Security Threat Identification and Prevention among Secondary Users in Cognitive Radio Networks

Reshma C R.[†] and Arun kumar B. R [††],

+Assistant Professor, Department of MCA, BMSITM, Research Scholar, VTU-RC, MCA Dept. BMSIT&M, Yelahanka, Bengaluru
.[†].[†] Professor, Department of Computer Science & Engineering, Research Supervisor, VTU-RC, Dept. of MCA,BMSIT&M ,Yelahanka, Bengaluru

Summary
The Cognitive radio (CR) is evolving technology for managing the spectrum bandwidth in wireless network. The security plays a vital role in wireless network where the secondary users are trying to access the primary user's bandwidth. During the allocation the any malicious user either he pretends to be primary user or secondary user to access the vital information's such as credentials, hacking the key, network jam, user overlapping etc. This research paper discusses on various types of attack and to prevent the attack in cognitive radio network. In this research, secondary users are identified by the primary user to access the primary network by the secondary users. The secondary users are given authorization to access the primary network. If any secondary user fails to provide the authorization, then that user will be treated as the malicious user. In this paper two approaches are suggested one by applying elliptic curve cryptography and the other method by using priority-based service access.

Key words: *malicious user, security, attacks, threats, cryptography*

1. Introduction

The evolving wireless technologies for different wireless application led to the scarcity of the spectrum bandwidth. The cognitive radio networks has two different types of user i) primary user (PU) who owns the spectrum ii) secondary user (SU) who utilize the primary user's network. The cognitive radio is capable of configuring the devices. The reason for cognitive radio technology is to maximize the utilization of the spectrum due to the scarcity of the spectrum. The resources are shared by both primary and secondary users.

Table1: Different frequencies used for wireless communication

3KHz	Marine Radio Navigation
30KHz	
300KHz	AM Radio
3MHz	Short Radio
30MHz	Television
300MHz	Mobile phones ,wi-fi
3GHz	Satellite communication
30GHz	Astronomy,Satellite Communication
300GHz	

Due to many applications which uses WI-FI technology there is a spectrum scarcity. While sharing the resources, there can be threat to the network. The CR users are also vulnerable to various attacks. The attacks caused by various reason can result into Denial of services, throughput, energy etc. The spectrum can be secured before the attack has attempted. There is a need to identify different security threats and prevention of these threats [6].

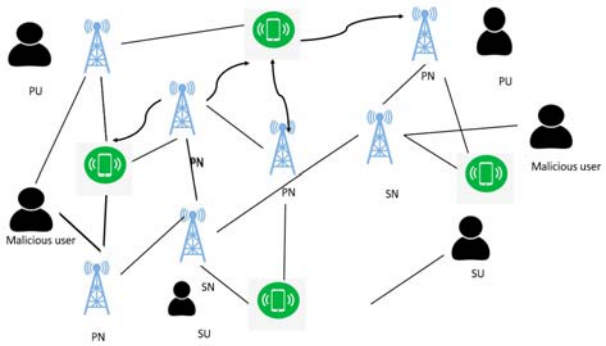

Figure 1: Malicious user pretend to be primary user to access network

The user can pretend either to be primary user or secondary user to access the vital information available in the primary network station. Hence security measures are considered to prevent unauthorized access to the primary network.

1.1 System Architecture for Cognitive Radio Network (CRN)

The wireless network follows IEEE standards 802.11 which comprises three working groups such as: 802.11 wireless LAN, PAN, MAN. The devices must be controlled and optimized for secured communication which can be achieved through software Defined Network (SDN). To access the wireless network access points must be deployed with the corresponding software's which supports IEEE 802.11. The author prescribed ethanol architecture which

Manuscript received May 5, 2021
Manuscript revised May 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.5.24

controls access points in wireless networks. To control Aps and other devices ethanol uses south bound interface. To manage home networks north bound interface is used [11]. The below architecture consists of allocation of bandwidth, webQoE, Load balancing, App Aware, Fault Detection and Hand over [12][13][14][15].

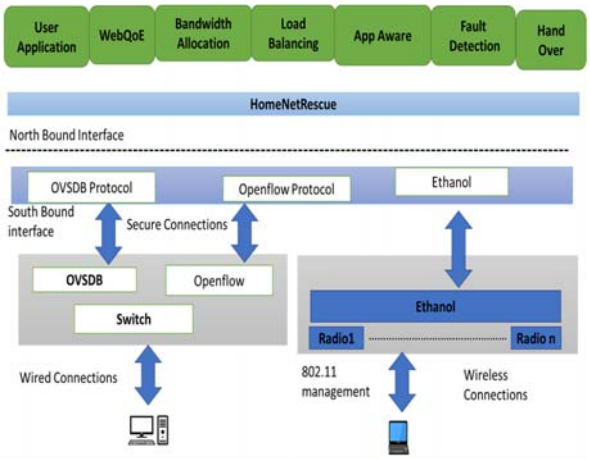

Figure 2: Ethanol implementation [source: Henrique and et.al Ethanol : A Software Defined Architecture for IEEE 802.11]

1.2 Proposed Architecture

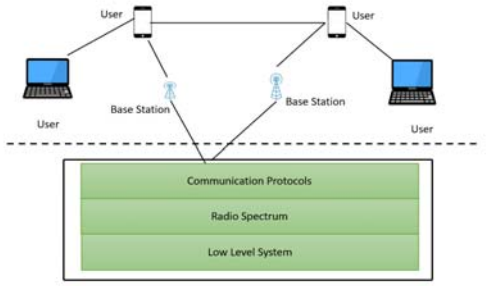

Figure3: Radio communication diagram

The above diagram, indicates the communication between the devise and the underlying communication mechanism. The low-level mechanism consists different hardware devices above which the radio spectrum is available. Through applications the radio communication is possible which are comprised of different protocols to manage various task such as file transfer, online video streaming, sharing audio and video files etc. The system counter to various security threats at different layers of network which is shown in figure 4. The network architecture for cognitive radio network is shown below where in network layers are available for communication in wi-fi technology. The user is trying to have an access to the network layer.

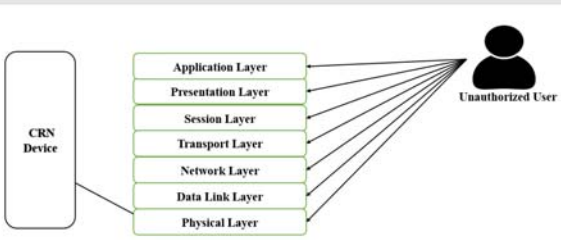

Figure 4: Accessing the network layer

2. Literature Review

The literature review is carried out for identifying security issues at different levels. There is a requirement to address the security at different levels and different layers of network. Sensing and emulation of primary signal (detecting and verifying the signal). Spectrum management (detecting, verifying channel capacity and allocating appropriate channel to cognitive users)
Checking interface level, signal strength and energy detection secure communication.
The below table describes the different types of attacks, in which layered the attack caused.

Table 2: Types of attacks

Attack Type	Network Layers	Reason	Measures to be taken
Primary and secondary User Jamming	Physical	Lack of knowledge About location and unclear access rights to cognitive users	Location consistency checks compare the signal strength and noise level
Primary signal sensing	Physical	Low level primary signal will be missed	Energy based sensing wave-form based sensing cooperative detection of PU
Overlapping secondary user	physical	Location based hard to prevent	Use game models and Nash equilibrium techniques to detect transmission power of Sus
SU unauthorized gain in bandwidth pretending as primary user /False feedback	MAC	Malicious SU tweaks with higher power bandwidth and feedback information to gain signal	Trust management on SU for resources hungry and collaborative management of systems objective functions by controlling radio parameter

Increase interference by malicious mode	Networks	Compromising with malicious node	Appropriate local spectrum sensing controller. Eliminating internal hidden parasite node
Ripple effects	Network	False information about spectrum assignment	Continuous trust management process on Secondary users
Key duplication	Transport	Break the cypher system	Reinvestigate the protocol activity in the context of session. Use secure protocols with robot distribution of key management
Jelly-fish	Transport	Effect on throughput	Trust of node by verifying the packet loss

Based on special characteristics security threats can be determined

i) Security Threats in AI characteristics- it involves reasoning and learning. A reasoning engine is set of logical interference rules. Cognitive radios need some policies for reasoning to deal in different environment. Learning engine in cognitive radios are capable to leave from past experience and current situation and then predict optimal spectrum to select.

ii) Policy Threats: It occurs due to lack of policies present and lack of knowledge base that attacker or malicious user can modify the actual statistics. If an attacker gets unauthorized access of knowledge base then the attacker can modify or delete the existing policy and inject false policies in knowledge base.

iii) Learning Threats: Learning comes from the past experience and the current situation to make the prediction. Learning engine can make wrong decision about the spectrum, if the knowledge base is wrongly updated.

iv) Security threats in dynamic spectrum access: during cooperative sensing, the cognitive user can sense false information in hostile environment or due to presence of malicious users. Sensors can be malfunctioned using some kind of malicious code. False sensing would not detect available spectrum or it can detect busy spectrum.

v) Primary user emulation attack: These attacks prevent the secondary users using the available bandwidth for communication. Intend the malicious user can utilize the spectrum. If there are unoccupied channels then the malicious user pretends to be primary user and attacks all the free channels. PUEA can be classified into two categories a) Malicious PUE Attack- wherein the attacker prevents the secondary user to utilize the available spectrum. b) selfish PUE Attack-It is performed by the selfish secondary user. If a selfish node detects idle spectrum, it prevents other secondary user to detect spectrum so that selfish user could get full access of spectrum. Sometimes the PUE attack is raised by the malicious user imitating as primary user to avail all the resources [9]. The data exchanges between the node are modified by malicious user which in turn leads to denial of services [8].

vi) Objective Function Attack-there are various radio parameters such as modulation, coding, and security. The attack force to enable CR to select sub-optimal value by altering objective function [7].

vii) Lion Attack-it is a kind of attack in CRN performed by an attacker at physical layer to degrade the performance of transmission control protocol (TCP) at transport layer. The secondary user performs spectrum handoff if primary user is active leading to temporal disconnection at physical layer. Data segments sent by TCP can be lost or delayed during handoff process at physical layer by degrading TCP throughput. TCP maintains a time if the receiver doesn't receive acknowledge it assumes that the data is lost. In lion attack the attacker performs PUE attack or Jam channel [2].

Attack Prevention Measures

Physical Layer Authentication: It includes physical layer validation, the physical properties of the flag to separate the essential client initiating assault from the first PU. The properties of physical layer are identified in two categories i) utilizing transmission specific characteristics ii) using channel-specific features.

In physical layer validation strategy incorporates the validity, identification and highlight recognition strategies. In validity recognition strategy hypothesis testing is carried out.

D= {PUEA H<Ht
PU H>Ht}

Ht- Threshold voltage of channel
H stands for channel property
D for the decision
High Layer Authentication Method
This layer uses cryptographic techniques for the authentication. This method uses public key cryptography. In this encryption and decryption can be done using different but related key.

$X= D_{KU} [E_{KR}[X]]$….(1)
$X=D_{KR}[E_{KU}[X]]$….(2)

Here X-Message
D-Decryption
E-Encryption
KU-public key
KR-Private key

In this approach, messages are transmitted using private key and at the receiving end messages are decrypted using public key.

Procedure for transmitting a signal

The client generates a private key and sends along with the signal, since the transmitter only knows the private key the data cannot be signed by any malicious user.

Procedure for the receiving signal

A receiver should recover the public key from the central facility using the public key appropriate transmitter signal can be decrypted and verified [3].
Quad-Type encryption of Data (QED) provides four tier encryption procedure to the main user. If a user needs to join a CR Network, it must start trust arbitration with the channel at closer network. The algorithm works on the basis of three level
Adaptive distance mechanism RSSI
Distributed energy power
User ID in frame format
Description level:
Step 1: The data is encrypted using distance as the key
Step 2: The result is encrypted using energy as it key
Step 3: Again the result is encrypted using user's ID as the key [4]
In delegation user authentication framework, SUs should be serviced by secondary network over the CRN by delegating authentication from PN which achieves the security from selfish nodes and malicious node by providing authentication, unthinkability, anonymity, PU protection, no registration and conditional traceability. The author suggests three phases for the secure authentication framework as a basic security and privacy module for CRN.
Authentication may be either online or offline. In online authentication the process requires that Secondary Network (SN) must connect to primary network (PN) when a new SU demands authentication. In offline the SN obtains the necessary parameters obtained from PN in advance. In setup and registration process PN generates process PN generates the large prime no's and a generator P in the additive group G. later PN chooses two private keys and computes the public key. Each computed value is stored in corresponding Sus smart card.
In online registration, first the SU sends a login request to SN. Later SN generates the ids and random no when SU inserts the smart card. It generates two random number and computes the hash chain. Later it verifies and computes symmetric key. PN decrypts using the secret key and verified by corresponding to SN. SN decrypts and verifies for SU, later it checks for the existence. In offline, the hash key parameters are derived from the online authentication [5].

3. Proposed Methodology for Preventing the Attacks

In this research paper, different methods are suggested for preventing the attack. The secondary user has to be identified where the secondary user can also be a malicious user. To identify the genuine SU, the key exchange algorithm is suggested if there is only one single user at any time t. In case of multiple secondary user's, it's very hard to identify the genuine SU, in that case priority-based algorithm is suggested.

3.1 Method 1:

In this method, Elliptic curve cryptography is applied where the key is shared between the primary users and the secondary user. In this approach it uses two different types of keys i) public key and ii) private key. Both PU and SU picks up a private key and exchange publicly to generate key to encrypt the message and to access the service request and response.

Steps1: Create public keys for both primary user and secondary user. Let p1 be the primary user key and p2 be the secondary user
Step2: primary user selects a private value m and secondary user selects a private value n
Step3: Both the user's computes the public values

$a=p_2\text{^}m \bmod p_1$ ----1
$b=p_2\text{^}n \bmod p_1$ -----2

Step 4: primary user and secondary user exchange the values of a and b
Step5: PU receives b, SU receives a
Step 6: the user creates a symmetric key

$Km = b^m \bmod p_1$

$Kn = a^n \bmod p_1$

Step 7: Km =Kn is the shared key
The above approach is considered for single secondary user and primary user.

3.2 Assessing the service for multiple user

In case of multiple secondary user's, key exchange for multiple user it is a tedious job. The alternative method for identifying the secondary user to mitigate the attack is based on the priority.
For providing secured service to the secondary user, priority-based service access algorithm (PBSAA) is used. In this approach the primary user verifies the secondary user using user token no and the random number generated for the secondary number. In this case time is a constraint where the time is valid only for 10 min of token exchange.

PBSAA procedure steps

Step 1: Secondary user sends a request to the primary user.
Step 2: Primary user sends the channel status either 1 or 0 where 1 denotes the channel is busy and 0 represents the channel is idle.
Step 3: Secondary user confirms. Primary user generates the token number and shares the number with secondary user.
Step 4: Secondary user generates a random number at time t and sends the information along with the token number.
Step 5: Primary user verifies the random number, token number and time
Step 6: If it is valid the services will be provided by the primary network else sends the report as unauthorized users.

3.3 Algorithm

1. Let n be the number of SU
2. Let m be the number of PU
3. For j->0 up to j <m

   Generate Tn for PU
   For i->0 up to i<n
   For j->0 up to j<m
   Sn=Tn
4. For i-0 to n
5. Sui<-Rand (1,10)
6. Check (sn, t, r)
7. For i=0 to n
8. S_{ti}= Generate time of request
9. If(Sn==Tn)
10. If(r>=0 r<10)
11. Allow Service Access
12. Else
13. Deny service for secondary user
14. Else
15. Token not matching

3.4 Flow chart

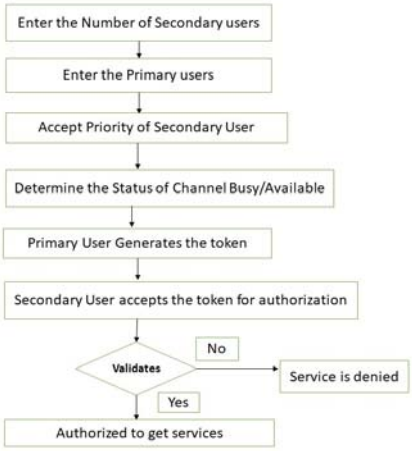

Figure 5: Service Generation

Different types of services

There two main types of services:
- Differentiated services
- Integrated services.

Differentiated services: it ensures that each secondary user gets the bandwidth and the services are provided by the primary users. Later the services can be considered as type-p and type -A.
In type-p service the secondary users are allocated with the bandwidth provided by the primary users. If the spectrum is idle for too long duration, then the maximum usage will be taken by the secondary user.

In type-A the secondary user will raise the demand, the primary user will evaluate the required bandwidth for the secondary user. If there are a greater number of secondary user then there is traffic which in turn reduce the performance of the service.
Integrated services: in this type of service, the secondary user gets the service from the primary user depending on the reservations done by the secondary user. The resource reservation protocol is used for reserving the bandwidth.

During the services, traffic can be generated in the network by the secondary user. The traffic can be managed by applying traffic shaping algorithm.

CCA (Channel Capacity Algorithm) for managing the Secondary users' services. In CRN, there are multiple secondary user who are in waiting state to get the channel allocated and these user's traffic has to be managed in the network to provide the service. The working of algorithm is given below:

Where the secondary users create a traffic in the network since secondary users are more in number than the primary user. The primary user displays the channel state when the channel is idle, during this stage the secondary user will be allotted the channel based on the reservation.

Step-1: Assume the capacity of the spectrum is β.

Step-2: The secondary users are allocated the channel at the rate λ.

Step-3: check the channel capacity. If the channel is already allocated, discard the remaining users.

Step-4: If channel allocated to secondary user has completed with the task at the rate λ else the channel will be idle till next user is allotted.

Flow Chart for Managing Secondary users' traffic

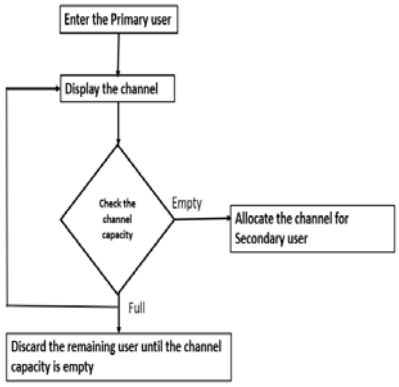

Figure 6: Identifying channel capacity

4. Experimental Results

The experiments were conducted using Scilab tool. The output is considered for both the methods i.e. key exchange algorithm and priority based access service. In Diffie Hellman key exchange two prime numbers are chosen and keys are exchanged publicly. The results are shown below for two different key values and both share a common key.

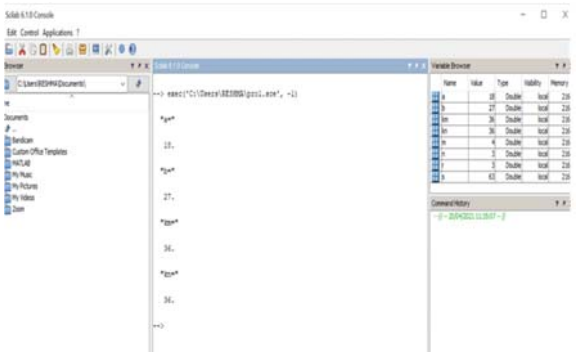

Figure 7: Key Exchange between PU and SU

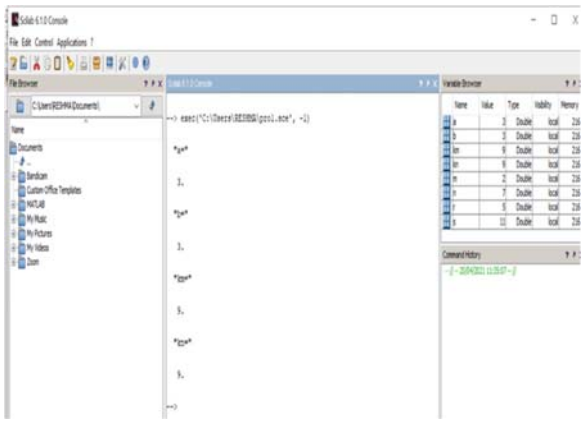

Figure 8: Key Exchange between PU and SU

Figure 9: Availability of spectrum

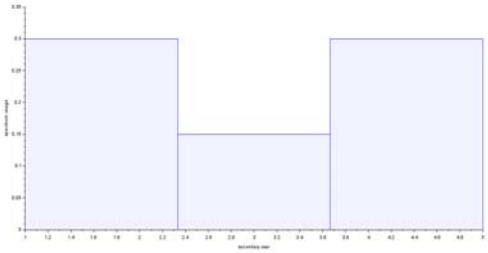

Figure 10: Histogram of priority of secondary user based on usage

5. Conclusion

In this research work, the system demonstrates the accessing of services by secondary users. This paper recognizes the malicious user based on the authorization of secondary user wherein the provision of token is provided by the primary user. The validity of the token is considered from the clock generated by the primary user. The secured spectrum management is vital and attracted several researchers across the world. The future work focuses on improved Block-chain based spectrum management to mitigate the different attacks.

6. References

[1] Yenumula B Reddy, "Security Issues and threats in Cognitive Radio Networks", The Ninth Advanced international conference on Telecommunications, AICT 2013.
[2] Kamal Kumar Chauchan, Amit Kumar Singh Sangar, "Survey of Security Threats and attacks in Cognitive Radio Networks".
[3] B. Sarala, S Rukmani Devi,M Suganty,S Jhansi Ida", A novel Authentication Mechanism for Cognitive Radio Network", International Journal of Recent Technologies Engineering (IJRTE), vol-8 Issue 4, November 2019.
[4] T. Lakshmi Bai, Dr Parthasarthy "Encryption Algorithm for Defending PUE Attack in Cognitive Radio" International Journal of Applied Engineering Research vol12, November 2019.
[5] Hysung Kin, Em Kying Ryu, "Delegation Based User Authentication Framework over Cognitive Radio Network", 2 December 2017.
[6] A.G. Fragkiadakir, E.Z .Tragos and I.G Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks,"IEEE Communications surveys and Tutorials, 2013,vol 15, Issue 1,PP 428-455.
[7] T. Charles Clancy, Nathan Goergen, "Security in Cognitive Radio Networks Threats and Mitigation.
[8] G, Jakimoski and K.P. Subbalkshmi, "Denial-of-Service Attacks on dynamic Spectrum access Networks", IEEE Cognets workshop IEEE International Conference on Communications May 2008.
[9] Aliyu Abukakar "An Investigation of Performance Versus Security issues in Cognitive Radio Networks", International Journal of Scientific and Engineering Research, volume 7, Issue 9 September 2016.
[10] Kurose and Ross "Computer Networking-A Top-Down Approach Featuring the Internet".
[11] Henrique Moura, Alisson R Alves, Jonas R A Borges, Daniel F Macedo, Macros A M Vieira "Ethanol: A Software Defined Networking Architecture for IEEE802.11 Networks, July 2015.
[12] A.R. Alves, H.M. Durate, J.R.A. Borges, V.F.S.Mota, L.H. Cantelli, D.F. Macedo and M.A.M. Vieria, " HomeNetRescue: an Software Defined Network service for troubleshooting Home Networks", IEEE/IFPF Network optimization and Management Symposium, April 2018.
[13] H.D.Moura,G.V.C Bessa,M.A.M Vieria, D.F.Macedo "Ethanol: Software Defined Network for 802.11 wireless Network", IFPF/IEEE Symposium on Integrated Networks Management,pp 388-396,2015.
[14] H.D. Moura, D.Fernandes Macedo and M.A.M Vieria "Automatic Quality of experience management for wlan networks using multi-armed bandit",IFPF/IEEE Symposium on Integrated Networks Management pp 279-288, April 2019.
[15] J.C.T Guimares, H.D.Moura,J.R.Borges,M.A,Vieria, L.F.Vieria and D.F.Macedo "Dynamic Bandwidth Allocation for Home and Soho Wireless Networks" IEEE Symposium on Computers and Communications, 2018.

Reshma C.R received MCA, degree from VTU, Belagavi. Working as Assistant Professor in BMS Institute of Technology and Management with 12 years of experience. Currently Pursing Ph.D in VTU.

Dr.ARUN KUMAR B.R , Professor in Computer Science & Engineering in BMS Institute of Technology and Management awarded the degree, Ph.D in Computer Science from DRAVIDIAN UNIVERSITY, a State University of Andrapradesh Govt., recognized by UGC, established in the year 1997, for his Thesis entitled, " Cross Layer Design for Quality of Service Multicasting in Mobile Ad-hoc Networks" on 20-9-2012. He carried out his research work under the guidance of Dr.Lokanatha.C Reddy, Professor, CS dept., Dravidian University and Dr.Prakash.S Hiremath, Professor, CS dept., Gulbarga University. He has been awarded with three post graduate degrees, MCA, M.Phil (CS) M.Tech (CS& E) from Kuvempu University, M.S University and from Dr.MGR Educational and Research institute University respectively. He obtained his post graduate diploma in IPR from National Law School of India University, Bangalore in July 2012. The author has published 70+research papers in National/International Journals. He has presented and published nearly 20+ papers in the National/International Conferences/proceedings including IEEE international conferences. He has authored one Book and 6 Book chapters on engineering contemporary concepts.

He is guiding 4 Ph.D scholars under VTU, delivered nearly 50 expert talks, working as a MCA BOS chairman, VTU. He is a research paper reviewer/editorial board member for various indexed journals. He chaired several sessions in international conferences. He is member/mentor in Department advisory boards of several UG/PG programmes and BOE of different universities.