International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:6, 2015

Wireless Transmission of Big Data Using Novel Secure Algorithm

K. Thiagarajan, K. Saranya, A. Veeraiah, B. Sudha

***Abstract*—**This paper presents a novel algorithm for secure, reliable and flexible transmission of big data in two hop wireless networks using cooperative jamming scheme. Two hop wireless networks consist of source, relay and destination nodes. Big data has to transmit from source to relay and from relay to destination by deploying security in physical layer. Cooperative jamming scheme determines transmission of big data in more secure manner by protecting it from eavesdroppers and malicious nodes of unknown location. The novel algorithm that ensures secure and energy balance transmission of big data, includes selection of data transmitting region, segmenting the selected region, determining probability ratio for each node (capture node, non-capture and eavesdropper node) in every segment, evaluating the probability using binary based evaluation. If it is secure transmission resume with the two- hop transmission of big data, otherwise prevent the attackers by cooperative jamming scheme and transmit the data in two-hop transmission.

***Keywords*—**Big data, cooperative jamming, energy balance, physical layer, two-hop transmission, wireless security.

I. Introduction

RECENT years, one of the world's irreplaceable technologies in networks is wireless networks. The packet transmission in wireless links is the distinguishing feature of wireless networks. The device-to-device transmission of data in wireless networks can be done via the wireless medium, air, with the condition that the transmission range of receiver is within that of sender [1]. It is used in many different applications such as military, enterprise and governmental communications where the amount of data is very massive and is called big data. Since the amount of data is very large in big data, it is very difficult to ensure the correctness of data. So security is one of the biggest concerns in the environment of big data [2]. It is necessary to have a data transfer mechanism for transmitting the big data, since the data size is increasing quicker and faster.

Two hop transmissions from source to destination node via relay node is becoming essential in wireless communication and plays a vital role in the environment of big data [3].The main focus in this paper will be the security criteria with the two hop transmission of big data in wireless networks. Fig. 1 represents the characteristics of big data which is volume, variety, velocity and veracity and their respective functions.

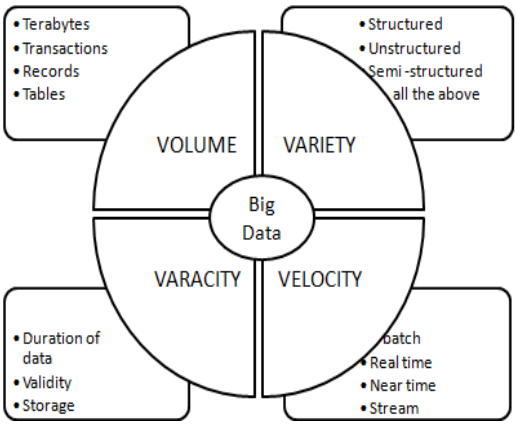


Fig. 1 Characteristics of Big Data

Cryptographically enforced security is the traditional approach for providing security in many different applications where it uses encryption and decryption algorithms. However, everlasting security cannot be determined by this approach due to increased attacks by capturing the secret key [4]. Physical layer security is the alternate method for retaining security at higher layers and to provide everlasting security in big data [5]. In this paper, physical layer security is used to prevent the eavesdroppers and the malicious nodes from capturing the data.

The remainder of this paper is organized as follows. Section II discusses about the cooperative network techniques. Section III highlights the cooperative jamming scenario. Section IV describes the network model that we have considered for transmission of big data and in Section V the novel secure transmission algorithm description with flow diagram is discussed. We conclude our paper by theoretical analysis of our proposed algorithm.

II. Cooperative Network Schemes

Cooperative communication helps in exploiting spatial diversity to enhance the quality of wireless links. The difference between single route networks and cooperative networks is shown in Fig. 2. 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 nodes of the expected destination [6]. There are three schemes to improve security by cooperative networks.

K. Thiagarajan and K. Saranya are with PSNA college of Engineering and Technology, Dindigul, Tamil Nadu, India (e-mail: vidhyamannan@yahoo.com,sharancse16@gmail.com).
A. Veeraiah is with Bharathiyar University, Coimbatore, Tamil Nadu, India (e-mail: jayavee09@gmail.com).
B. Sudha is with SRM University, Chennai, Tamil Nadu, India (email: sudhabala10@gmail.com).

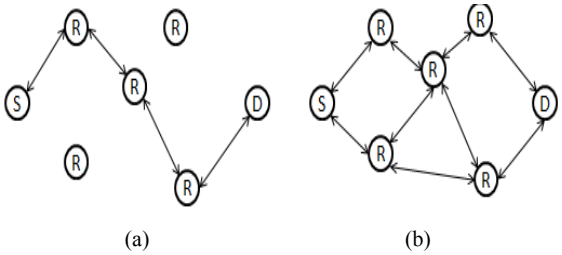


Fig. 2 Difference of Single routing networks (a) and Cooperative Networks (b)

A. Distributed Beam Forming

It is a scheme of two-stage [7]. In the first stage, the message which is broadcast by the source node is received by the relays, the eavesdroppers and the destination node. In the next stage, with the physical layer security function, the received message from source will be multiplex by the relays and forwards it with the beam weights. It results in high overhead for the more coordination it requires between the source and relay nodes for handling the eavesdroppers.

B. Cooperative Relay Selection

The second method in cooperative networks is cooperative relay selection [8]. It is used in conventional wireless networks with less secrecy constraints (i.e., presence of no or single eavesdropper) and is preferred for nodes cooperation with amplify-and-forward and decode-and-forward schemes.

C. Cooperative Jamming

The last method is the cooperative jamming [9]. It is one of the recently proposed techniques in the presence of eavesdroppers to improve the physical layer security. In wireless communication, occurrence of interference is considered as unwanted and redundant. This fetches the work of cooperative jamming for flexible and efficient wireless network technique, to confuse the eavesdroppers and making the source message uncertain by generating friendly interference. 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 in capturing the data as shown in Fig. 3.

Among these three cooperative networks technique for communication, we are going to enumerate the last method cooperative jamming because in physical layer security everlasting security is guaranteed by selecting the acceptable channel for transmitting the data over the attacker channel. To create better acceptable channel many ideas have been proposed in the recent past [9], [10], but due to high cost for multiple antenna deployment and efficient noise designing, these techniques are not flexible for handling wireless networks of large scale of single antenna. This fetches the interest on cooperative jamming, an efficient communication technique for secure two-hop transmission of big data [10].

III. Cooperative Jamming Schemes

Cooperative jamming technique has three schemes. They are attacker location known, attacker location unknown, attacker and relay co-located. In the attacker location known scheme [11], the presence of the eavesdroppers will be detected by the network, whereas in attacker and relay co-located scheme [12], direct jamming will be created by destination node while the source node sends the data to the co-located node, in this reliability is not ensured while amount of data is very large. In attacker location unknown scheme as shown in Fig. 3, the eavesdroppers E will be jammed by the jamming signal emitted by the source S, destination D and relay nodes R in the jamming subspace. Though eavesdroppers aware of this jamming signal, it cannot be removed. Here, we use attacker location unknown scheme for secure transmission of big data.

In this article, we focus on secure transmission of big data via cooperative relays from source to the destination node from protecting the data from eavesdroppers. The consumption of energy should be equally distributed among all relays is ensured by our novel secure transmission algorithm. From early papers of attacker location unknown in [7] optimal relay selection based transmission technique is proposed, in [13] a secure transmission scheme is proposed for both one dimensional and two dimensional networks, in [14]

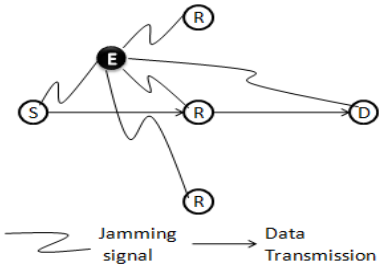


Fig. 3 Cooperative Jamming with Attacker Location Unknown Scheme

Two transmission technique is proposed by using the relays which are opportunistic, in [15] a technique in which for the given transmitter signal is protected by the other transmitter by using aggregate interference. Our work is different from the above papers, as we focus on the secure transmission as well as the energy balance performance.

IV. Network Model

The network model for the two-hop secure transmission of big data in wireless network technique is determined by having the source node S wishes to transmit the data securely to the destination node D without knowing about the locations and channels. Also in between the source and destination node there will be multiple half duplex i relay nodes from R_1, R_2,….R_i and j eavesdropper nodes from E_1, E_2 ,….E_j is placed.

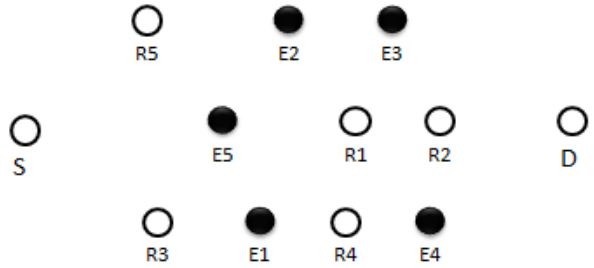


Fig. 4 Network Model with Number of Relays i=5 and Number of Eavesdropper j=5

By assumption, eavesdroppers will hide itself without transmitting the data and also based on their observation they attempts to decode the message. We are going to determine the time slotted system in which the eavesdroppers and relay nodes will stay statically for the whole slot after selecting the place for them in the network both independently and uniformly. The network model is shown in Fig. 4. Our aim is to build the secure transmission architecture for reliable and flexible transmitting of big data and to have the energy control mechanism for balanced use of energy by all nodes in the network.

V. Novel Secure Transmission Algorithm

A. Flow of Novel Secure Transmission Algorithm

The goal in our constructed flow diagram is to tolerate the number of eavesdropper j and assisting the transmission in the environment with number of relay nodes as i. The algorithm has to guarantee the secure transmission still the presence of eavesdropper is more in the network. The structure of the secure transmission flow diagram is two-hop transmission (source-relay-destination). As mentioned above, cooperative jamming technique is adopted in two hop transmission at physical layer security of wireless networks to have transmission of big data more reliable and flexible. The flow of the secure transmission as shown in Fig. 5, it includes selection of data transmitting region, segmenting the selected transmission region of equal size, determining the probability ratio for each node i.e., capture node, non-capture node and eavesdropper nodes, evaluation of the probability ratio. If the probability ratio for capture node equals 1 then we say the data can able to transmit securely by two hop transmission. Otherwise, we have to prevent the eavesdroppers by deploying cooperative jamming method for pursuing the secure transmission of big data by two hop wireless networks.

B. Novel Secure Transmission Algorithm

1) Description Scenario

As mentioned in above flow diagram we establish the scenario of two-hop secure transmission and to provide energy balance control. To elaborate and calculate our algorithm, the network has to be mapped as shown in Fig. 6 is an entity square with correlative system [-0.5,0.5]*[-0.5,0.5]. Here, in (-0.5,0) source is placed and in (0,0.5) destination is placed. The working of algorithm is as follows,

2) Selection of Data Transmitting Region

Select the origin point between the source and destination with square of side length l from the location area provided.

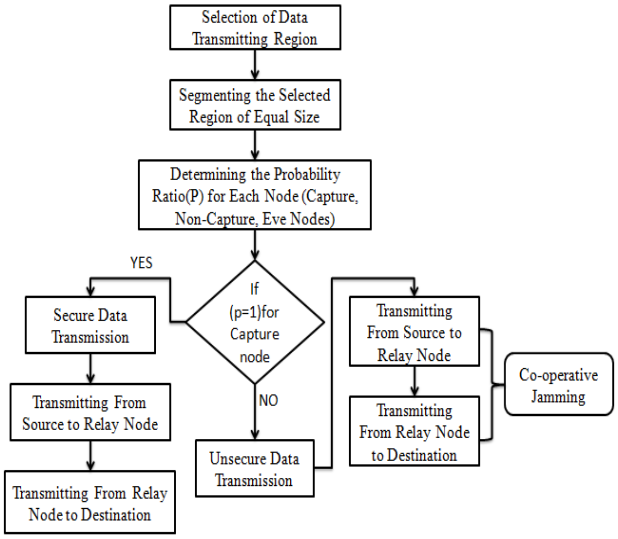


Fig. 5 Flow Diagram for Novel Secure Transmission Algorithm

3) Segmentation of Selected Region

Segment the selected region square of side length l into four equal segments of length l/2 each. The possibilities of relay nodes in each segment will be classified into four naming nodes. They are capture node (the node which is ready to get the data for transmission), non-capture node (the node which is present in the network but will not transmit the data), eavesdropper node (it is the attacker node that illegally captures the data and causes malicious activities), and ideal node (the node which is physically present and does not do any action).

Therefore, the total number of nodes in each segment will be, Total Nodes (T) = Capture Nodes (C) + Non-capture Nodes (NC) + Eavesdropper Nodes (E) + Ideal Nodes (I).

4) Probability Ratio Evaluation for Each Node

The probability ratio is calculated as, each node present in a segment is divided by the total number of nodes in a segment.

a) Probability ratio for the capture node is calculated as, the number of capture nodes in a segment divided by the total number of nodes in a segment i.e., $P(C) = \frac{C}{T}$
b) Probability ratio for the non-capture node is calculated as, the number of non-capture nodes in a segment divided by the total number of nodes in a segment i.e., $P(NC) = \frac{NC}{T}$
c) Probability ratio for the eavesdropper node is calculated as, the number of eavesdropper nodes in a segment divided by the total number of nodes in a segment i.e., $P(E) = \frac{E}{T}$
d) For ideal nodes, the probability ratio is unnecessary.

Therefore, the total probability evaluation for single time slot in one complete end-to-end transmission is calculated as,

P(T)=P(C)+P(NC)+P(E). If the probability ratio of any two naming node (capture and non-capture node) is known, it is easy to find the probability of eavesdropper node since attacker location is unknown in a segment.

5) Selection of a Relay Node for Transmission

As mentioned in the above step, in each segment the probability ratio will be evaluated. The segment which has maximum probability for a capture node, that segment will be selected for secure transmission of big data. If the probability value is maximum for two or more capture nodes in the selected segment, then a capture node will be selected randomly for transmission in that segment.

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

For checking the probability ratio and the secure transmission of big data, we are going for binary based evaluation as shown in Table I. The capture, non-capture and eavesdropper nodes probability value lies between 0 and 1. Based on the above tabulation we will be able to predict the transmission of data, whether it is secure or unsecure. As per the transmission results the following actions has to be done,

a) Secure- If the transmission assures secure with probability of capture node as 1 in a segment, then select the segment and particular capture node to transmit the data.
b) Secure/Unsecure- If the transmission cannot be predictable, having the probability ratio for the non-capture and eavesdropper node, then emit jamming signal by the capture nodes which has significantly high probability ratio to prevent the eavesdroppers from capturing the data.
c) Unsecure- If the transmission assures unsecure, either omit the transmission or adopt the step (b).

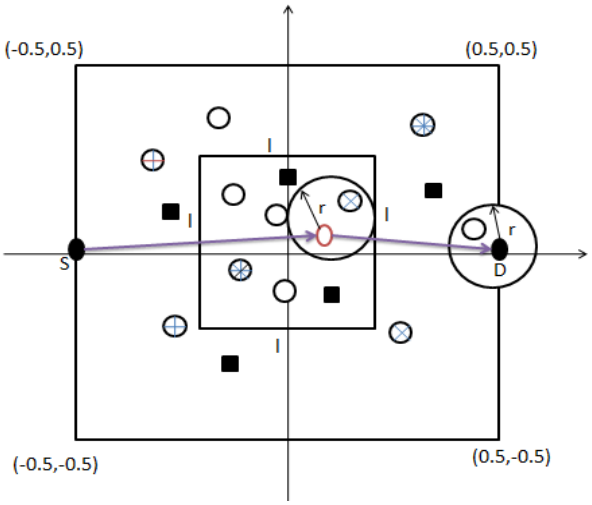
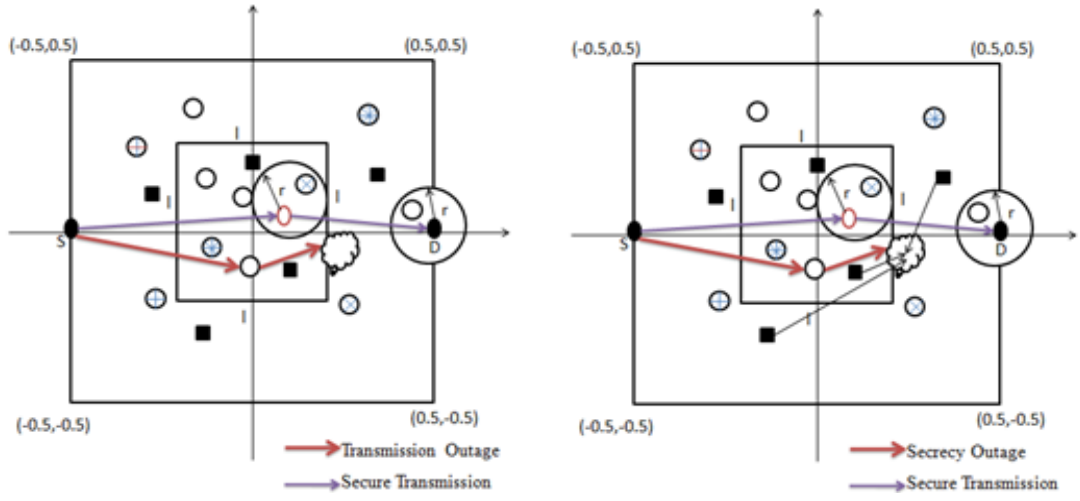


Fig. 6 Proposed Scenario

6) Transmission from Source to Selected Relay Node

After selecting the relay node for transmitting the data, transmission will be done from source to relay node. In the meanwhile, based on the transmission results as mentioned in Table I, actions will be performed.



(a) (b)

Fig. 7 (a) Transmission Outage probability (b) Secrecy Outage Probability

7) Transmission from Selected Relay Node to the Destination

After transmitting in one-hop, data is transmitted from the relay node to the destination node. In the meanwhile, based on the transmission results as mentioned in Table I, actions will be performed. We assume that only one end-to-end transmission can be conducted in one time slot. It is notable that in our protocol the energy balance can be flexibly controlled by a proper setting of relay selection region side-length l. Here parameter r indicates that the jammers must be at least distance r away from the intended receivers and thus the interferences at the intended receivers are controlled.

VI. Theoretical Analysis

To analysis our algorithm theoretically we use two metrics secrecy outage probability and transmission outage probability as shown in Fig. 7. Outage probability is used to estimate the correctness of our novel algorithm scenario. The packet is determined as lost, if outage occurs.

A. Transmission Outage Probability

From the source S to destination D transmission of data packets, probability of transmission outage occurs if, the packet cannot be received at destination D. The probability of transmission outage while transmitting the data from S to D under the algorithm scenario is

$$P_{out}^{T} = P\left(O_{S\to R_{m*}}^{(T)}\right) + P\left(O_{R_{m*\to D}}^{(T)}\right) - P\left(O_{S\to R_{m*}}^{(T)}\right) * P\left(O_{R_{m*\to D}}^{(T)}\right) (1)$$

From the above equation, transmission outage probability is verified for the transmission of data from source S to the selected relay R_{m*} and from selected relay R_{m*} to D, and is defined as $O_{\mathrm{S}\to\mathrm{Rm}*}^{(T)}$ and $O_{\mathrm{Rm}*\to\mathrm{D}}^{(T)}$respectively.

B. Secrecy Outage Probability

From the source S to destination D transmission of data packets, probability of secrecy outage occurs if, during the process of this two-hop transmission at least one eavesdropper can recover the transmitted packets. The probability of secrecy outage while transmitting the data from S to D under the algorithm scenario is

$$P_{out}^{C} = P\left(O_{S\to R_{m*}}^{(\mathrm{C})}\right) + P\left(O_{R_{m*\to D}}^{(C)}\right) - P\left(O_{S\to R_{m*}}^{(C)}\right) * P\left(O_{R_{m*\to D}}^{(C)}\right) (2)$$

From the above equation, secrecy outage probability is verified for the transmission of data from source S to the selected relay R_{m*} and from selected relay R_{m*} to D, and is defined as $O_{\mathrm{S}\to\mathrm{Rm}*}^{(C)}$ and $O_{\mathrm{Rm}*\to\mathrm{D}}^{(C)}$respectively.

VII. Conclusion

The paper describes the secure and energy efficient transmission of big data in wireless network using novel secure transmission algorithm. The algorithm can provide flexible control of security and reliability through proper settings of parameters (l, r) and the energy balance can be controlled by proper setting of the side-length of region of relay selection. Theoretical analysis verifies the correctness of the data transmission based on our novel algorithm. The proposed algorithm will be discussed and verified thorough Markovian process and finite state automaton process in future.

Acknowledgment

The authors would like to thank Dr. Ponnammal Natarajan worked as Director–Research, Anna University-Chennai, India for her cognitive ideas and dynamic discussions with respect to the paper's contribution.

Reference

[1] Chip Craig J. Mathias Principal, Farpoint Group COMNET 2003 —Wireless Security: Critical Issues and Solutions 29 January 2003.
[2] R. Schell, Security – a big question for big data, in: IEEE International Conference on Big Data, October 2013, pp. 5–5.
[3] S. Narayanan, P. University, Two-hop Forwarding in Wireless Networks, Polytechnic University, 2006.
[4] J. Talbot, D. Welsh, Complexity and Cryptography: An Introduction, Cambridge University Press, 2006.
[5] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[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] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation", in Proc. 46th Ann. Allerto Conf. Commun., Control, Comput., Champaign, IL, USA, Sep. 2008, pp. 1132–1138.
[8] Gaojie Chen, Member, IEEE, Zhao Tian, Student Member, IEEE, Yu Gong, Member, IEEE, Zhi Chen, Member, IEEE, and Jonathon A. Chambers, Fellow, Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks IEEE transactions on Information Forensics and Security, Vol.9,no.4, April 2014.
[9] R. Negi, S. Goel, Secret communication using artificial noise, in: IEEE Vehicular Technology Conference, 2005, pp. 1906–1910.
[10] S. Goel, R. Negi, Secret communication in presence of colluding eavesdroppers, in: IEEE Military Communications Conference, 2005, pp. 1501–1506.
[11] L. Dong, Z. Han, A. Petropulu, H.V. Poor, Improving wireless physical layer security via cooperating relays, IEEE Trans. Signal Process. 58 (2010) 1875–1888.
[12] Alvaro Araujo, Javier Blesa, Elena Romero, Octavio Nieto-Taladriz, Cooperative jam Technique to Increase Physical-layer Security in CWSN, in: COCORA 2012: The Second International Conference on Advances in Cognitive Radio.
[13] C.Capar, DGoeckel, B. Liu, D.Towsley, Secret communication in large wireless networks without eavesdropper location information in: Proceedings IEEE INFOCOM, 2012, pp. 1152–1160.
[14] Z. Ding, K. Leung, D. Goeckel, D. Towsley, Opportunistic relaying for secrecy communications: cooperative jamming vs. relay chatting, IEEE Trans. Wirel. Commun. 10 (6) (2011) 1725–1729.
[15] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, D. Towsley, Physical layer security from inter-session interference in large wireless networks, in: Proceeding of IEEE INFOCOM, 2012, pp. 1179–1187 .

Dr. K. Thiagarajan working as Associate Professor in the Department of Mathematics in PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India. He has completed his Ph.D from University of Mysore, Mysore in February 2011 and 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 36 international journal. 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.

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 10years 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.