Jurnal Teknologi

Full Paper

LIGHT AND SECURE COMMUNICATION ALGORITHM FOR COGNITIVE RADIO NETWORK BY USING LABYRINTHINE AUTHENTICATION FORMULA

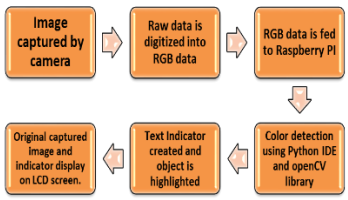
Fawad Salam Khan[a*], Talha Naqash[b], Muhammad Ibrar Khatak[b], Raja Masood Larik[a]

[a]Faculty of Electrical Engineering (FKE), Universiti Teknologi Malaysia (UTM)
[b]Department of Computer Science, Bahria University Islamabad, Pakistan

Article history
Received
13 April 2014
Received in revised form
2 April 2015
Accepted
1 August 2015

*Corresponding author
fawad.salam@fkegraduate.utm.my,

Graphical abstract



Abstract

Facilities for different sight and sound provisions in remote systems requests extra transmission capacity in the radio frequency range. Effective range administration calculations are important to accomplish massive accomplishment in remote correspondences. Usage of licensed spectrum is increasing day by day so Cognitive Radio is proposed as a solution to meet the demands. CR is a symbolization procedure that distributes the authorized range (the licensed spectrum) despite the fact that facing least obstruction to the authorized clients. In this paper, we investigate the versatile qualities of cognitive radio in secure and dependable correspondence. Anyway the inquiry is the way to make the correspondence dependable such that there happens no spying and data spillage. The conceivable results incorporate coordinating the benefits of spread range balance, utilizing encryption calculations (Encryption keys), and its possibility to switch over different recurrence groups. We concentrate on the different requisitions of CR and the various philosophies which empower a safe Communication system.

Keywords: Cognitive radio network, authentication, security

1.0 INTRODUCTION

Cognitive Radio (CR) [1-3] provides the guarantee of keen communication systems that can gain from and adjust to nature's domain. Many researchers have proposed many ideas about CRN and taking calculations that permit CR to work ideally with a huge assortment of diverse circumstances. On the other hand, as with a lot of people new innovations, introductory examination has not kept tabs on safety parts of CR. Regularly safety is constantly "blasted on" sometime later by including a connection confirmation and encryption. This commonly works well for information crossing a remote system, not so much for things key to the operation of the distant link itself. Since CRs can adjust to their surroundings and change how they impart, it's essential that they select ideal, secure method of correspondences. Information uprightness and secrecy could be taken care of by algorithms related to security at above layer, that's why; we concentrate on ambushes central to this task was subsidized by the Laboratory for Telecommunication Sciences, US Department of Defense. Conclusions communicated in this archive speak to the creators, and ought not be viewed as an authority slant or supported by the Department of Defense, or US Federal Government. Cognitive radio itself and autonomous of its higher-layer interchanges procedures. The idea proposed in [4] about cognitive radio is to characterize as a specialized standard

equipped to adjust itself alterable to use the radio assets at the time, Frequency, and space suits. A specific frequency range is isolated into more diminutive frequency groups. Every frequency band is dispensed to authorized essential clients. It is being watched tentatively that significant bits of frequency groups hang idle over considerable interims of the instance. These idle shares of the range are acknowledged as "spectrum holes " or "white spaces". The cognitive radio can use these range gaps successfully and brilliantly while not forcing forbidden impedance to neighboring authorized essential clients. For instance: "television White Spaces" in the TV range speak to range gaps and are utilized by the CR with the end goal of sending additional remote administrations. Due to its various attributes and adroit adjustment parameters, CR discovers a great deal of provisions in the different fields requesting dependable and secure correspondence, for example, military requisitions, open wellbeing provisions [5, 6], and so forth. It is their remarkable versatility that makes the correspondence imperceptible for outside dangers and consequently permits the private discussions to be completed in a secured manner. In spite of the fact that in the present innovative period, unlimited results are described for the different protection worries that are the subjects of examination around the entire logical brotherhood, yet not many of them have been acknowledged for all intents and purpose. These cognitive radios do experience the ill effects of a ton number of tests, for example, on neighbor revolution in the radio system, range determination and sensing, recognizing the client area and adjusting itself to its requests and so forth. Cognitive radio, when consolidated with the spread range adjustment systems, gives a very secure correspondence position impervious to ponder narrowband sticking and other block strategies [7]. Spread range method, as a result of its special characteristic to make the information look like clamor, is truly secure as in the sticking and the meddling components are unable to recognize the information (blended with commotion) being sent over the channel and henceforth it may be a conceivable answer for abstain from listening in or data spillage. Indeed the different encryption strategies, for example, public key and private key encryption calculations could be utilized in pair with CR to give a manifestation of protected correspondence. The encryption calculations verify that the key at the source side ought to be given by the collector (much same as the pseudo-arbitrary succession utilized within the spread range modification) for right data recovery and henceforth guarantees the security and likewise keep the pernicious clients from taking control over the framework, obstructing the right to gain entrance to other auxiliary clients. Artificial intelligence (AI) engine techniques are now used in our wireless devices, but it is also a considerable thing that these engines could be given forged tangible include by foes, and forged enter influences its convictions and conduct as shown in Figure 1. We have to take a gander at the threats we would conventionally see in societal communication, instead of Communication systems. We characterize three classes of assaults: tangible control ambushes against approach radios, conviction control strike against taking in radios, and multiplying toward oneself conduct prompting cognitive radio infections [8]. Numerous sorts of assaults control the conduct of a CR framework such that it demonstrations either sub ideally or even malignant. Securing against assaults like these can't be carried out through cryptographic methods. It includes giving some measure of instinct and practical judgment skills into a cognitive radio that permits it to expose convictions that don't bode well.

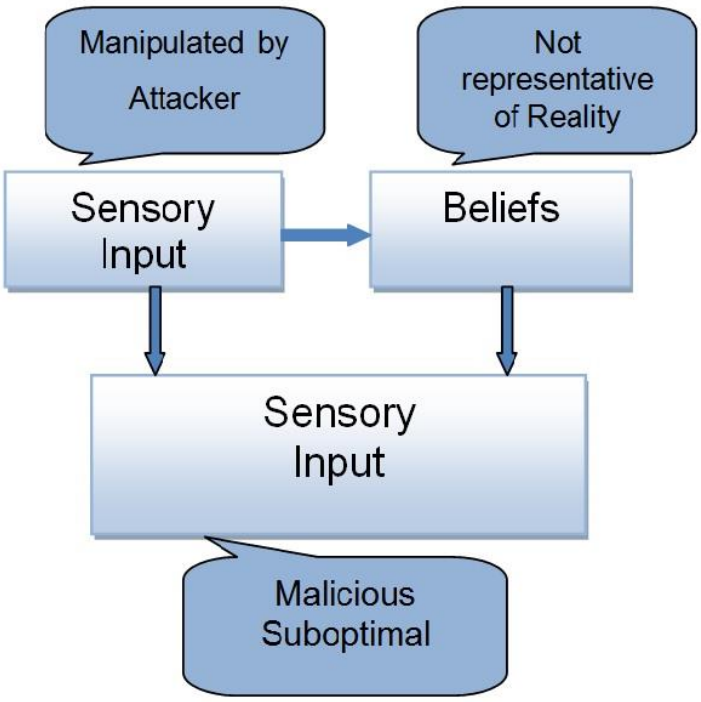


Figure 1 Relationship between sensor include, convictions, and conduct in a cognitive engine, indicating how a foe controlling tangible information can change the convictions and conduct of a cognitive radio

2.0 PURPOSE OF SECURE COMMUNICATION

In this profoundly aggressive world, the dangers of financial also political secret activities excessively have expanded putting a ton of government and singular property in danger. A ton of strategies being utilized in completing correspondence is unstable as in their security might be broken out and critical discussions might be listened to or recorded. Indeed a significant number of them don't require the confirmation of the singular reached. For instance: the GSM administrations, however, they give great connectivity yet they are inclined to numerous security dangers as examined prior. Indeed the

standard cellular telephones don't give end to end security. Thus we can say that the safe correspondence is obliged to associate and give transmission, preparing, recording and overseeing for different purposes, for example, secure phone and system supplies and encryption administration, secure information joins in and from ground and satellite based remote stages for constant data accumulation, interchanges between manned space flights, and so forth [8].

2.1 Conceivable Results Towards Secure Correspondence

Numerous existing advances have such a capacity, to the point that if joined with the cognitive radio innovation can give a corresponding configuration free from regular security dangers [9]. Spread ranges balance organization is one of them. Indeed the essential encryption innovations, for example, open key and private key encryption could be utilized as a part of coupled with cognitive radio for such purposes. We will examine the likelihood of a protected correspondence arrange by utilizing spread range balance strategy with Cognitive radio. First and foremost, the essential spread range tweak strategy will be talked about [10].

2.2 Modulation and De Modulation in Spread Spectrum Technique

As stated by the standard definition: "Spread range (SS) [11] is a method of transmission in which a sign possesses a data transfer capacity in overabundance of the base important to send the data: the band spread is proficient by method for a code which is autonomous of the information, and synchronized gathering with the code of the beneficiary is utilized for de-spreading and resulting information recuperation". As indicated in Figure 2, the information sign is initially increased with a pseudo-arbitrary arrangement, otherwise called spreading code and afterward adjusted (for the most part utilizing stage movement keying) and after that transmitted over the channel. On the collector side, as demonstrated in Figure 3, first the approaching indicator is checked for some commotion substance (contingent on the clamor qualities of the channel) and in the event that it holds some commotion, then the clamor is evacuated first and afterward the sign is demodulated (depending upon the balance system that has been utilized at the transmitter side). Presently, the demodulated sign is increased with the same pseudorandom arrangement that was utilized within the starting and the last data indicator is acquired. The beneficiary area is as appeared. In this manner we see that in a SS procedure, to recover the first indicator being sent from the sender side, the information of pseudo-arbitrary grouping is must. Additionally, the information, having been increased with the PN arrangement gets changed over to a wide band sign picking up the shape and qualities like commotion. This novel characteristic of the spread range tweak method makes it recognizable from the other existing balance procedures in such a path, to the point that it makes the information covered up around the arbitrary clamor display or created in the framework and thus giving a getaway from any outsider (attempting to sneak into the continuous discussion). This nature of spread range balance calculation could be misused to give a safe and solid nature's turf [12, 13].

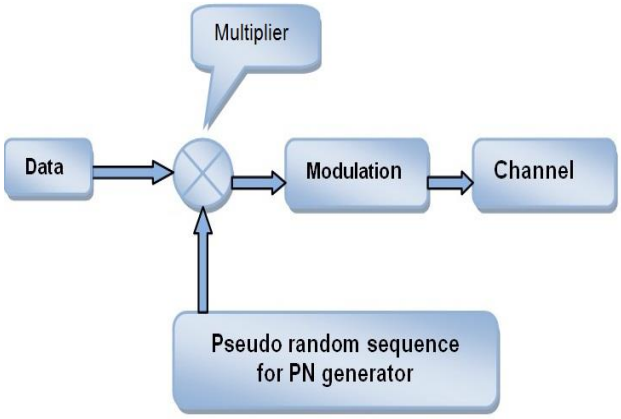


Figure 2 Sender side in SS

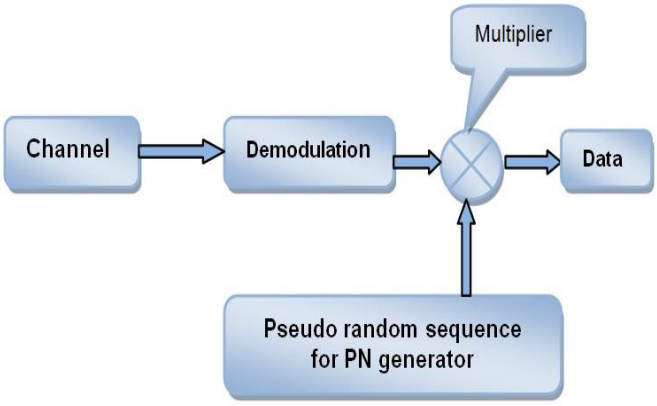


Figure 3 Receiver side in SS

2.3 Encryption Methods for Communication

It has turned into a need to keep the information escaped the prying eyes to administer security. What's more to accomplish that different encryption methods have been proposed, for example, symmetric and deviated encryption strategies [14]. A symmetric encryption system is otherwise called private key encryption calculation. A couple of such strategies are: RSA, Elliptic, SHA and so on. In such a strategy, both sender and beneficiary have a private key, which they have to impart before the transmission of the information begins. What happens really, the sender scrambles the information with the private key of the beneficiary and the collector unscrambles it utilizing the same private key. Consequently, such an encryption calculation utilizes just a solitary key.

However, if there should be an occurrence of open key encryption (DES, Triple DES, AES) technique we have two sets of keys connected with a client. Both sender and recipient have a set of open and private keys connected with them. These open keys are made available to the others over the system before the information transmission begins. Sender scrambles the information with general society key of the beneficiary and the collector unscrambles it utilizing its private key and this is the way a deviated key calculation work. Despite the fact that the private key encryption calculations are quick, however looking from the point of view of security acquired open key encryption procedures have an edge over the private key encryption method.

3.0 SECURE COMMUNICATION METHOD FOR CRN

According to the IEEE 802.19 standard [15], the key segments of a cognitive radio system are the accompanying:

- Incumbent client insurance utilizing range sensing,
- White space database access
- Security in getting to database and authorized range,
- Range imparting

For the ideal learning of the essential clients in the authorized range, the auxiliary clients are anticipated to have entry to the white space database as in Figure 4, i.e., a database holding data of essential clients in every last authorized band. The Federal Communications Commission (FCC) has ordered range sensing [16] alongside access to this white space database. Range sensing is a system utilized by a CR to recognize range gaps in the authorized range. Existing exploration work has proposed utilization of physical layer, and medium access control (MAC) layer aspects of the essential client sign to discover such range openings. The location procedure, or rather range sensing includes two sorts of lapses: mis-discoveries (presence of an authorized client in one band is located to be sit) and false cautions (an unmoving band is distinguished as a possessed band). The IEEE 802.19 standard is proposing a joint discovery and access to the white space database for better range sensing. Be that as it may, two essential inquiries emerges: (i) validate a CR before giving a select access to the white space database and (ii) confirm clients in correspondence before offering data about the white space database. Hence, security in the setting of cognitive radio networks is managed in three stages:

- Step1: Authenticate a CR,
- Step2: Authenticate two clients in correspondence
- Step3:ensure security throughout the interim of correspondence between clients

In this Paper a proposed method is described to mutually authenticate the client and the database in CRN environment

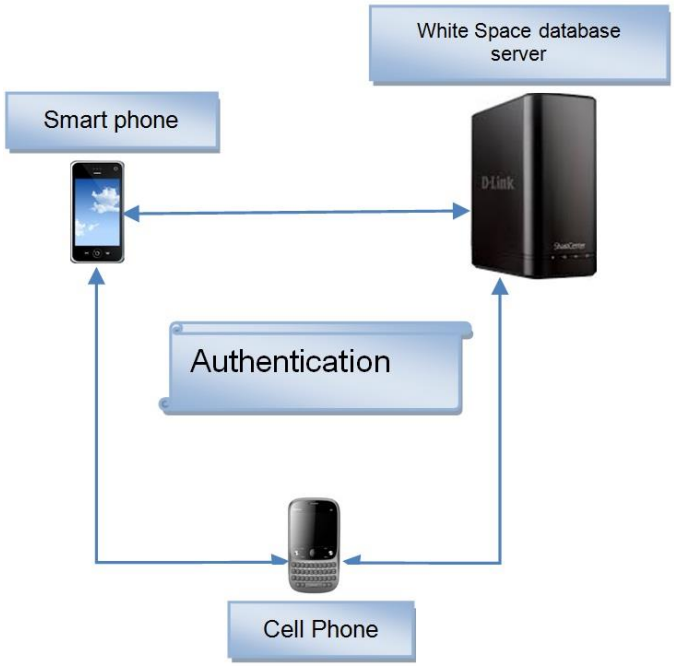


Figure 4 Security in CRN

A. Authenticate a Cognitive user

Each user will authenticated by the server then can communicate with each other both users will be authenticated by the user with a secure method which is described in Figure 5. By using this advance method each user is authenticated securely. Let's suppose that the white space database server is SJ and the cell phone is used equipment (UE).

Server (Sj) generates two large prime numbers "P" and "q" for the Rivest, Shamir and Adleman Protocol (RSA) and calculates public key (e,n) and private key (d,n) for it. User Equipment (UE) will choose a unique IDi of a fixed bit length and launch a request. Sj will calculate Mi by using the UE' IDi send to UE via secure channel. Two random numbers "a" and "b" are chosen by the Sj and UE respectively; three random nonces are also selected for the proposed solution.

Where $Mi=(IDi||h(IDi))d \bmod N$ (1)

$n= (P-1)*(q-1)$

And

$N= P *q$ (2)

UE sends a request to get services and the nonce1 to HeNB (Sj) so the Sj calculate "X" for DH, "A=h(X||IDs||nonce1)" where IDs is the identity of the Sj then "B=(A||h(A))d mod N" is calculated by using the values of A and private key element "d" and send a message m2=(X,B,nonce2) to wireless device. A pre installed application in the wireless device will compute the "Y" for DH to generate encryption key "Gij". "C=Mi h(Qij||Y||nonce2)" is a secure credential as the generation of Mi require "d" which is not publically available. Now UE will send message "m3= (Y,C,I)" and I= Eij (IDi||nonce3||nonce2). Sj will generate DH secure key "Gij" and also decrypt the m3 and get the value of "Qij". Now if the

$$MIDi\ h(Qij||Y||nonce2) = Ce \bmod N \quad (3)$$

Otherwise connection will be terminated; in fourth message m4 hash of the nonce3 is calculated and sent, UE will verify it by comparing sent nonce3 and received nonce3. In m3 UE sent a credential which is used to prove that UE has a valid record of Sj without showing its value

$$C = MIDi\ h(Qij||Y||nonce2)$$

The "C" is calculated in such a particular way that only UE and the Sj can calculate it.

B. Communication in Secured CRN

Once the CRN users are validated, the following step is to guarantee security in the data being imparted. It is accepted that all the cognitive clients have notable data about the essential client used in the wanted Spectrum. As far as the operation of a cognitive radio, an operational radio recurrence range is separated into N non-covering sub-groups. The set of sub-groups is indicated by Sub = {1, 2, . . . ,N}. Taking into account the notable data, it is further expected that the likelihood of essential client used in each one sub-band is known to every cognitive radio. Give us a chance to characterize pi as the likelihood of the ith sub-band being free at any moment of time. As stated by these sub-band free probabilities, the cognitive radio isolates the sub-groups into three separate classes: little likelihood, huge likelihood, and moderate probabilities of being free. The amount of sub groups with little probabilities of being free are spoken to as Nfreesmall , with huge probabilities as Nfreelarge , and with moderate probabilities as Nfreemod .The circulation of Nfreesmall is as in [16] and the likelihood that there are k free sub-groups is

$$Pr(N_{free_{small}} = k) \simeq \frac{\lambda_s{}^k e^{-\lambda_s}}{k!} = Pr_{Poi}(N_{free_{small}} = k),$$

where λg = Σi∈Subsmall pi

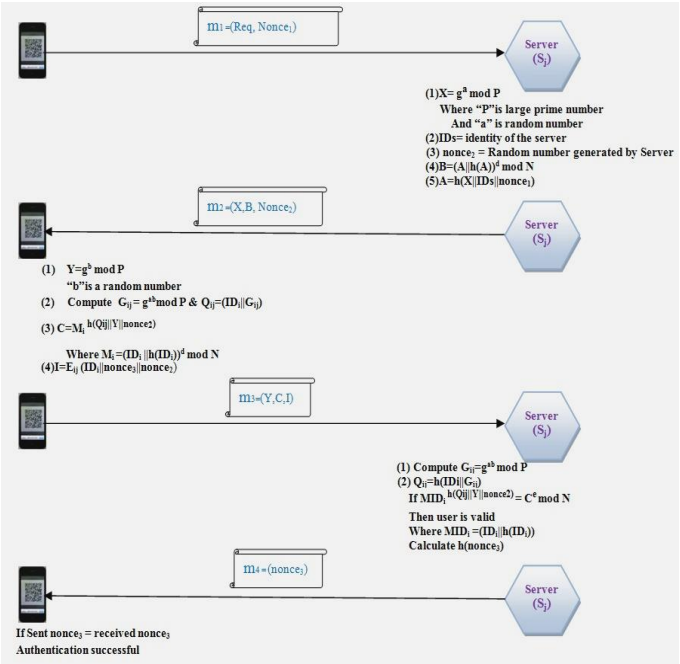


Figure 5 Mutual authentication method for the CRN

Distribution of Nfreemod in submods as described in [17]and if there are k free sub bands the probability

$$Pr(N_{free_{mod}} = k) \simeq \int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \frac{1}{\sqrt{2\pi C_n}} e^{-\left(\frac{(x-\bar{N}_{mod})^2}{2C_n}\right)} dx = Pr_{Normal}(N_{free_{mod}} = k),$$

will be

Table 1 Notations

Notation	Meaning
n	Size of SUB_{mod}
k	0,1,2,3,4,5……n
N_{mod}	$E[N_{freemod}] = \sum i2Sub_{mod}\ pi$
C_n (Vacancies of $N_{freemod}$)	$\sum i2Sub_{mod}\ pi\ (1-pi)$

The estimate of the dispersion of Nfreelarge takes after basically the way set by Nfreesmall . Note that (1 −pi) is little for i 2 Sublarge. Utilizing the Law of Rare Events, the circulation of Nfreelarge can likewise be approximated by a Poisson appropriation. The accompanying lemma encourages reckoning of the likelihood dispersion of Nfreelarge clients
where λl = Σi2Sublarge (1−pi). So the probability of free sub bands is

$$Pr(N_{free_{large}} = k) \simeq \frac{e^{-\lambda_l}\lambda_l^{(N-m-n-k)}}{(N-m-n-k)!} = Pr_{Poi}(N_{free_{large}} = k),$$

where the summation is taken over all k1 ≥0, k2 ≥0, and k3 ≥0 with k1 + k2 + k3 = k

$$Pr(N_{free} = k) = \sum Pr(N_{free_{small}} = k_1, N_{free_{mod}} = k_2, N_{free_{large}} = k_3)$$

4.0 CONCLUSION

In the keep going decade, expanding requests for the remote access to the Internet has brought about congestion of some particular groups of the radio range. Nonetheless, there are a few groups of recurrence that will be appointed to the authorized client and will be underutilized most of the time. Cognitive radio (CR) will be a guaranteeing engineering that can overcome these challenges by giving crafty access to the underutilized range. Regardless of the numerous favorable circumstances brought by CRs to remote systems, this innovation faces new security dangers and challenges in expansion to those that will be as of recently present in the remote systems. In this paper, we have examined the different characteristics of cognitive radios that make them ideal for correspondence in a nature's turf. We additionally investigated the conceivable outcomes of having a protected correspondence by consolidating the characteristics of spread range balance strategies and encryption calculations with the cognitive radio engineering. We have likewise examined the different fields and buyer requisitions where cognitive radio engineering is pertinent

References

[1] R. Pal, *et al*. 2008. Characterizing Reliability In Cognitive Radio Networks. First International Symposium on Applied Sciences on Biomedical and Communication Technologies, 2008. 1-6, 25-28 Oct.

[2] E. Trigui *et al.* 2013. A Mobility Scheme for Cognitive Radio Networks. 12th Annual Mediterranean of Ad Hoc Networking Workshop (MED-HOC-NET), 2013. 102: 24-26 June.

[3] V. Marojevic, *et al.* 2007. Integrated Resource Management in Cognitive Radio. 16th IST on Mobile and Wireless Communications Summit, 2007. 1(5): 1-5 July.

[4] J. Mitola III, 2000. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. Ph.D. Thesis, Swedish Royal Institute of Technology.

[5] S. Ball, A. Ferguson, and T. W. Rondeau. 2005. Consumer Applications of Cognitive Radio Defined Networks. First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySpan'05. 518-525, Nov.

[6] A. Gorcin and H. Arslan. 2008. Public Safety and Emergency Case Communications: Opportunities from the Aspect of Cognitive Radio. 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks. 1-10, Oct.

[7] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney. 2011. Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks. *IEEE Transactions on Signal Processing.* 59: 774-786.

[8] S. Liu, Q. Liu, J. Gao, and J. Guan. 2011. Attacker-exclusion Scheme for Cooperative Spectrum Sensing Against SSDF Attacks Based On Accumulated Suspicious Level. IEEE International Conference on Cyber Technology in Automation. *Control, and Intelligent Systems (CYBER).* 239-243.

[9] A. G. Fragkiadakis, *et al.* 2013. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. *IEEE Communications Surveys & Tutorials*. 15(1): 428-445.

[10] L. Duan, A. W. Min, J. Huang, and K. G. Shin. 2012. Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications*. 30: 1658-1665.

[11] R. E. Ziemer. 2007. Fundamentals of Spread Spectrum Modulation, Colorado Springs: Morgan & Claypool Publishers.

[12] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney. 2010. Countering Byzantine Attacks in Cognitive Radio Networks. *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*. 3098-3101.

[13] S. Haykin, D. J. Thomson, and J. H. Reed. 2009. Spectrum Sensing for Cognitive Radio. Proceedings of the IEEE. 97: 849-877.

[14] L. Freitas, Y. Pires, J. Morais, J. Costa, and A. Klautau. 2012. Data Mining Applied to Cognitive Radio Systems.

[15] C. N. Mathur and K. Subbalakshmi. 2007. Digital signatures for centralized DSA networks. Proc. First IEEE Workshop on Cognitive Radio Net- works, CCNC), Las Vegas, NE, Jan. 11.

[16] Y.-C. Liang, H.-H. Chen, J. Mitolla III, P. Mahonen, R. Kohno and J. H. Reed. 2008. Cognitive Radio: Theory and Applications. *IEEE Journal on Selected Areas in Communications*. 26(1): Jan.

[17] C. Ghosh. 2009. Innovative Approaches to Spectrum Selection, Sensing, and Sharing in Cognitive Radio Networks, PhD Thesis, University of Cincinnati, May.