IJRSET AUGUST 2019 Volume 6, Issue 8 Pages: 1-10

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

FRIEND RECOMMENDATION FOR EFFICIENT NOVEL SECURE COMMUNICATION USING ONLINE SOCIAL NETWORK

[1] K. SUBRAMANIAN, [2] S. NIRMAL RAJ, [3] S. KIRUTHIGA
[1, 2, 3] Students, Department of Electronics and Communication Engineering,
[1, 2, 3] Rajalakshmi Institute of Technology, Chennai, India.

ABSTRACT- Recommendation system (RS) plays a vital role for the online data users. But most of the approaches based on the RS in online public networks are not reliable with the interest of data users. In order to overcome the untrustworthiness and uncertainty of user based RS in public network. We have proposed a Novel Secure Key Distribution based Recommendation System (NSKD-RS) for preserving the privacy of the data users using neural networks. Data User (DU) send request to other DU through the Trusted Third Party (TTP). TTP will search the similar interest DUs based on the received search request. The DUs interest is placed in terms of tag. If the DU interest matches with other DU interest then two DU's will become friends by using neural networks. The cloud has the collection of the data user's files, here the neural networks are used for the data classification based on the data user's interest in addition to neural networks provide the recommended users based on the similar interest. We have proposed the secure recommendation system based key distribution mechanism for the tag decryption as well as to have secure communication between the DUs. The secure tag matching process is developed in order to reduce the computation complexity as well as to have the secure data sharing between the DUs. By using our proposed NSKD-RS the commutation as well as the communication complexity is reduced.

Keywords: [Neural networks, privacy, key distribution, computation complexity, communication complexity.]

1. INTRODUCTION

Social Networks (SN's) are the essential domain for the DU's. By the usage of the SN the DU's can create friends. The existing SN applications are as follows: Facebook, SinaWeibo, Twitter as well as instagram [1]. RS will recommend the trustworthy as well as the good friends to the DU's by the usage of RS, the DU's can get huge number of friends [2–10]. The data sharing method can be enriched. In order to have the good and trustworthy friends in the SN's the secure RS is necessary [11–14]. The job of RS is to recommend the friends based on the DU's interest. To suggest the correct friends to the end entity is really a challenging task [15]. Many researches in many areas are researching in the recommendation field. The RS domain is classified into 3 major classifications:1) DU's link recommendation mechanism 2) DU's interest recommendation system 3) locality based RS all the above said mechanisms also has the positive as well as negative side [16–20]. By concluding the

above said process we say that RS is still an on-going challenging No. Due to the growth of the online networks, the DU's submit their private photos as well as their communication messages towards the cloud for protecting the DU's privacy the outsourced data should be encrypted before submitting to the Cloud Service Provider (CSP) [21–24]. In order to resolve the above said No. we have proposed a Novel Secure Key Distribution based Recommendation System (NSKD-RS) for the online networks to have a secure as well as the accuracy based RS [25–27].

Objectives of the NSKD-RS research paper is:

1. To propose the DU's authentication phase with secure key distribution and minimized computation complexity.
2. To propose the label matching mechanism in order to improve the accuracy of the recommended friends with reduced communication complexity.
3. To propose the decryption mechanism in order to view the information about the friends with less computation complexity.

2. RELATED WORKS

RS is classified into three types: Firstly, data user'sattribute based recommendation system, secondly, data user's friend link based recommendation system and finally, the data users locality based recommendation system.

a. DU's attribute based RS

A potential friend recommendation in online social network projected method is mainly used for finding the various friends with mutual interest. But incorporating the RS for huge volume of DU's with various tastes is a challenging No.The proposed unified frame work for link recommendation with user attributes. Relation based RS is the serious job which not only supports the progress of DU's knowledge, moreover it also plays a vital part in network development. Ganesh Babu and Amudha (2014)proposed joint link prediction and attributes inference using a Social Attribute Network (SAN). The SAN structure is enhanced with numerous supervised as well as unsupervised connection predictions. Link prediction is additionally upgraded by deducing lost attribute.Karthika and VidhyaSaraswathi(2019) proposed outsourcing privacy preserving social network to cloud. The existing scheme suffers due to neighbourhood attack. In order to overcome that attack the authors haveproposed heuristic indistinguishable group anonymisation protocol.Ganesh Babu and Amudha (2015)proposed greedy algorithm for social network anonymisation. The previous protocols suffer due to anonymisation cost. In order to reduce the cost No. partial anonymity is proposed.Karthika and VidhyaSaraswathi(2017) have proposed omnisuggest cloud based context aware RS for mobile social networks. The earlier schemes suffer due to scalability problems, cold start No. as well as data sparseness.Ganesh Babu and Amudha(2016) proposed novel feature selection strategy for friend RS. Even though there are numerous methods for RS. The author has used the feature selection model as well as data processing mechanisms for the RS. By using this method friend RS can be implemented with more accuracy.Karthika and VidhyaSaraswathi(2017) proposed friend RS based on DU's online behaviour. Since DU's are with different interest it is difficult to recommend the friend based on their interest. To recommend a friend in social network domain. The author have used multi layered classification algorithm for friend recommendation. Ganesh Babu and Amudha (2019)proposed tag with E-Fuzzy sets for the friend recommendation. The tag is used for classifying the DU's based on the importance as well as interested items and their respective properties.

3. PROPOSED SYSTEM ARCHITECTURE

Our system is highly efficient for providing the privacy preserving recommendations based on the tag used by the data users who has the same interest. The NSKD-RS

mechanism contains four modules namely: 1) Data users with different interest 2) Trusted third party 3) cloud service provider 4) Data users with same interest as represented in the Figure 1.

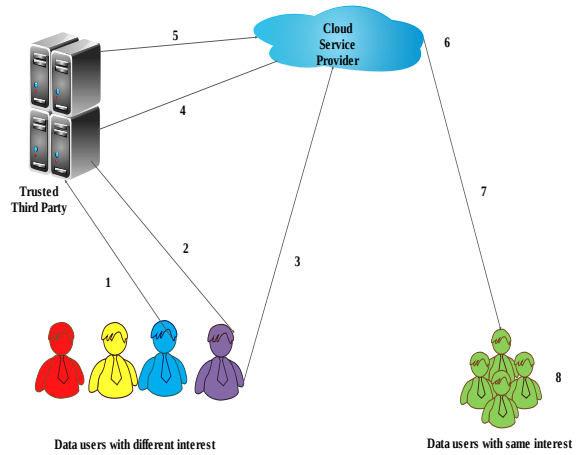

Figure 1: Proposed System Architecture of the NSKD-RS

The modules of the NSKD-RS as well as its working mechanism are explained as follows:

A. Data Users with different Interest

Data users with different interest have to register towards the TTP. After successful registration the TTP will authenticate the data users based on their credentials. Once if the data users are authenticated then they can submit their request towards the CSP for finding the friends with similar interest.

B. Trusted Third Party

In order to minimize the work load of the CSP the TTP helps in terms of authenticating the data users as well generating the key for the authenticated data users to decrypt the downloaded tag.

C. Cloud Service Provider

Once the data users submits their tag towards the CSP. Initially the CSP has to forward the tag to the TTP. TTP will verify whether the data user is authenticated and sends the verified message to the CSP. Once if the data user is authenticated then the tag matching process is successfully done by the CSP and sends the recommendation of friends based on the data user's interest.

3.1 Tag Matching Mechanism

1. Data user generates the communication key as well as the encrypted message. The communication secret key is generated as follows:$CSK_1 = A^{\text{pri key }1} \bmod p$. Moreover the encrypted message is generated as follows: $E = msg \oplus CSK_1$. Data user 1 register with the TTP with the interest of a_1, k_1.
2. Data user 2 registers with the TTP by using the interest value a_2, k_2.
3. Now TTP find the similarity between the tags and generate the group key value as: $x = \sum_{i=1}^{n}(a_i m_i y_i) \bmod \partial_g$ as well as $A = b^x \bmod x$.
4. TTP send the group key value A to the authenticated data users.
5. Data user 1 generate the communication secret key as :$CSK_1 = p^{A-1} \bmod A - 1$ as well as the data user 2 generates the communication secret key as $CSK_2 = p^{A-1} \bmod A - 1$.
6. Data user 1 sends CSK_1 to TTP. Data user 2 sends the$CSK_2$to the TTP.
7. The TTP verifies both the CSK values are same.
8. If the values are same the TTP sends the tag value. Is the values are not same then the TTP will reject the tag values.
9. The data user1 generates the communication key based on the group key value as follows: $CSK_1 = A^{\text{pri key}-1} \bmod p$.
10. Data user1 sends the encrypted message as well as the communication key in the secure channel to the data user 2.
11. The data user 2 will decrypt the message with the help of the communication key as follows :$D = \text{enc msg} \oplus CSK_1$

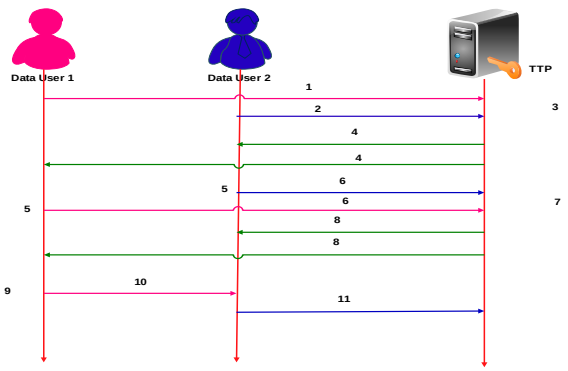

Figure 2: Tag Matching Mechanism

1. Setup

Let G0 and G1 be two multiplicative cyclic groups with prime order p. The g is the generator of G0 as well as e is the bilinear mapping, e : G0 ×G0 →G1.

2. Key generation

Let G be the group. All the DU's public key should be prime number p. All the DU's a_i should be integer value. The DU's public key should be k_i, where i=1 to n. CA generates the key based on the prime values.

$$\partial_g = k_1 \times k_2 \dots \dots k_i \quad (1)$$

The M_i value is created by the TTP based on the equation 2. $M_i = \partial_g \div k_i$ (2)

By dividing the equation 2 with the k_i values the y_i values are created as follows in

$$y_i = M_i \bmod k_i \quad (3)$$

Multiplying the values of the $a_i * m_i * y_i$ and taking mod with ∂_g will generate the x value. $x = \sum_{i=1}^{n}(a_i m_i y_i) \bmod \partial_g$ (4)

Selecting the random number 'b' with respect to the group and applying the exponential as well as the modular operation the group key value 'A' is created.

$A = b^x \bmod x$ // where b is the random number (5)

3. Communication key generation

TTP sends the prime number p and A for the authenticated DU's. By using the p and A the DU's can generate the Communication Secret Key (CSK_i).

$$CSK_i = A^{U_i - 1} \bmod p \quad (6)$$

4. Encryption

Data users encrypt the message with the help of the communication key. The data users will send that communication secret key as well the encrypted message to the other data users. For the similar interest data users the TTP will send the message that in order to decrypt the message the data users should apply the XOR operation.

$$DU(enc)_i = msg \oplus csk_i \quad (7)$$

Data user broadcast the messageas well ascsk_i to all other users in the online social networks in SSL.

5. Decryption

Once the data users receive the message as well as the communication key of the similar data users then by applying the XOR operation the data users can decrypt the message as follows:

$$DU(dec)_i = enc\ msg \oplus csk_i \quad (8)$$

4. SECURITY ANALYSIS

1. Impersonation Attack

The attacker cannot do impersonation attack because the credentials of the legitimate data user are placed in terms of the encrypted tag. Thus the attacker cannot decrypt the tag unless he knows the key generation algorithm which is used to decrypt the tag.

2. Replay Attack

If the data user captures the message and replay the encrypted message as the legal data user. He does not know the data users who have the similar interest. Since he does not know the communication secret key as well the XOR operation the hacker cannot perform the replay attack.

3. Man in the Middle Attack

When the data is communicated between the data user and the trusted third party the man in the middle attack is not possible. Only for the authenticated data users the trusted third party will send the group key to generate the communication secret key which is used for the message encryption as well as the decryption. For the attacker who enters in the middle the group key is unknown. Thus the attacker cannot generate the communication secret key which is used for the encryption and decryption.

4. Eavesdropping

The TTP is trasmitting the group key after secure authentication. The attacker cannot eavesdrop the group key. Because the group key is generated based on the random number selected by the TTP as well as the data user.The attacker cannot eavesdrop the communication key because for each session the communication key is varied, even if the attacker eavesdrop the key if the session is finished the message is invalid.

5. DDOS Attack

The communication between the data user as well as the trusted third party is done based on the session time. So if the message delayed and received, the session is completed. So the late message is not authenticated. Based on the session time the message should be reached. If any delay happens then the message is not valid.

5. PERFORMANCE ANALYSIS

In this performance analysis part, we compute the computation complexity as well we the communication complexity of the NSKD-RS against various mechanisms proposed in the survey. The computational complexity of the NSKD-RS scheme was computed using Cygwin tool 1.7.35 using language C, windows 8, processor :Intel Core i3-5005U, CPU : 2.00 GHz, RAM :4.00 GB.

Table.3 briefly explains about the computation time required for the Key generation phase, Tag Matching Phase, Encryption phase and Decryption phase are computed. The symbols on Table 3 are listed for the easy understanding of the computational complexity. TA –Addition time, TE- Exponential time, TM-multiplication time , TP- paring time, TD-division time, TXOR –time taken for xor operation and TH- hashing time.

Parameters / Methods	Key generation	Encryption	Decryption
Proposed	$T_E + T_{MOD}$	T_{XOR}	T_{XOR}
9	$2T_{MAT}$	$2T_E + T_A + T_{MOD}$	$T_E + T_D + T_{SRT}$
11	$T_M + T_D + 2T_H$	$T_P + 2T_H + 2T_E$	$T_P + 2T_H + 2T_E$

Table 3.Computational Complexity of the parameters

A. Key generation phase

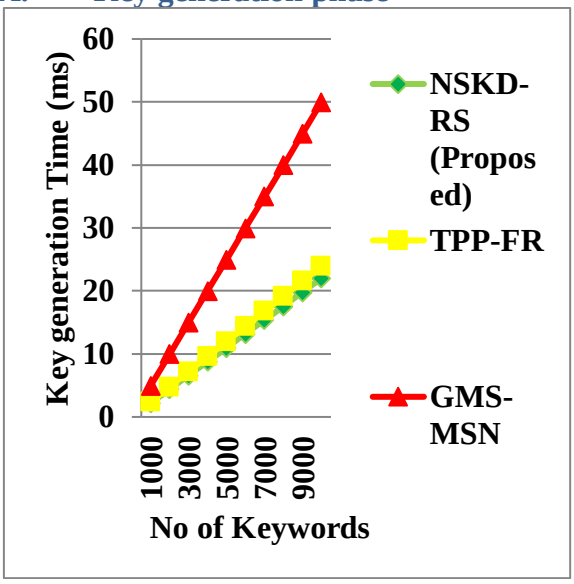

Figure 3:key generation phase

From Figure 3, it is clear that, the time taken for the Group matching scheme for mobile social networks(GMS-MSK) is 50ms for 10000 keywords. The time taken for the Trusted Privacy Preserving friend recommendation scheme (TPP-FR) is 24ms. Finally the time taken for the proposed Novel Secure Key Distribution based Recommendation System (NSKD-RS) is 22ms. From the Figure 3, it is clear that for the key generation phase the computation complexity is very low for our proposed mechanism when compared to the existing papers.

B. Encryption Phase

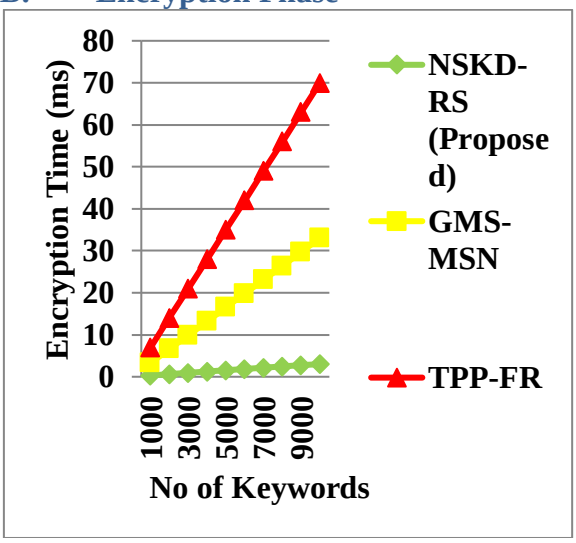

Figure 4:Encryption Phase

C. Decryption phase

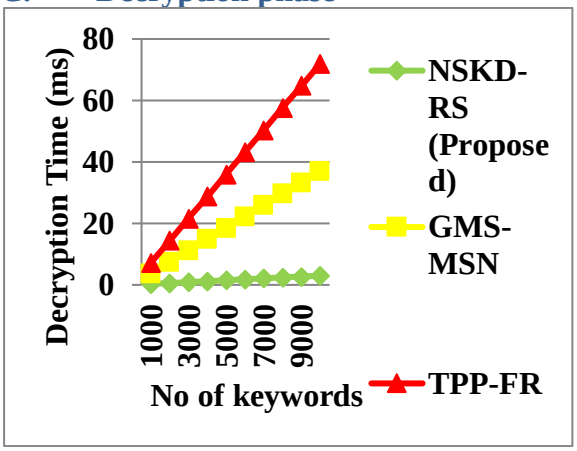

Figure 5: Decryption Phase

From Figure 5, it is clear that, the time taken for the Trusted Privacy Preserving friend recommendation scheme (TPP-FR) is 72ms for 10000 keywords. The time taken for the Group matching scheme for mobile social networks (GMS-MSK) is 37ms. Finally the time taken for the proposed Novel Secure Key Distribution based Recommendation System (NSKD-RS) is 3ms. From the figure 5 it is clear that for the Decryption phase the computation complexity is very low for our proposed mechanism when compared to the existing schemes.

D. Communication Complexity

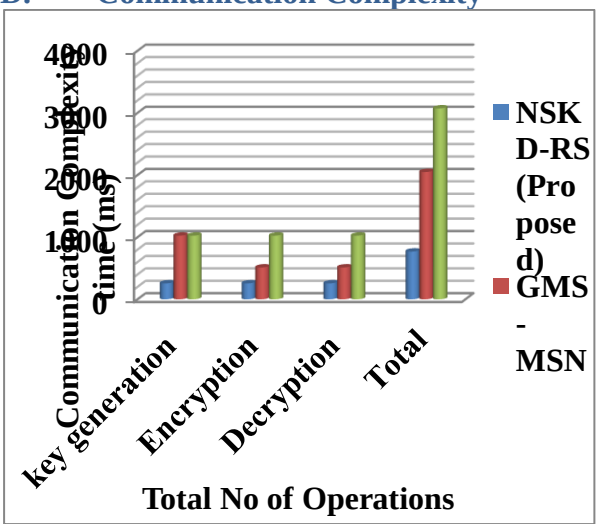

Figure 6: Communication Complexity

From Figure 6, it is clear that, for the key generation phase, the no of bits taken for the Trusted Privacy Preserving friend recommendation scheme is 1024 for 10000 keywords. The no of bits taken for the Group matching scheme for mobile social networks is 1024. Finally the no of bits taken for the proposed NSKD-RS is 256.

For the encryption phase, the no of bits taken for the TPP-FR is 1024 for 10000 keywords. The no of bits taken for the GMS-MSK is 512. Finally the no of bits taken for the proposed Novel Secure Key Distribution based Recommendation System is 256. For the decryption phase, the no of bits taken for the 11 is 1024 for 10000 keywords. The no of bits taken for the 9 is 512.

Finally the no of bits taken for the proposed Novel Secure Key Distribution based Recommendation System is 256. The total operation, the no of bits taken for the Trusted Privacy Preserving friend recommendation scheme is 3072 for 10000 keywords. The no of bits taken for the Group matching scheme for mobile social networks is 2048. Finally the no of bits taken for the proposed NSKD-RS is 768.

CONCLUSION AND FUTURE WORKS

In this research proposal, we have developed a Novel Secure Key Distribution based Recommendation System (NSKD-RS). The proposed protocol has the key generation module which is used for the group key generation for the DUs. We have constructed the encryption as well as the decryption phase with less computational complexity. This will ensure the reduced computational complexity when compared to the previous schemes. The existing papers are based on the data mining as well as the link based recommendation mechanism. This shows the very high computation as well communication complexity. Some of the papers are facing the No.s like high storage complexity. In order to resolve the gaps based on the computation as well as the communication complexity we have proposed the secure and reliable recommendation mechanism.

We have also proposed the tag matching phase, which has a secure construction format. This may consume only less computation complexity when compared with the present research papers. We have

also reduced the overall communication complexity as shown in the Figure 6. Future research work will include the actual data set. This will have challenging computations since we are using the actual world data set.

REFERENCES

[1]. R.GaneshBabu, and Dr.V.Amudha, "SPECTRUM SENSING TECHNIQUES IN COGNITIVE RADIO NETWORKS: A SURVEY", International Journal of Scientific and Engineering Research, Vol.5, No.4,April 2014, pp.23-32.

[2]. P.Karthika, R.GaneshBabu, and A.Nedumaran, "MACHINE LEARNING SECURITY ALLOCATION IN IOT" Proceedings of IEEE International Conference on Intelligent Computing and Control Systems [ICICCS 2019] with ISBN.No-978-1-5386-8113-8, conducted at Vaigai College of Engineering, Madurai, India, May 15-17,2019, (Accepted and in Press).

[3]. R.GaneshBabu, and Dr.V.Amudha, "ANALYSIS OF DISTRIBUTED COORDINATED SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS", International Journal of Applied Engineering Research,Vol.10,No.6,March 2015, pp.5547-5552.

[4]. Ms.P.Karthika, Dr.R.GaneshBabu, and Mr.K.Jayaram, "BIOMETRIC BASED ON STEGANOGRAPHY IMAGE SECURITY IN WIRELESS SENSOR NETWORKS" Proceedings of Second International Conference on Computational Intelligence and Data Science (ICCIDS 2019) in association with Elsevier-Procedia Computer Science conducted at The NorthCap University, Gurugram, India, Sept 06-07,2019,(Accepted and in Press).

[5]. R.GaneshBabu, and Dr.V.Amudha, "PERFORMANCE ANALYSIS OF DISTRIBUTED COORDINATED SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS", Middle East Journal of Scientific Research, Vol.23,No.23,May 2015, pp.50-55.

[6]. A.Nedumaran, R.GaneshBabu, Mesmer MeseleKass, and P.Karthika, "MANET: IMAGE SECURITY CLASSIFICATION USING SUPPORT VECTOR MACHINE" AIP Conference Proceedings of International Conference on Sustainable Manufacturing, Materials and Technologies (ICSMMT 2019) conducted at Coimbatore, Tamil Nadu, India, Oct 25-26, 2019, (Accepted and in Press).

[7]. R.GaneshBabu, and Dr.V.Amudha, "CLUSTER TECHNIQUE BASED CHANNEL SENSING IN COGNITIVE RADIO NETWORKS", International Journal of Control Theory and Applications, Vol.9,No.5,May 2016, pp.207-213.

[8]. P.Karthika, R.GaneshBabu, and P.A.Karthik, "FOG COMPUTING USING INTEROPERATIBILITY AND IOT SECURITY ISSUES IN HEALTH CARE", In: Devendra Kumar Sharma., Valentina Emilia Balas., Le Hoang Son., Rohit Sharma., KorhanCengi. (eds) Proceedings of Third International Conference on Micro-Electronics and Telecommunication Engineering. Lecture Notes in Networks and Systems, Springer, in Press (2019).

[9]. R.GaneshBabu, "HELIUM'S ORBIT INTERNET OF THINGS (IOT) SPACE", International Journal of Computer Science & Wireless Security, Vol.01, No.01,Mar-Apr 2016,pp.123-124.

[10]. P. Karthika and P. VidhyaSaraswathi "A SURVEY OF CONTENT BASED VIDEO COPY DETECTION USING BIG DATA", International Journal of Scientific Research in Science and Technology, Vol. 3, No.5, March-April 2017, pp. 114-118.

[11]. R.GaneshBabu, "MISMATCH CORRECTION OF ANALOG TO DIGITAL CONVERTER IN DIGITAL COMMUNICATION RECEIVER", International Journal of Advanced Research Trends In Engineering and Technology, Vol.3,No.19,April 2016,pp.264-268.

[12]. P. Karthika and P. VidhyaSaraswathi, "CONTENT BASED VIDEO COPY DETECTION USING FRAME BASED FUSION TECHNIQUE", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, No. 17, September 2017, pp. 885-894.

[13]. R.GaneshBabu, "DYNAMIC SPECTRUM ACCESS TECHNIQUES IN COGNITIVE RADIO NETWORKS", International Journal of Emerging

Technology in Computer Science and Electronics, Vol.22,No.2,May 2016,pp.508-512.
[14]. P. Karthika, P. VidhyaSaraswathi, "DIGITAL VIDEO COPY DETECTION USING STEGANOGRAPHY FRAME BASED FUSION TECHNIQUES," In: Pandian D., FernandoX., Baig Z., Shi F. (eds) Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering, Lecture Notes in Computational Vision and Biomechanics, vol. 30. Springer, 2017.
[15]. R.GaneshBabu, "RESOURCE ALLOCATION IN QOS SCHEDULING FOR IEEE 802.16 SYSTEMS", International Journal of Science and Innovative Engineering and Technology, Vol.1,No.5,May 2016, pp.50-55.
[16]. R.GaneshBabu, "WIMAX CAPACITY ENCHANCEMENTS INTRODUCING FULL FREQUENCY REUSE USING MIMO TECHNIQUES", International Journal of Advanced Research in Biology Engineering Science and Technology, Vol.2,No.16,May 2016, pp.1-7.
[17]. R.GaneshBabu, "COGNITIVE RADIOS SPECTRUM ALLOCATION IN WIRELESS MESH NETWORKS", International Journal of Global Research and Development, Vol.1,No.6,July 2016, pp.289-294.
[18]. R.GaneshBabu, and Dr.V.Amudha, "ALLOW AN USEFUL INTERFERENCE OF AUTHENTICATED SECONDARY USER IN COGNITIVE RADIO NETWORKS", International Journal of Pure and Applied Mathematics, Vol.119,No.16,May 2018, pp.3341-3354.
[19]. R.GaneshBabu, and Dr.V.Amudha, "COMPARATIVE ANALYSIS OF DISTRIBUTIVE FIREFLY OPTIMIZED SPECTRUM SENSING CLUSTERING TECHNIQUES IN COGNITIVE RADIO NETWORKS", Journal of Advanced Research in Dynamical & Control Systems, Vol.10,No.9,June 2018, pp.1364-1373.
[20]. R.GaneshBabu, and Dr.V.Amudha, "COMPARATIVE ANALYSIS OF DISTRIBUTIVE OPTIMIZED CLUSTERING TECHNIQUES IN COGNITIVE RADIO NETWORKS", International Journal of Engineering and Technology-UAE, Vol.7,No.3.27,August 2018, pp.504-507.
[21]. R.GaneshBabu, and Dr.V.Amudha, "DISTRIBUTED COOPERATIVE AI TECHNIQUES FOR COGNITIVE RADIO NETWORKS", International Journal of Recent Technology and Engineering, Vol.8,No.1S2, May 2019, pp.198-203.
[22]. R.GaneshBabu, and V.Amudha, "A Survey on Artificial Intelligence Techniques in Cognitive Radio Networks", In: Abraham A., Dutta P., Mandal J., Bhattacharya A., Dutta S. (eds) Emerging Technologies in Data Mining and Information Security, Advances in Intelligent Systems and Computing, vol. 755,pp. 99–110. Springer, Singapore, 2019.
[23]. R.GaneshBabu, and Dr.V.Amudha, "SPECTRUM SENSING CLUSTER TECHNIQUES IN COGNITIVE RADIO NETWORKS" Proceedings of 4th International Conference on Recent Trends in Computer Science and Engineering (ICRTCSE'16) in association with Elsevier-Procedia Computer Science conducted at Apollo Engineering College, Chennai, India, April 29-30,2016,pp.258-263.
[24]. R.GaneshBabu, P.Karthika, and V.AravindaRajan, "SECURE IOT SYSTEMS USING RASPBERRY PI MACHINE LEARNING ARTIFICIAL INTELLIGENCE" Proceedings of Second International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT-2019) in association with Springer Lecture Notes on Data Engineering and Communications Technologies with ISBN.No- 978-981-10-8681-6, conducted at RVS Technical campus, Coimbatore, India, May 23-24,2019, (Accepted and in Press).
[25]. R.GaneshBabu, P.Karthika, and K.Elangovan, "PERFORMANCE ANALYSIS FOR IMAGE SECURITY USING SVM AND ANN CLASSIFICATION TECHNIQUES" Proceedings of Third IEEE International Conference on Electronics, Communication and Aerospace Technology (ICECA 2019) with ISBN.No-978-1-7281-0167-5, conducted at RVS Technical campus,

Coimbatore, India, June 12-14,2019, (Accepted and in Press).
[26]. R.GaneshBabu, P.Karthika, and G.Manikandan, "POLYNOMIAL EQUATION BASED LOCALIZATION AND RECOGNITION INTELLIGENT VEHICLES AXIS USING WIRELESS SENSOR IN MANET" Proceedings of Second International Conference on Computational Intelligence and Data Science (ICCIDS 2019) in association with Elsevier-Procedia Computer Science conducted at The NorthCap University, Gurugram, India, Sept 06-07,2019, (Accepted and in Press).
[27]. R.GaneshBabu, M.N.Saravana Kumar, and R.Jayakumar, "DYNAMIC EXCHANGE BUFFER SWITCHING AND BLOCKING CONTROL IN WIRELESS SENSOR NETWORKS" In: Devendra Kumar Sharma., Valentina Emilia Balas., Le Hoang Son., Rohit Sharma., KorhanCengi. (eds) Proceedings of Third International Conference on Micro-Electronics and Telecommunication Engineering. Lecture Notes in Networks and Systems, Springer, in Press (2019).