Proceedings of the 18th International Conference on Automation & Computing, Loughborough University, Leicestershire, UK, 8 September 2012

A Novel Multi-fold Security Framework for Cognitive Radio Wireless Ad-hoc Networks

Munam Ali Shah, Sijing Zhang, Carsten Maple
Department of Computer Science and Technology
University of Bedfordshire
Park Square, Luton, LU1 3JU, United Kingdom
{munam.shah, sijing.zhang, carsten.maple}@beds.ac.uk

***Abstract*— Cognitive Radio (CR) Technology has emerged as a smart and intelligent technology to address the problem of spectrum scarcity and its under-utilization. CR nodes sense the environment for vacant channels, exchange control information, and agree upon free channels list (FCL) to use for data transmission and conclusion. CR technology is heavily dependent on the control channel to dialogue on the exchanged control information which is usually in the Industrial-Scientific-Medical (ISM) band. As the ISM band is publically available this makes the CR network more prone to security vulnerabilities and flaws. In this paper a novel multi-fold security framework for cognitive radio wireless ad-hoc networks has been proposed. Multiple security levels, such as, encryption of beacon frame and privately exchanging the FCL, and the dynamic and adaptive behaviour of the framework makes the proposed protocol more resilient and secure against the traditional security attacks when compared with existing protocols.**

Keywords-Cognitive Radio; MAC Protocols; Security Framework; Co-operative Communication; Control Channel

I. INTRODUCTION

The modern communications have become more dependent on wireless technology. Wi-Fi, Cellular phones, Bluetooth, TV broadcasts and satellite are proliferation of wireless services. The increased number of wireless applications from home appliances to satellite control has created huge demand for more radio spectrum. For every wireless application, certain portion of the radio spectrum need to be purchased, and the Federal Communication Commission (FCC) allocates the spectrum for fee for such services [1]. This has led to the problems like scarcity of spectrum, shortage of spectrum to use in new wireless services, and lack of radio resource and wireless services to those who are more appropriate and needy. Most of the frequencies in the radio spectrum have been allocated although many studies have shown that the allocated bands are not efficiently being used [2] . Cognitive radio technology [3][4][5] is a solution to the shortage of spectrum and the inefficiency of its utilization. Cognitive radios are intelligent wireless devices that sense the environment, observe the network changes, and then make intelligent decisions, based on knowledge learnt from the previous interaction with the network, to seize the opportunities to transmit. This process of scanning the spectrum (S), exchanging control information (E), agreeing upon white space (A) and transmitting data (T) on the network is repeated continuously in a cycle. Figure 1 shows how a cognitive radio learns from its environment and tunes its transceivers to adapt the network changes. CR network serves as a framework in accessing the spectrum allocation dynamically, and spectrum opportunity [5] deals with the usage of a free channel that is part of radio spectrum and is not currently being used by primary users (PUs). The licensed user or PU of the frequency band is the wireless application who purchases the portion of radio spectrum from FCC for fee, and those who utilizes spectrum opportunistically for communication without interference to the PU is called secondary user (SU). Each cognitive device is equipped with sensors and transceivers that sense the spectrum and allow SUs to access licensed spectrum bands as long as SUs do not impose any interference to PUs.

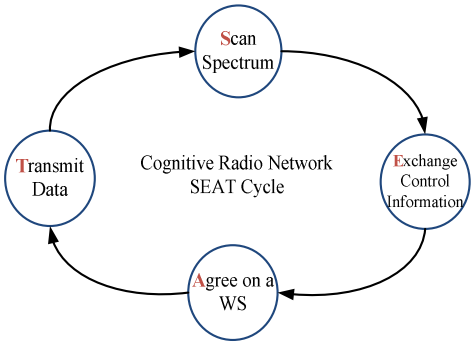

Figure 1. SEAT Cycle for Cognitive Radio Networks

PUs when not transmitting create free channels or empty spaces in the spectrum, and these empty spaces, also called white spaces, are used by SUs opportunistically. The existence of Common Control Channel (CCC) is mandatory for all CR nodes for control information exchange. Before any cognitive devices start sending and receiving data, they first have to coordinate and decide about the transmission on the CCC. The pair of SUs exchange initial information such as how to send requests, which white spaces to be used and how long the communication will last. This information could also include the exchange of Request-To-Send (RTS) and Clear-To-Send (CTS) control frames in order to solve hidden terminal problem and avoid collisions in random access protocols which are mostly used by cognitive radio devices for exchange of control information. Figure 2 shows the process of formation of white spaces in the spectrum. The CCC could be static or dynamic. Under the static case, the control channel can be either specially licensed to the secondary users by FCC or use an unlicensed spectrum band (e.g., 2.4GHz). In the latter case

it is commonly called GCCC. In the dynamic case, the control channel could be one of the most reliable and available white spaces.

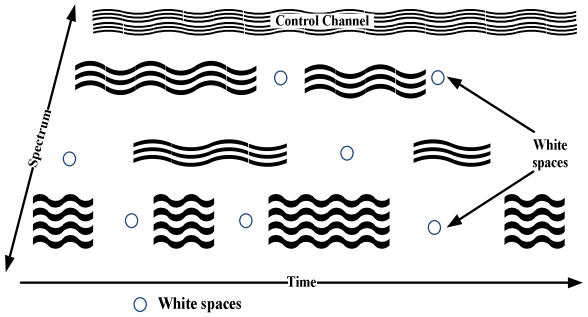

Figure 2. Spectrum usage by PUs and formation of white spaces

II. REVIEW OF THE PREVIOUS WORK

The cognitive radio technology that consists of nodes, architecture and control strategies, has appeared to be an efficient solution for heterogeneous networks. However, this leads to security issues because same security standards could not be applied in all heterogeneous networks. The CR technology merges core network with access networks in the heterogeneous environment. Wireless standards have different security strategies. For example in WLAN and personal area network (PAN) the only mechanism to incorporate security is identity authentication. In GSM [6], WiMAX [7], WCDMA [8] and WCDMA2000 [9], the legality of terminals and user is controlled by strict authentication process from base station and SIM card authentication. The differences between technologies used for cognitive radio and for existing wireless networks make the security incorporation a veiled question. The adaptive nature of cognitive radio technology imposes additional complications and introduces new challenges. For example an attacker may pretend to be a secondary user and without authentication can intercept the FCL by a false claim of being an SU, or in another case it can mimic the behavior of licensed user and can increase the probability of false alarm detection. This is a special type of denial-of-service (DoS) attack in CR networks and is commonly known as primary user emulation (PUE) attack [10] [11] [12]. Another type of attacks specific to CR networks is the jamming attack [13] that can push the nodes in the vicinity to select a specific spectrum band for control information exchange where another attacker seizes the control information.

Physical layer techniques have been intensively focused in recent studies to detect the anomalous usage of spectrum [11][12][14][15]. The detection of an unauthorized usage of the spectrum in zone-based networks has been investigated in [14]. Authorized users do not impose interference to each other because at most one authorized user, i.e., either none or one authorized user, can exist in each network zone. Received signal powers of unknown signals are measured to detect unauthorized spectrum usage. Chen *et al* [11] have proposed a mechanism to verify transmitter which assumes that the Primary Signal Transmitter (PST) location is known in advance and that PUE attacker cannot duplicate the energy of the legitimate signal. If the suspicious signal is being transmitted outside the range of PST, it is considered as a PUE attack. If the transmission of the suspicious signal is received in the PST vicinity, energy detection is used to authenticate the signal. A protocol for mitigating PUE attacks has been proposed in [16] in which each SU uses a centralized spectrum decision to decrease the probability of false alarm. Goergen *et al* [17] present a method in which a watermark is added to the PU signal. CR nodes retrieve the watermark to authenticate the transmitted signal. These tasks make use of the physical layer information only, and either PU signals are modified or prior information about the PU is required to detect PUE and jamming attacks. Jamming attacks have also been studied in different recent studies [18][19][15]. A primary number sequence code has been used by the scheme proposed in [15], in which jammer could not compute which channel to jam in given time. A game theoretic approach is presented in [19] to model the jamming and its contravention in cognitive radio multichannel networks. One-stage game and multi-stage game are obtained by Nash equilibrium and stochastic control strategy respectively. Xu *et al* [20] discuss the signal measurement for jammer detection and argue that smart jamming attack is a new trend in CR networks and new artifacts need to be developed to efficiently address these issues.

To summarize, the work published so far mostly emphasizes on the physical layer to address the security vulnerabilities in cognitive radio networks. It is believed that, apart from the security measurements at the physical layer, mechanisms must be derived to incorporate security at MAC layer in CR networks. This motivates us to design a novel security model for cognitive radio wireless ad-hoc networks, which provides multiple levels of security at MAC layer. The next section discusses the framework of the proposed security model for CR networks.

III. A NOVEL MULTI-FOLD SECURITY FRAMEWORK FOR COGNITIVE RADIO NETWORKS

Cognitive radio networks are opportunistic networks, and CR nodes are always haunting to seize the opportunity to transmit. It is very important that CR nodes efficiently and securely exchange data with each other before the PU interference is sensed. The opportunistic nature of the CR network under the effect of traditional security flaws could not let the CR nodes afford the cost of retransmission.

We have proposed a novel secure adaptive MAC protocol for cognitive radio networks. To the best of authors' knowledge, the proposed protocol named DDH-MAC (dynamic decentralized and hybrid MAC) is the first hybrid CR MAC protocol lying between GCCC and non-GCCC family of CR protocols. DDH-MAC not only overcomes drawbacks of GCCC but also benefits from the 24x7 free of cost availability of GCCC. The dynamic, adaptive and hybrid behavior of the proposed MAC protocol makes a partial use of GCCC to advertise the information about control channel establishment within the white spaces amongst cognitive nodes. It efficiently sets one of the white spaces as the primary control channel (PCCH) to exchange control information with other

cognitive nodes and sets another as the backup control channel (BCCH) in case there is a PU claim on PCCH. DDH-MAC has a novel design of the MAC protocol for CRNs which not only benefits from the anytime license-free availability of GCCC but also enjoys the secure communication by privately exchanging the FCL over one of the white spaces. The best features of decentralized family of MAC protocols have been combined to make the proposed hybrid protocol efficient, dynamic, and decentralized. A detailed operation of the protocol including 2 levels of selection has already been presented in our previous work [21]. The protocol takes into account different case scenarios in the cognitive radio environment and tunes its parameters efficiently and intelligently according to the current situation of the network, which makes the protocol adaptive, secure and energy efficient. We have defined these case scenarios in the following section and will represent all the states with a 2^n binary function where n = 2. All the possible states of DDH-MAC are 00, 01, 10 and 11 as specified below:

Network initialization and launch of beacon frame (BF)	00
Reading BF and contending for exchange of FCL	01
Concluding transmission on agreed WS and scanning PCCH	10
Concluding transmission on agreed WS and scanning BCCH	11

Upon initialization, cognitive nodes implementing the proposed MAC scan the GCCC for BF. If the node does not find any BF then one node is responsible for launching BF in the GCCC which let other CR nodes in the vicinity know about one of the white spaces to be used as the primary control channel and about another as backup control channel.

Initialization Phase:

```
01.     Search the GCCC for a BF
02.     if      BF found
03.             Read the BF
04.             Switch to the PCCH
05.             Sense the PCCH for control information
06.     else    Select channels to serve as PCCH & BCCH
07.             Launch BF
08.             Go to Step 03
```

Negotiating Phase:

```
09.     After Step 03, sense control information
10.     Contend for the newly found control channel
        (PCCH/BCCH)
11.     Exchange free channel list (FCL)
12.     Agree on a white space
13      Conclude transmission
14.     Go to Step 05
```

Actions after the PU Interference:

```
15.     Upon finding information about PCCH and BCCH
16.     Go to Step 04
17.     if      Any PU activity sensed on PCCH
18.             Switch to the BCCH
19.             Repeat Steps 10-13
20.         if  Any PU activity sensed on the BCCH
21.             Go to Step 01
22          else Go to Step 10
23.     else    Go to Step 10
```

Figure 3. The DDH-MAC Algorithm

It is important to note that BCCH is a reserved control channel and is used only when there is a PU re-claim on PCCH. If the node finds the BF, it reads the information about PCCH and BCCH, updates its FCL and switches to PCCH for the subsequent control information exchange, otherwise it considers itself as the starting node and launches the BF in GCCC. During the initial scanning, if the BF is successfully found by a CR node in GCCC, it learns about the chosen PCCH and BCCH. The communicating CR nodes always verify the re-claim of PCCH by PU before they actually switch to it for further exchange of FCL. After the successful exchange of FCL on the chosen PCCH, the CR nodes eventually switch to agreed empty spaces to be used as data channels for the actual data transmission. The CR nodes may come up with a case when there is a re-claim by PUs on both PCCH and BCCH; and in this case the nodes go to the initial state (00) where they scan the GCCC for any new BF. The algorithm for proposed scheme is provided in Figure 3. The protocol is dynamic because every time there is a PU claim, nodes switch to a newly found and agreed-upon control channel. Moreover, the CR nodes are always certain that they have access to at least one control channel.

As shown in Figure 4 the proposed protocol provides multiple levels of security. Each level provides an unique feature of security which altogether makes the proposed protocol secure and energy efficient.

Level 1: Encryption of BF

The first node in the CR network makes partial use of GCCC by launching an encrypted beacon frame. The recipients of the BF apply the relevant decryption scheme [22][23] to read the information about the PCCH and BCCH.

Level 2: Secure FCL Transaction

Most of the CR protocols [24][25][26][27][28] exchange the FCL through the GCCC which is publically available to everyone and is more prone to security vulnerabilities and threats. DDH-MAC uses one of the white spaces as PCCH and exchanges the FCL secretly on the chosen control channel which is only known to the CR nodes in the vicinity. Furthermore, prior to the FCL transaction, all frames are encrypted using the public key cryptography and only those nodes which have the knowledge of the private key can retrieve the information in cryptographic frames.

Level 3: Inclusion of Time Stamp in Data Transmission

Man-in-the-middle attack is not unusual in the cognitive radio environment and any type of the information could be retrieved by the intruders. DDH-MAC smartly and efficiently addresses the criticality of the situation by adding a time stamp in each data transmission. Data is expected to reach the destination in a specified time which confirms the secure transmission. If the data does not reach the intended recipient in specified time with a reasonable amount of delay (considering the propagation delay), this means that the integrity of the data could have been compromised and therefore data is no longer trustworthy.

Level 4: Dynamicity of the Control Channel

Since DDH-MAC uses one of the white spaces as the PCCH and another as the BCCH, the PU claim on these local control channels could happen at any time. If the PCCH has been reclaimed by the PU, CR nodes implementing DDH-MAC will switch to the BCCH to continue exchanging control information. If, in the worst case, BCCH has also been reclaimed by the PU then nodes will switch to the GCCC to search for any BF. The PU claim on PCCH and BCCH is beneficial to DDH-MAC and actually provides another level of security to CR nodes. An attacker targeting PCCH/BCCH through smart jamming and PUE attacks will have to re-compile the attack strategy from time to time. The dynamicity of control channels (PCCH/BCCH) offers CR nodes a high level of security.

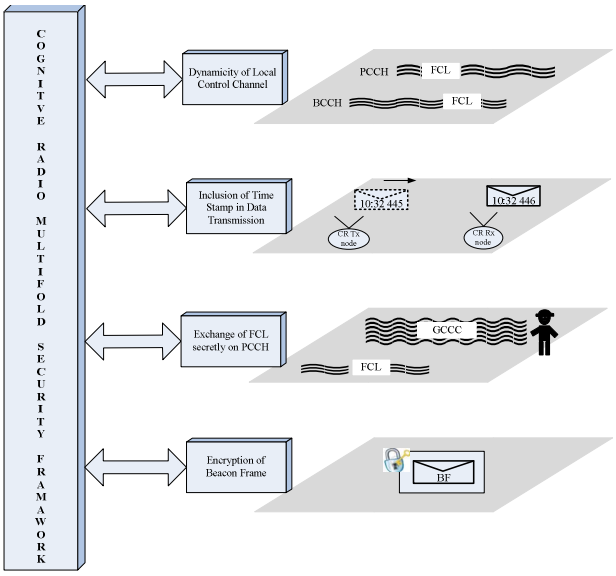

Figure 4. The DDH-MAC multi-fold security framework for CR networks

IV. PERFORMANCE EVALUATION

To analyze the performance of DDH-MAC protocol, pre-transmission time has been computed. Pre-transmission time is defined as 'the time required in exchanging control information on CCC before the actual data transmission starts'. Pre-transmission is calculated by the number and the size of control frames exchanged over the control channel and is heavily affected by the responses to PU claims. For example quite a few previously proposed CR MAC protocols [26][27][28] have no mechanisms to resume data transmission whenever there is a PU interference, and these protocols have to re-negotiate the entire configuration dialogue over the control channel. Since DDH-MAC has got a backup control channel and the PU interference is smartly addressed by performing a switch operation which not only provides time and energy efficiency but also enables CR nodes holding delay sensitive data to have to wait less time before they actually to send data. Figure 5 shows the case scenario in DDH-MAC where CR nodes exchange control information over the control channel and PU interference is sensed.

The Pre-Transmission Time

In this section pre-transmission time has been computed for different CR MAC protocols including DDH-MAC. After successful exchange of FCL on the chosen PCCH, the CR nodes eventually switch to an agreed empty space to be used as data channel for the actual data transmission. The protocol performs a few operations before the network is fully converged. These operations include scanning GCCC, launching BF, deciding which white spaces to use as PCCH and BCCH, and how long to take to exchange control information. Not all the operations are performed by CR nodes, and the number of operations performed depends on the role of the CR node and on the case scenario. For example if a node has already found BF, it will not perform the beacon launching operation and thus the time T_{BS} will be

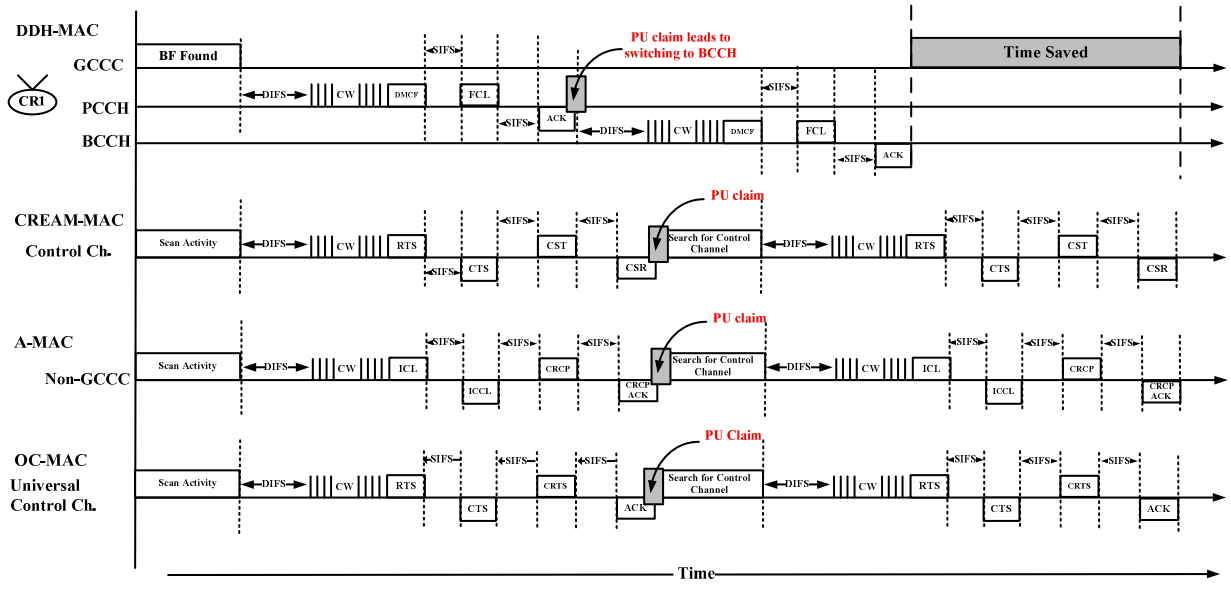

Figure 5. Timing Diagram for the proposed protocol, in comparison with CREAM-MAC, A-MAC and OC-MAC

omitted. T_{BS} is defined as the time required to search the BF in GCCC, T_{BF} is the time required to launch BF in GCCC, T^{PCCH} and T^{BCCH} denote the estimated contention time to access PCCH and BCCH, and T_{DMCF} and T_{FCL} are time required to exchange the DDH-MAC control information. The time it takes to do any or all of these operations form part of the pre-transmission time and can be expressed in (1).

$$T_{PT} = \{ T_{BS}, T_{BF}, T^{PCCH}, T^{BCCH}, T_{DMCF}, T_{FCL}\} \quad (1)$$

where DMCF, FCL and ACK are control frames being exchanged in DDH-MAC with the sizes of 20 bytes, 20 bytes and 14 bytes respectively. This control information is exchanged in GCCC which is publically available to every application. The free availability of GCCC makes it heavily insecure, and it is believed that the less time spent in GCCC, the less would be CR nodes exposed and less prone to security vulnerabilities. Thus the higher secuirty could be achieved.

The pre-transmission time for the scenario, when the PU interference is detected, is computed using IEEE 802.11b as benchmark. The normal response by CR nodes is to abort the transmission and re-exchange the control information to agree upon another white space to conclude transmission while the proposed protocol efficiently deals with the situation by switching to the BCCH. Less number of frames exchanged with other CR nodes results in faster network convergence, and nodes remain in the state where at least one control channel remains always available with all CR nodes. Figure 6 shows the comparison of our protocol with several other CR MAC protocols [28][25][27] in terms of pre-transmission time.

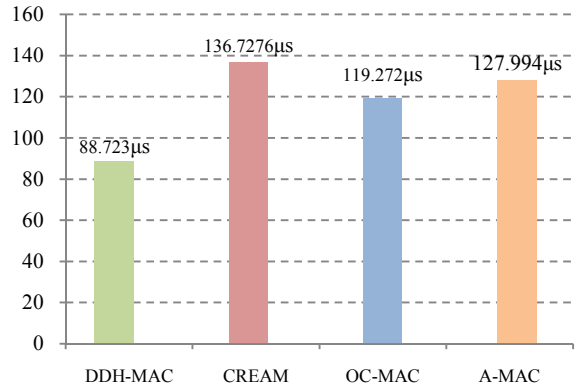

Figure 6. Effect of pre-transmission time on security vulnerability

CONCLUSION

Cognitive radio networks aim to be a promising technology to resolve the problem of spectrum scarcity. CR nodes must exchange the control information on CCC prior to any data transmission. The selection criteria of CCC make the CR technology exposed to security risks. In addition to traditional security vulnerabilities, CR nodes are more prone to new security challenges. In this paper a novel multi-fold security framework for CR networks has been presented. Incorporation of security at different levels in the proposed protocol makes it more resilient against security attacks. Especially the selection of control channel in white spaces gives the protocol extra security where the FCL is privately and secretly exchanged with other CR nodes. The less CR nodes stay in CCC, the more secure transactions could take place. Analytical results show that CR nodes implementing the proposed protocol have to access the GCCC only for BF transmission which is just a 20-byte frame. The GCCC access time for DDH-MAC is only 14.54µs, while the GCCC access time for any of other protocols is 4 times higher. Currently the proposed protocol is being simulated for analysis of the effect of PUE and jamming attacks on throughput. In future, the incorporation of cryptographic algorithms such as RSA and DSA for BF and FCL encryption will be investigated.

REFERENCES

[1] "The Radio Spectrum," *Available Online: http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp38 chart.pdf.*

[2] P. Kolodzy, "Spectrum policy task force," *Fed. Commun. Comm., Washington, DC, Tech. Rep. ET Docket*, no. 02–135, 2002.

[3] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13-18, 1999.

[4] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[5] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, 2006.

[6] M. A. Ozkan, B. Ors, and G. Saldamli, *Secure voice communication via GSM network*. IEEE, 2011, p.288-292.

[7] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions," *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, vol. 7, no. 11, pp. 828-833, 2008.

[8] Y. X. J. H. L. W. L. Khit Y K, "Synchronization of WCDMA TDD node B using better security sequences," in *2005 Fifth International Conference on Information Communications and Signal Processing*, 2005, vol. 2005, pp. 989-993.

[9] J. Y. Choung, T. Hameed, and I. Ji, "Catch-up in ICT standards: Policy, implementation and standards-setting in South Korea," *Technological Forecasting and Social Change*, vol. 79, no. 4, pp. 771-788, 2012.

[10] A. Sethi and T. X. Brown, "Hammer model threat assessment of cognitive radio denial of service attacks," *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 1-12, 2008.

[11] R. C. R. Chen, J.-M. P. J.-M. Park, and J. H. Reed, Defense against Primary User Emulation Attacks in Cognitive Radio Networks, vol. 26, no. 1. 2008, p. 25-37.

[12] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 1-6, 2008.

[13] J. L. Burbank, A. R. Hammons, and S. D. Jones, "A common lexicon and design issues surrounding cognitive radio networks operating in the presence of jamming," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1-7, 2008.

[14] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks," *IEEE INFOCOM 2009 The 28th Conference on Computer Communications*, pp. 675-683, 2009.

15] L. Ma and C. C. Shen, "Security-enhanced virtual channel rendezvous algorithm for dynamic spectrum access wireless

networks," in *Third IEEE International Symposium on Dynamic Spectrum Access Networks 2008 DySPAN 2008*, 2008.

[16] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks," *Communications Society*, pp. 6-10, 2010.

[17] N. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channel emulation," *2010 IEEE Symposium on New Frontiers in Dynamic Spectrum DySPAN*, pp. 1-7, 2010.

[18] H. Li and Z. Han, "Dogfight in spectrum: jamming and anti-jamming in multichannel cognitive radio systems," *IEEE Global Telecommunications Conference*, pp. 1-6, 2009.

[19] H. L. H. Li and Z. H. Z. Han, "Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics, vol. 9, no. 11, pp. 3566-3577, 2010.

[20] W. Xu, W. Trappe and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc ACM Mobihoc*, 2005, pp. 46-57.

[21] M. A. Shah, G. A. Safdar, and C. Maple, "DDH-MAC: A novel Dynamic De-Centralized Hybrid MAC protocol for Cognitive Radio Networks," IEEE *2011 RoEduNet International Conference 10th Edition: Networking in Education and Research*, pp. 1-6, 2011.

[22] E. Yoon and K. Yong, "An Efficient Diffie-Hellman-MAC Key Exchange Scheme," *Advances*, pp. 9-11, 2009.

[23] Z. Min and H. Ting-lei, "A RSA keys sharing scheme based on dynamic threshold secret sharing algorithm for WMNs," in *Intelligent Computing and Integrated Systems ICISS 2010 International Conference*, 2010, pp. 160-163.

[24] C. Cordeiro and K. Challapali, "C-MAC: A cognitive MAC protocol for multi-channel wireless networks," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007, pp. 147-157.

[25] S.-Y. Hung, Y.-C. Cheng, E. H.-K. Wu, and G.-H. Chen, "An opportunistic cognitive MAC protocol for coexistence with WLAN," in *2008 IEEE International Conference on Communications*, 2008, pp. 4059-4063.

[26] A. C.-C. Hsu, D. S. L. Wei, and C.-C. J. Kuo, "A cognitive MAC protocol using statistical channel allocation for wireless ad-hoc networks," in *2007 IEEE Wireless Communications and Networking Conference*, 2007, pp. 105-110.

[27] G. P. Joshi, S. W. Kim, and B. S. Kim, "An efficient MAC protocol for improving the network throughput for cognitive radio networks," in *2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies*, 2009, pp. 271-275.

[28] X. Zhang and H. Su, "CREAM-MAC: Cognitive Radio-EnAbled Multi-Channel MAC Protocol Over Dynamic Spectrum Access Networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 110-123, Feb. 2011.