \\ C \\ NC \\ E \end{matrix} \begin{matrix} \begin{matrix} C & NC & E \end{matrix} \\ \begin{bmatrix} 0.9 & 0.1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

LEVEL 4

$$\begin{matrix} \\ C \\ NC \\ E \end{matrix} \begin{matrix} \begin{matrix} C & NC & E \end{matrix} \\ \begin{bmatrix} 0.85 & 0.15 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

LEVEL 5

$$\begin{matrix} \\ C \\ NC \\ E \end{matrix} \begin{matrix} \begin{matrix} C & NC & E \end{matrix} \\ \begin{bmatrix} 0.8 & 0.2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

LEVEL 6

$$\begin{matrix} \\ C \\ NC \\ E \end{matrix} \begin{matrix} \begin{matrix} C & NC & E \end{matrix} \\ \begin{bmatrix} 0.75 & 0.25 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{matrix}$$

……LEVEL N-1, LEVEL N

⇒ COMPLETE MARKOV CHAIN

$$\begin{matrix} C \\ NC \\ E \end{matrix} \begin{bmatrix} 1 & 0.95 & 0.9 & 0.85 & 0.8 & 0.75 & \cdots & N-1 & N \\ 0 & 0.05 & 0.1 & 0.15 & 0.2 & 0.25 & \cdots & N-1 & N \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & N-1 & N \end{bmatrix}$$

Since the eavesdropper probability value is zero in the above case, obviously the big data transmission is more secured and the novel algorithm [9] satisfies with this case.

B. Case II

With non-capture node NC=0, and summation of capture and eavesdropper node is 1 (i.e., $\sum (C_i + E_i = 1)$. This case is verified in the following Table III as transition table, in Fig. 5 as transition diagram as well as in transition matrix of Markov principle.

a) Probability Value Distribution Table

TABLE III. Transition Table (Case II)

C	NC	E
1	0	0
0.95	0	0.05
0.9	0	0.1
0.85	0	0.15
0.8	0	0.2
0.75	0	0.25
……..N-1, N		

b) Markov Transition Diagram

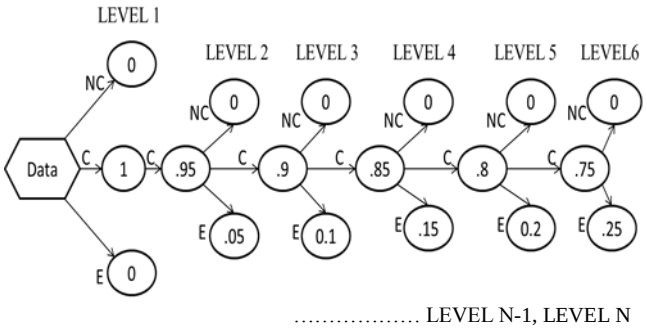


Fig. 5. Transition diagram (case II)

c) Markov Transition Matrix

$$\text{LEVEL 1}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL2}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.95 & 0 & 0.05 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.9 & 0 & 0.1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

$$\text{LEVEL 4}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.85 & 0 & 0.15 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL 5}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.8 & 0 & 0.2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL 6}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.75 & 0 & 0.25 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

……LEVEL N-1, LEVEL N

⇒ COMPLETE MARKOV CHAIN

$$\begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccccccccc} 1 & 0.95 & 0.9 & 0.85 & 0.8 & 0.75 & \cdots & N-1 & N \end{array} \\ \begin{bmatrix} 1 & 0.95 & 0.9 & 0.85 & 0.8 & 0.75 & \cdots & N-1 & N \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & N-1 & N \\ 0 & 0.05 & 0.1 & 0.15 & 0.2 & 0.25 & \cdots & N-1 & N \end{bmatrix} \end{array}$$

The above case with non-capture nodes probability value as zero identifies that the transmission of big data is more secured by setting the probability for eavesdropper node as minimum. If the eavesdroppers try to capture the data it will be prevented by cooperative jamming scheme [9].

C. Case III

With addition of capture node C, non-capture node NC, and eavesdropper node E value as 1(i.e., $C_i + NC_i + E_i = 1$). The Table IV and Fig. 6 check the correctness of Markov rule to this case in our proposed algorithm.

a) Probability Value Distribution Table

TABLE IV. TRANSITION TABLE (CASE III)

C	NC	E
1	0	0
0.95	0.04	0.01
0.9	0.09	0.01
0.85	0.14	0.01
0.8	0.19	0.01
0.75	0.24	0.01
……..N-1, N		

b) Markov Transition Diagram

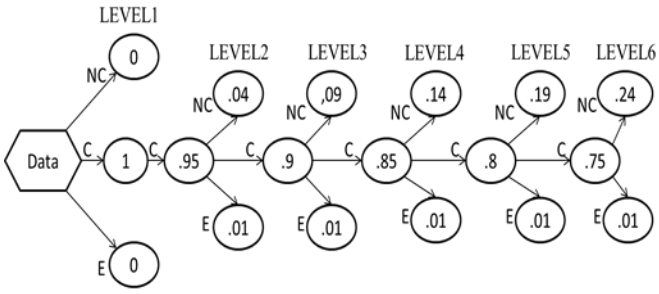


Fig. 6. Transition diagram (case III)

c) Markov Transition Matrix

$$\text{LEVEL 1}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL2}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.95 & 0.04 & 0.01 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL 3}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.9 & 0.9 & 0.01 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

$$\text{LEVEL 4}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.85 & 0.14 & 0.01 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL 5}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.8 & 0.19 & 0.01 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{LEVEL 6}\quad \begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccc} C & NC & E \end{array} \\ \begin{bmatrix} 0.75 & 0.24 & 0.01 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

……LEVEL N-1, LEVEL N

⇒ COMPLETE MARKOV CHAIN

$$\begin{array}{c} \\ C \\ NC \\ E \end{array}\begin{array}{c} \begin{array}{ccccccccc} 1 & 0.95 & 0.9 & 0.85 & 0.8 & 0.75 & \cdots & N-1 & N \end{array} \\ \begin{bmatrix} 1 & 0.95 & 0.9 & 0.85 & 0.8 & 0.75 & \cdots & N-1 & N \\ 0 & 0.04 & 0.09 & 0.14 & 0.19 & 0.24 & \cdots & N-1 & N \\ 0 & 0.01 & 0.01 & 0.01 & 0.01 & 0.01 & \cdots & N-1 & N \end{bmatrix} \end{array}$$

The above Markov process haves probability for all naming nodes ensures secured transmission and proves for proposed novel secure transmission algorithm [9].

V. CONCLUSION AND FUTURE WORK

The verification through Markovian process revealed that proposed novel secure transmission algorithm is more secure and energy efficient to transmit big data by our binary based evaluation process with minimum probability at eavesdroppers and maximum at capture node. In future the proposed algorithm will be discussed and verified through finite state automaton (FSA).

ACKNOWLEDGEMENT

The authors would like to thank Dr. Ponnammal Natarajan worked as Director–Research, Anna University-Chennai, India and Dr. K. Sarukesi former vice chancellor in Hindustan University-Chennai, India for their cognitive ideas and dynamic discussions with respect to the paper's contribution.

REFERENCE

[1] Almudena Konrad, Ben Y. Zhao, Anthony D. Joseph, Reiner Ludwig "A Markov-Based Channel Model Algorithm for Wireless Networks", http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/winet01.pdf.

[2] Chip Craig J. Mathias Principal, Farpoint Group COMNET 2003 —"Wireless Security: Critical Issues and Solutions" 29 January 2003.

[3] A. Divyakant, B. Philip, and et al., "Challenges and opportunities with Big Data," 2012, a community white paper developed by leading researchers.

[4] IBM, "Four vendor views on big Data and big data analytics: IBM," http://www-01.ibm.com/software/in/data/bigdata/, Jan. 2012.

[5] R. Negi, S. Goel, "Secret communication using artificial noise", in: IEEE Vehicular Technology Conference, 2005, pp. 1906–191.

[6] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation", IEEE Trans. Inf. Forensics Security,vol. 4, no. 2, pp. 242–256, Jun. 2009.

[7] S. M. Ross, "Stochastic Processes", John Wiley and Sons, 1996.

[8] R. Schell, "Security – a big question for big data", in: IEEE International Conference on Big Data, pp. 5–5, October 2013.

[9] K. Thiagarajan, K. Saranya, A. Veeraiah, B Sudha, "Wireless Transmission of Big Data Using Novel Secure Algorithm", in 17th International conference on Mathematical Sciences, Engineering and Application. WASET- June 2015., in Press.

[10] J. Talbot, D. Welsh, "Complexity and Cryptography: An Introduction", Cambridge University Press, 2006.

[11] A. D. Wyner, "The wire-tap channel", Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.

[12] M. Zorzi., and R. R. Rao.," On the statistics of block errors in bursty channels". In IEEE Transactions on Communications (1997).

AUTHOR PROFILE

Dr. K.Thiagarajan working as Associate Professor in the Department of Mathematics in PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India. He obtained his Doctorate in Mathematics from University of Mysore, Mysore, India in Feb 2011. He has totally 14 years of experience in teaching. He has attended and presented 38 research articles in national and international conferences and published one national and 42 international journals. Currently he is working on web mining and big data analytics through automata and set theory. His area of specialization is coloring of graphs and DNA computing in Ph.D. program.

K. Saranya received B.E in Computer Science and Engineering from PSNA College of Engineering and Technology, Dindigul, affiliated to Anna University-Chennai, India in 2013. Currently she is pursuing masters in Computer Science and Engineering (with Specialized in Networks) in PSNA College of Engineering and Technology, Dindigul, affiliated to Anna University-Chennai, India.She presented papers in conferences and published in international journals. Currently she is working on big data analytics.

A. Veeraiah completed M.Sc, M.Phil Madurai Kamaraj University (School Of Mathematics) Madurai. He is a Gold medalist of M.sc in Mathematics. Currently he is working as Associate Professor in K.L.N College of Engineering, Pottapalayam, Tamil Nadu, India. He has totally more than 10 years of teaching experience in UG and PG Level. He has passed SET exam conducted by Bharathiyar University, Coimbatore, during the year October 2012

B. Sudha received M.Phil degree at Bharathidhasan University, Trichy, India in 2010. Currently she is working as a Assistant Professor in SRM university, Chennai, India. She is a life member of Indian mathematical society (IMS). She also presented papers in conferences and published in international journals.