



# Secure MAC Protocols for Cognitive Radio Networks

Wajdi Alhakami

This is a digitised version of a dissertation submitted to the University of Bedfordshire.

It is available to view only.

This item is subject to copyright.

# **Secure MAC Protocols for Cognitive Radio Networks**

By  
Wajdi Alhakami

A thesis submitted in partial fulfilment for the degree of  
*Doctor of Philosophy*

From the



Department of Computer Science and Technology  
University of Bedfordshire

January 2016



# Acknowledgement

I am sincerely thankful and appreciative to my Director of Studies Dr Ali Mansour, for his vital guidance, invaluable assistance and constant support during my PhD study.

I also would like to thank my second supervisor, Dr Ghazanfar Safdar, for his personal attention and full support and suggestions, during my PhD research.

I also extend my truthful thanks and appreciation to my friends, Ahmed Alenesi, Bandar Almiman and Dr Faisal Qureshi, and colleagues at the Institute for Research in Applicable Computing at the University of Bedfordshire for their advice and encouragements and best wishes throughout my study period.

Special thanks to my mother, wife and family members for their love, support and patient during my study, also to my daughters; Rose and Ronza. I also extend my gratitude to my relatives for their encouragement and motivations.

## Publications

- **Alhakami, Wajdi;** Mansour, Ali and Safdar, Ghazanfar A. (2014) "Spectrum Sharing Security and Attacks in CRNs: a Review", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.
- **Alhakami, Wajdi;** Mansour, Ali; Safdar Ghazanfar. (2014). "Shared-key Based Secure MAC Protocol for Cognitive Radio Networks" NGMAST2014 International Conference on Next Generation Mobile Applications, Oxford, United Kingdom, 10th -12th September 2014.
- **Alhakami, Wajdi;** Mansour, Ali; Safdar, Ghazanfar A; Albermany, Salah, (2013) "A secure MAC protocol for Cognitive Radio Networks (SMCRN)," Science and Information Conference (SAI), 2013, pp.796,803, 7-9 Oct. 2013
- **Alhakami, Wajdi. Haisoun;** Mansour, Ali; Zhang, Sijing, (2012)" ESMCRN: An Enhanced Security Mechanism for Cognitive Radio Networks", Proceedings of the 7th IB2COM, November 5-8, 2012, Sydney, Australia.
- **Alhakami, Wajdi.** Mansour Ali; Safdar Ghazanfar. (2014). "Abstract No. 483: A Secure MAC Protocol for Cognitive Radio Networks", 7th Saudi Students Conference in the UK – 2014

### *Papers under review:*

- **Alhakami, Wajdi;** Mansour, Ali; Safdar, Ghazanfar A. (2016) "Performance Analysis of a Novel Decentralised MAC Protocol for Cognitive Radio Networks ", APWiMob 2016 conference. Submitted on 15 June 2016.
- **Alhakami, Wajdi;** Mansour, Ali; Safdar, Ghazanfar A. (2016) "Digital-Signature and Shared-Key Based Secure MAC Protocols for CRNs", Computer Networks - The International Journal of Computer and Telecommunications Networking, Elsevier, under process.

## Abstract

With the rapid increase in wireless devices, an effective improvement in the demand of efficient spectrum utilisation for gaining better connectivity is needed. Cognitive Radio (CR) is an emerging technology that exploits the inefficient utilisation of the unused spectrum dynamically. Since spectrum sharing is responsible for coordinating channels' access for Cognitive Users (CUs), the Common Control Channel (CCC) is one of the existing methods used to exchange the control information between CUs. However, the unique characteristics and parameters of Cognitive Radio Networks (CRNs) present several possible threats targeting spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility leading to the deterioration of the network performance. Thus, protection and detection security mechanisms are essential to maintaining the CRNs. This thesis presents a novel decentralised CR MAC protocol that successfully utilises the unused portion of the licensed band. The protocol achieves improved performance; *communication time* and *throughput* when compared to two benchmark protocols. Less communication time and higher throughput are accomplished by the protocol due to performing fast switching to the selected available data channel for initiating data transmission. The proposed protocol is then extended to two different versions based on two authentication approaches applied to it; one using *Digital Signature* and another is based on *Shared-Key*. The two proposed secure protocols address the security requirements in CRNs leading to subsequent secure communication among CUs. The protocols function effectively in providing defence against several attacks related to the MAC layer such as; Spectrum Sensing Data Manipulation/Falsification, Data Tempering and Modification, Jamming attacks, Eavesdropping, Forgery and Fake control information attacks, MAC address spoofing, and unauthorised access attacks. The associated security algorithms ensure the successful secure communication between CUs in a cooperative approach. Moreover, the security protocols are investigated and analysed in terms of security flows by launching unauthorised access and modification attacks on the transmitted information. The testing results demonstrated that two protocols perform successful detection of threats and ensure secure communication in CRNs.

# Table of Contents

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
1.1. Cognitive Radio.....	1
1.2. Cognitive Radio core functions.....	2
1.3. Spectrum sharing classifications .....	4
1.3.1. Network architecture .....	5
1.3.2. Allocation behaviour .....	5
1.3.3. Access technology .....	6
1.4. Research Background.....	6
1.4.1. Security requirements in CRNs .....	8
1.4.1.1. Access control .....	8
1.4.1.2. Confidentiality .....	8
1.4.1.3. Authentication.....	8
1.4.1.4. Availability .....	9
1.4.1.5. Authorisation.....	10
1.4.1.6. Integrity.....	10
1.4.1.7. Non-repudiation .....	11
1.4.2. Cryptographic schemes .....	11
1.5. Motivation .....	12
1.6. Problem statement .....	13
1.7. Research aim and objectives .....	16
1.8. Research Contributions .....	16
1.9. Research methods.....	17
1.10. Scope and limitations of the research work .....	18
1.11. Thesis organization .....	19
<b>CHAPTER 2 LITERATURE REVIEW .....</b>	<b>21</b>
2.1. Common features of CR MAC protocols.....	23
2.1.1. Control channel .....	23
2.1.1.1. Non-dedicated CCC .....	24
2.1.1.2. Dedicated Common Control Channel .....	25
2.1.2. Spectrum Access Techniques .....	29
2.1.3. Sensing channels .....	30
2.1.4. Licensed channel selection .....	31
2.1.5. Number of associated transceivers .....	32
2.2. Security Threats.....	35
2.2.1. Common security threats in conventional wireless and CR Networks.....	37
2.2.1.1. Fake Authentication Attacks .....	37
2.2.1.2. Information Tampering .....	38
2.2.1.3. Service Repudiation .....	38
2.2.1.4. Replay Attack.....	38
2.2.1.5. Denial of Service and Information Interference.....	39
2.2.1.6. Malicious and Selfish behaviour attacks.....	39
2.2.1.7. Black and Grey Hole Attacks.....	40
2.2.2. Specific security threats in CRNs.....	40
2.2.2.1. Security in spectrum sensing .....	41

2.2.2.2. Security in spectrum management .....	43
2.2.2.3. Security in spectrum mobility .....	44
2.2.2.4. Security in spectrum sharing .....	44
2.3. Secure Communication Scheme in CRNs .....	47
2.3.1. Protection mechanisms in CRNs .....	48
2.3.1.1. Digital signature and certificate authority .....	49
2.3.1.2. EAP-SIM .....	49
2.3.1.3. Trust values procedures .....	49
2.3.1.4. Other framework architectures .....	49
2.3.2. Detection schemes in CRNs .....	53
2.3.2.1. Selfish behaviours .....	53
2.3.2.2. Timing parameter .....	54
2.3.2.3. Anomalous Spectrum Usage Attacks (ASUAs) .....	54
2.3.3. Comparisons of the presented schemes against MAC layer's attacks .....	55
2.4. Summary .....	56

### **CHAPTER 3 DESIGN OF THE PROPOSED MAC PROTOCOLS WITH AND WITHOUT SECURITY .....58**

3.1. Assumptions .....	58
3.2. A MAC protocol for CRNs (MCRN).....	59
3.2.1. Dedicated CCC for MCRN .....	60
3.2.2. MCRN features .....	61
3.2.2.1. Multiple transceivers in MCRN .....	62
3.2.2.2. Sensing channels and licensed channel selection in MCRN .....	63
3.2.3. MCRN architecture .....	63
3.2.4. Header fields in MCRN frames .....	66
3.2.5. MCRN Phases .....	67
3.2.5.1. Control Phase.....	68
3.2.5.2. Data transmission Phase .....	69
3.2.6. Medium Access Control (MAC) for MCRN.....	70
3.2.6.1. MAC access modes and timing .....	71
3.2.6.2. NAV period .....	72
3.3. Secure MAC Protocols for Cognitive Radio Networks (SMCRN)....	73
3.3.1. Symmetric and Asymmetric keys cryptography in SSMCRN and DSMCRN .....	73
3.3.1.1. Associated cryptographic keys in SSMCRN.....	74
3.3.1.2. Associated cryptographic keys in DSMCRN .....	76
3.3.2. Secure keys exchanges in DSMCRN and SSMCRN .....	77
3.3.3. DSMCRN and SSMCRN architecture .....	78
3.3.4. Digital-Signature based secure MAC protocol for Cognitive Radio Networks (DSMCRN) .....	82
3.3.4.1. Registration phase of DSMCRN .....	83
3.3.4.2. Authentication and control phase of DSMCRN .....	88
3.3.4.3. Data transmission phase of DSMCRN .....	98
3.3.5. Shared-key based Secure MAC protocol for CRNs (SSMCRN) .	101
3.3.5.1. Registration phase of SSMCRN .....	102
3.3.5.2. Authentication and control phase of SSMCRN.....	105

3.3.5.3. Data transmission phase of SSMCRN.....	106
3.3.6. Analysis of the DSMCRN and SSMCRN protocols using BAN logic .....	108
3.3.6.1. What is the BAN logic?.....	108
3.3.6.2. BAN logic messages meaning rules .....	109
3.3.6.3. Established initial assumptions for the proposed DSMCRN and SSMCRN.....	110
3.3.6.4. DSMCRN and SSMCRN protocols phases' analysis.....	110
3.3.6.5. Security Analysis.....	115
3.3.6.6. Vulnerability Analysis.....	116
3.4. Summary .....	118
<b>CHAPTER 4 APPLYING SECURITY MECHANISMS.....</b>	<b>121</b>
4.1. Applying digital signature.....	121
4.2. Applying Message Authentication Code (MAC).....	125
4.2.1. MAC-Key Generation and verification in the Registration Phase of DSMCRN and SSMCRN .....	127
4.2.2. MAC-key Generation and verification in Control Phase of DSMCRN and SSMCRN .....	128
4.2.3. MAC Key Generation and verification in the Data Transmission Phase of DSMCRN and SSMCRN.....	130
4.3. Encryption and Decryption cryptography schemes .....	131
4.3.1. Advanced Encryption Standard – AES implication .....	131
4.3.1.1. AES algorithm in the registration Phase of DSMCRN and SSMCRN.....	131
4.3.1.2. AES algorithm in the control phase of DSMCRN and SSMCRN .....	132
4.3.1.3. AES algorithm in the data transmission phase of DSMCRN and SSMCRN .....	134
4.3.2. RSA implication in DSMCRN and SSMCRN .....	134
4.3.2.1. RSA algorithm in the registration phase of DSMCRN and SSMCRN.....	135
4.3.2.2. RSA algorithm in the control phase of DSMCRN.....	136
4.4. Summary .....	136
<b>CHAPTER 5 MEDIUM ACCESS CONTROL (MAC) FOR DSMCRN AND SSMCRN .....</b>	<b>137</b>
5.1. The common features of DSMCRN and SSMCRN.....	137
5.2. MAC access model and timing in DSMCRN and SSMCRN .....	137
5.2.1. MAC for the registration phase in DSMCRN and SSMCRN .....	138
5.2.2. MAC for control phase and data transmission .....	139
5.3. Simulation and Performance evaluation of SSMCRN and DSMCRN .....	140
5.3.1. The network parameters .....	141
5.3.2. Communication time of DSMCRN and SSMCRN .....	143
5.3.3. DSMCRN and SSMCRN throughput analysis.....	147
5.4. Impact of malicious users on DSMCRN and SSMCRN.....	151

5.4.2. Impact of modification attacks on the time taken to perform DSMCRN and SSMCRN .....	152
5.4.2.1. Modification attack in DSMCRN .....	152
5.4.2.2. Modification attack in SSMCRN .....	153
5.4.3. Impact of modification attacks on the throughput of DSMCRN and SSMCRN .....	155
5.4.3.1. Throughput in DSMCRN with modification attacks.....	155
5.4.3.2. Throughput in SSMCRN with modification attack.....	156
5.4.4. Impact of unauthorised access on the time performance of DSMCRN .....	157
5.4.4.1. Communication time in DSMCRN with unauthorised access	158
5.4.4.2. Throughput in DSMCRN with unauthorised access .....	160
5.5. Discussion of DSMCRN and SSMCRN .....	162
5.6. Summary .....	166
<b>CHAPTER 6 COMPARATIVE ANALYSIS OF THE PROPOSED AND BENCHMARK PROTOCOLS .....</b>	<b>169</b>
6.1. Simulation and performance evaluation of the MCRN.....	169
6.1.1. Channel sensing results .....	170
6.1.2. Control channel activities .....	173
6.1.3. Probability of successful access of common control channel .....	173
6.1.4. Communication time over control and data channels .....	174
6.1.5. Throughput analysis of the MCRN .....	180
6.2. Benchmarks CREAM and RACRN protocols .....	182
6.3. Handshaking frames over the control channel and data channels in MCRN, CREAM and RACRN .....	183
6.4. Comparative analysis of the proposed and benchmarks protocols without security .....	184
6.4.1. Time performance analysis of MCRN, CREAM and RACRN....	184
6.4.2. Throughput performance analysis of MCRN, CREAM and RACRN .....	186
6.5. Comparative analysis of the proposed and benchmark protocols with security .....	188
6.5.1. Time performance analysis of DSMCRN, DSCREAM and DSRACRN .....	189
6.5.2. Throughput performance analysis of DSMCRN, DSCREAM and DSRACRN .....	190
6.5.3. Time performance analysis of SSMCRN, SSCREAM and SSRACRN.....	192
6.5.4. Throughput performance analysis of SSMCRN, SSCREAM and SSRACRN .....	194
6.6. Summary .....	196
<b>CHAPTER 7 CONCLUSIONS .....</b>	<b>199</b>
7.1. Summary of the current research .....	199
7.2. Contributions Revisited.....	201
7.2.1. The proposed MCRN network protocol .....	201
7.2.2. Security protocols .....	201

7.3. Future work .....	204
7.3.1. Incorporating a backup data channel to improve network performance .....	204
7.3.2. Detection of selfish activities .....	205
7.3.3. Detection of Licensed/Primary User Emulation (PUE) Attacks ..	205
7.3.4. Threshold cryptography against DoS Attack .....	206
<b>CHAPTER 8 REFERENCES .....</b>	<b>208</b>

# List of Figures

Figure 1-1: Cognitive Radio Main Functions .....	3
Figure 1-2: Spectrum sharing Classifications .....	4
Figure 1-3: CRNs Architecture .....	6
Figure 2-1: Spectrum sharing classification in Ad hoc CRNs and the current research direction.....	22
Figure 2-2: Challenges & Security in CRNs.....	36
Figure 2-3: Common Security threats in conventional wireless and CRNs .....	37
Figure 2-4: CRNs specific security threats .....	41
Figure 2-5: Malicious activities in decentralised CRNs .....	46
Figure 3-1: MCRN network scenario .....	65
Figure 3-2: Frame structure.....	66
Figure 3-3: Control and data frames sequences in MCRN .....	68
Figure 3-4: RTS frame format.....	69
Figure 3-5: CTS frame format.....	69
Figure 3-6: Data frame format .....	70
Figure 3-7: ACK frame format .....	70
Figure 3-8: Timing and process of Medium Access Control (MAC) in MCRN ..	71
Figure 3-9: Secure keys exchanges in DSMCRN and SSMCRN.....	78
Figure 3-10: DSMCRN and SSMCRN Network scenario.....	80
Figure 3-11: DSMCRN and SSMCRN architecture .....	81
Figure 3-12: Messages' sequence of the registration phase.....	84
Figure 3-13: RTR frame format .....	84
Figure 3-14: CTR frame format .....	85
Figure 3-15: IOR frame format in DSMCRN .....	86
Figure 3-16: COR frame format.....	86
Figure 3-17: Flow chart of the registration process in DSMCRN .....	87
Figure 3-18: Authentication and control phase framework in DSMCRN and SSMCRN .....	88
Figure 3-19: ITA frame format in DSMCRN .....	89
Figure 3-20: RTA frame format in DSMCRN.....	89
Figure 3-21: Failure of authentication process of the sender .....	91
Figure 3-22: FTA frame format .....	91
Figure 3-23: The authentication process flow chart in DSMCRN.....	92
Figure 3-24: CUA1 frame format .....	93
Figure 3-25: CUA2 frame format .....	93
Figure 3-26: RTS frame format.....	95
Figure 3-27: CTS frame format.....	96
Figure 3-28: Secure control phase transmission in DSMCRN and SSMCRN .....	97
Figure 3-29: Data transmission phase .....	98
Figure 3-30: Data frame format .....	99
Figure 3-31: ACK frame format .....	99
Figure 3-32: RES frame format.....	100
Figure 3-33: Data transmission phase flow chart in DSMCRN and SSMCRN..	100
Figure 3-34: IOR frame format in SSMCRN.....	102
Figure 3-35: COR frame format in SSMCRN .....	103
Figure 3-36: Flow chart of the registration process in SSMCRN.....	104

Figure 3-37: ITA frame format in SSMCRN.....	105
Figure 3-38: RTA frame format in SSMCRN.....	106
Figure 3-39: Authentication process flowchart in SSMCRN .....	107
Figure 3-40: Protocol analysis methods.....	108
Figure 4-1: Verification process of the digital signature .....	124
Figure 4-2: MAC Key generation and verification .....	125
Figure 5-1: The time required for each user to register and join the network ....	138
Figure 5-2: The time required for CUs to exchange their control frames.....	139
Figure 5-3: The communication time for a single pair of CUs in DSMCRN and SSMCRN .....	143
Figure 5-4: The communication time for 10 pairs of CUs in DSMCRN and SSMCRN .....	145
Figure 5-5: Time performance of DSMCRN and SSMCRN with and without LUs' activities.....	147
Figure 5-6: Throughput in DSMCRN and SSMCRN without involving LUs ...	149
Figure 5-7: Throughput in DSMCRN and SSMCRN with LUs activities .....	151
Figure 5-8: Communication time of a single pair of CUs in DSMCRN and DSMCRN with modification attack .....	152
Figure 5-9: Communication time of 20 CUs in DSMCRN and DSMCRN with modification attack .....	153
Figure 5-10: Communication time of a single pair of CUs in SSMCRN and SSMCRN with modification attack.....	154
Figure 5-11: Communication time of a 20 pair of CUs in SSMCRN and SSMCRN with modification attack .....	155
Figure 5-12: Throughput for 20 pair of CUs in DSMCRN and DSMCRN with modification attack.....	156
Figure 5-13: Throughput for 20 pair of CUs in SSMCRN and SSMCRN with modification attack.....	157
Figure 5-14: Communication time for 20 pairs of users, including 1 malicious user in DSMCRN.....	159
Figure 5-15: Communication time for 20 pair of users include 4 malicious users in DSMCRN .....	160
Figure 5-16: Throughput for 20 pair of users include 1 malicious user in DSMCRN.....	161
Figure 5-17: Throughput for 20 pair of users include 4 malicious users in DSMCRN.....	162
Figure 6-1: Recording LUs activities over licensed data channels.....	172
Figure 6-2: Total communication times for 10 pairs of CUs over control and data channels.....	176
Figure 6-3: 1500 bytes of Data activities over the SLDCHs (Red colour represents CUs activities and green colour represents the LUs activities).....	179
Figure 6-4: Total communication time of 20 pair of CUs in MCRN.....	180
Figure 6-5: Throughput for 20 pair of CUs in MCRN without LUs activities ...	181
Figure 6-6: Throughput for 20 pair of CUs in MCRN with LUs activities .....	182
Figure 6-7: Communication time of 20 pair of CUs in MCRN, CREAM and RACRN with and without LUs activities .....	186
Figure 6-8: Throughput for 20 pair of CUs in MCRN, CREAM and RACRN without LUs activities.....	187

Figure 6-9: Throughput for 20 pair of CUs in MCRN, CREAM and RACRN with LUs activities .....	188
Figure 6-10: Communication time of a single pair of CUs in DSMCRN, DSCREAM and DSRACRN .....	189
Figure 6-11: Communication time of 20 pair of CUs in DSMCRN, DSCREAM and DSRACRN without LUs activities .....	190
Figure 6-12: Throughput for 20 pair of CUs in DSMCRN, DSCREAM and DSRACRN without LUs activities .....	191
Figure 6-13: Throughput for 20 pair of CUs in DSMCRN, DSCREAM and DSRACRN with LUs activities .....	192
Figure 6-14: Communication time of a single pair of CUs in SSMCRN, SSCREAM and SSRACRN without LUs activities .....	193
Figure 6-15: Communication time of 20 pairs of CUs in SSMCRN, SSCREAM and SSRACRN without LUs activities .....	194
Figure 6-16: Throughput for 20 pair of CUs in SSMCRN, SSCREAM and SSRACRN without LUs activities .....	195
Figure 6-17: Throughput for 20 pair of CUs in SSMCRN, SSCREAM and SSRACRN with LUs activities .....	196

# List of Tables

Table 2-1: Characteristics of some existing MAC protocols .....	33
Table 2-2: Overview of the attacks occurring at different CR functions .....	47
Table 2-3: Protection mechanisms in CRNs .....	53
Table 2-4: Detection mechanisms in CRNs .....	55
Table 3-1: Security Keys in SSMCRN .....	75
Table 3-2: Security Keys in DSMCRN.....	77
Table 3-3: Encryption methods used in DSMCRN .....	83
Table 3-4: Encryption methods used in SSMCRN .....	101
Table 3-5: The BAN logic symbols .....	109
Table 3-6: The assumptions that are used in DSMCRN and SSMCRN.....	110
Table 3-7: The variables that are used in DSMCRN and SSMCRN .....	110
Table 4-1: Generating and verifying digital signatures in DSMCRN.....	124
Table 4-2: Time to generate and verify MAC-keys in the registration phase of DSMCRN .....	128
Table 4-3: Time to generate and verify MAC-keys in the registration phase of SSMCRN .....	128
Table 4-4: Time to generate and verify MAC-key in the control phase of SSMCRN .....	130
Table 4-5: Time to generate and verify MAC-key in the control phase of DSMCRN.....	130
Table 4-6: Time to apply and verify MAC-keys in Data phase of DSMCRN and SSMCRN .....	130
Table 4-7: AES and RSA implications in DSMCRN and SSMCRN .....	131
Table 4-8: AES implication in Registration phase of the DSMCRN and SSMCRN .....	132
Table 4-9: AES implication in control phase of the SSMCRN .....	133
Table 4-10: AES implication in the common frames of control phase SSMCRN and DSMCRN.....	134
Table 4-11: AES implication in the data phase of DSMCRN and SSMCRN ....	134
Table 4-12: RSA implication in the registration phase of the DSMCRN and SSMCRN .....	135
Table 4-13: RSA implication in the control phase of the DSMCRN.....	136
Table 5-1: The network parameters .....	142
Table 5-2: DSMCRN and SSMCRN frames .....	142
Table 5-3: Throughput parameters.....	148
Table 5-4: The differences in the time and throughput of DSMCRN and SSMCRN .....	164
Table 5-5: Contributions regarding the security threats and countermeasures in DSMCRN and SSMCRN.....	165
Table 5-6: Contributions regarding the security threats and countermeasures in DSMCRN and SSMCRN (cont.) .....	166
Table 6-1: MCRN frames.....	169
Table 6-3: Control and data frames in MCRN, CREAM and RACRN.....	183

# Chapter 1 INTRODUCTION

Radio spectrum is a natural resource, spanning a range from 3 KHz to 300GHz, with most of it remaining underutilised (Tang & Wu, 2012). In 1999, Joseph Mitola (Mitola & Maguire, 1999) introduced a new technology called Cognitive Radio Network (CRN). This is based on different techniques namely Software Defined Radio (SDR), Opportunistic Spectrum Allocation (OSA), and Dynamic Spectrum Allocation (DSA). This technology intelligently adapts its environment to facilitate transmission among the cognitive nodes.

This chapter discusses the background of the CRN technology and its main core functions that enable the unique characteristics and operations of the technology. In addition, it focuses on the details of the spectrum sharing classifications, security, and their related challenges. Since spectrum sharing is enabled through usage of the common control channel (CCC), more attention is paid to the security of this channel. The chapter also introduces the security requirements in CRNs, and the research issue. The main aim and objectives of the research along with its scope and limitations are defined. The chapter is concluded with an overview of thesis organisation.

## 1.1. Cognitive Radio

Cognitive Radio (CR) (Tang & Wu, 2012) technology promises to intelligently solve the issues in conventional wireless technology related to their limited and under-utilised spectrum (Shin, et al., 2010). This problem has become an issue of greater concern given the continued increase in wireless devices that use unlicensed bands to operate, which has resulted in overcrowding, leading to inefficient use of these spectrum (Zhao, et al., 2007) (Zheng, et al., 2008) (Wang, et al., 2008). Therefore, CR provides a resolution to spectrum inefficiency and the shortage on these bands by allowing CR users to opportunistically access the vacant spectrum (Chen, et al., 2008). This in turn results in great opportunities for a rising number of cognitive users (CUs) to use these bands through an optimised approach for utilising radio resources (Lin, et al., 2011) (Baldini, et al., 2012).

A cognitive radio network (CRN) has its own intrinsic fundamental approach and principle for dynamic operation within the environment, unlike the conventional wireless network approach that is based on static radio frequency spectrum with fixed licensed users (LUs) and fixed channel (Zhang & Li, 2009). This indicates that the cognitive ability and re-configuration capability are the core elements that make CR an advanced technology that grants dynamic access to the unused spectrum for both licensed and unlicensed users through certain characteristics: *adoption, awareness, modification, capability of learning, observation, and communication* in realistic environments (Ucek & Arslan, 2009) (Sanyal, et al., 2009) (Wang, et al., 2010) (Huayi & Baohua, 2011) (Parvin & Hussain, 2011) (Tang & Wu, 2012) (Gao, et al., 2012). These characteristics provide reliable communication among CUs at anytime and anywhere as a smart and intelligent choice to operate dynamically through Artificial Intelligence algorithms such as *spectrum sensing, spectrum sharing* and *spectrum mobility* (He, et al., 2010) (Tang & Wu, 2012). Moreover, they differentiate this new CR technology from existing wireless technologies. Due to these sophisticated features, the CR approach is known as Dynamic Spectrum Access (DSA) or Dynamic Spectrum Management (DSM) (Datla, et al., 2009) (Baldini, et al., 2012), in recognition of the potential to realise dynamically different paradigms within a network. Therefore, CRN can be defined as:

*A wireless system-based network with more intelligent functions that provide unique characteristics to adjust to sophisticated network environments, parameters, and policies for CUs to improve the spectrum utilisation.*

## 1.2. Cognitive Radio core functions

There are four fundamental functions that a CRN device must perform as shown in Figure 1-1 and stated below (Baldini, et al., 2012) (Domenico, et al., 2012):

1. **Spectrum sensing** identifies the parts of the accessible spectrum and senses the presence of the primary (licensed) user operating in the licensed band.
2. **Spectrum management** determines the best channel to establish communication.
3. **Spectrum sharing** sets up a coordination access among users on the selected channel.
4. **Spectrum mobility** vacates the channel in case the LU is detected.

One failure can easily affect and deteriorate the communication or introduce vulnerabilities to the network. Each piece of information gained from a specific spectrum element will be supplied to the next component in order to initiate its task (Baldini, et al., 2012).

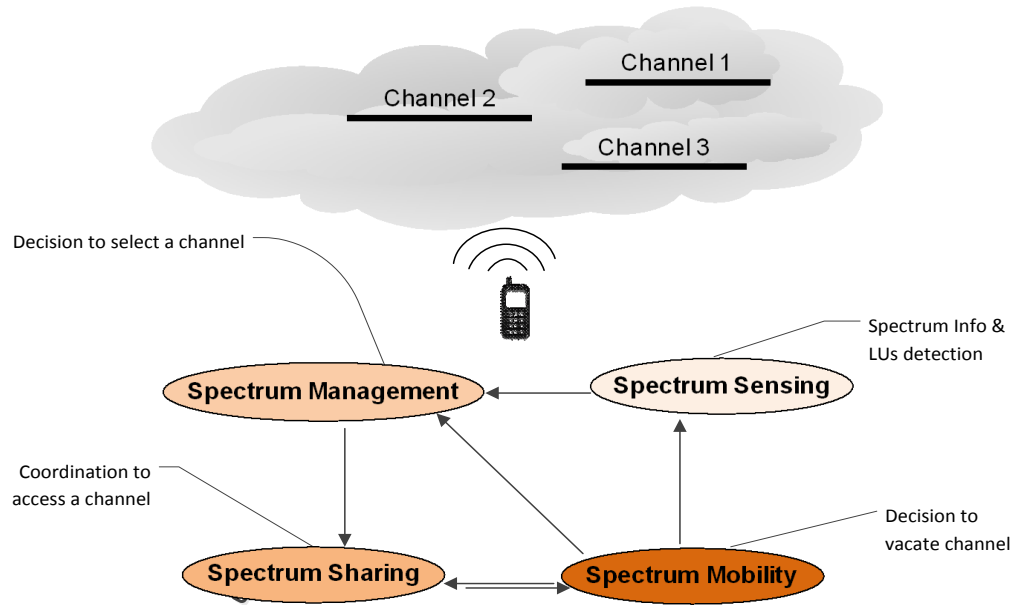


Figure 1-1: Cognitive Radio Main Functions

These embedded functions have a strong relationship between them for the process of establishing an efficient communication considering the regulations and policies that govern CRNs. Each function influences another by providing the necessary information required during the process of reaching a final decision. For instance, once the spectrum is sensed in order to identify the available point of access, there are two possible decisions that can be taken: 1) If the LU is detected, then the process will be discontinued; and 2) if they are not detected, then the obtained information will move forward to the next stage. The spectrum management function then decides upon and selects the proper channel for the communication. Once the most appropriate channel is chosen, users are directed to access the channel by providing their information. During a successful communication, spectrum mobility remains ready for any changes that resulted from the appearance of a LU by a regular check of the spectrum sensing element, or from other alterations to the environment in terms of the current

allocation that is provided by spectrum management and spectrum sharing elements (Baldini, et al., 2012) (Umamahesw, et al., 2012).

As long as CRNs have a set of nodes that interact with each other using determined policies, regulations and sophisticated protocols (Kamruzzaman & Alam, 2010), they have different capabilities, relating to the spectrum awareness of the network operation and spectrum context, defined regulations and policies, quality of service (QoS), and user requirements for requesting traffic load capacity, resilience and security (Ji & Liu, 2007) (Zhang, et al., 2008). This means that cognitive nodes are able to dynamically reconfigure themselves according to the current environment in order to transmit and receive on different frequencies, in addition to supporting a variety of transmission access technology schemes (Akyildiz, et al., 2009) (Shin, et al., 2010). Another capability is for resource management that plays an important role in collaborating to assign the vacant network spectrum management resources, whether these are internal to the current network or external to conventional wireless networks (Wei, 2011) (Baldini, et al., 2012).

### 1.3. Spectrum sharing classifications

Spectrum sharing can be generally classified into three major criteria based on the; *Network architecture*, *Access technology*, and *Allocation behaviour* (Figure 1-2). These classifications can be described as follows:

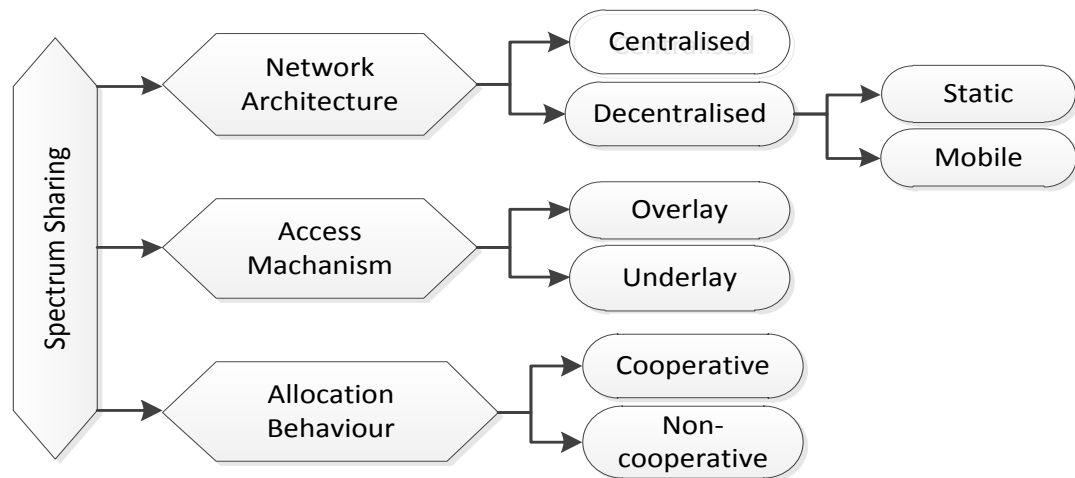


Figure 1-2: Spectrum sharing Classifications

### 1.3.1. Network architecture

The first technique is based on the network architecture, whether it is centralised or distributed (or ad-hoc). In centralised networks such as IEEE 802.22 cognitive radio, a base station governs and senses the free channel information from its neighbour's nodes within range (Huahui, et al., 2010). Unlike distributed CRNs, the IEEE 802.22 standard requires the final decision on the availability of a channel to be performed at the local observation (Figure 1-3). CR nodes in ad-hoc fashion generate and utilise a common spectrum allocation for the exchange of information about available channels (José, et al., 2015) (Baldini, et al., 2012) (Zhang, et al., 2008). Even though there is a positive perspective of the centralised entity in order to address better efficiency, the main drawback is that the central entity represents a single point of failure (José, et al., 2015) (Baldini, et al., 2012). More classifications can be added into ad-hoc networks, classifying them into *static* and *mobile* networks. These apply in Wireless Sensor Networks as a static form, and in MANETs (Mobile Ad-hoc Networks) as mobile ad-hoc networks in which a set of autonomous mobile terminals are liberated to move to other existing hybrid networks (Alhakami, et al., 2014).

### 1.3.2. Allocation behaviour

The second technique is based on allocation behaviour whether it is *cooperative* or *uncooperative*. In terms of the cooperative method, CUs are responsible for coordinating the functionalities of the CRN in order to ensure the optimisation of the utilisation of the spectrum and improving network efficiency through the exchange of information. However, in the case of uncooperative systems, CUs are not responsible for coordinating the functionalities of the cognitive devices with other CUs. Instead, they implement these functions on their own (Ejaz, et al., 2011) (Umamahesw, et al., 2012). The main difference between these two methods is relatively clear: the first approach essentially requires the exchange of information, hence a control channel is strongly required to facilitate the exchange of this information. Whereas in the second approach the cognitive nodes do the network functions' tasks on their own without the need for any collaboration from other CUs. This would make the task more challenging and

difficult for a CU. In addition, this can affect the performance due to reasons like lower efficiency, slower sharing of spectrum resources' allocation, and less reliability than the cooperative technique (Wang, 2009) (Baldini, et al., 2012) (Gao, et al., 2012) (Umamahesw, et al., 2012).

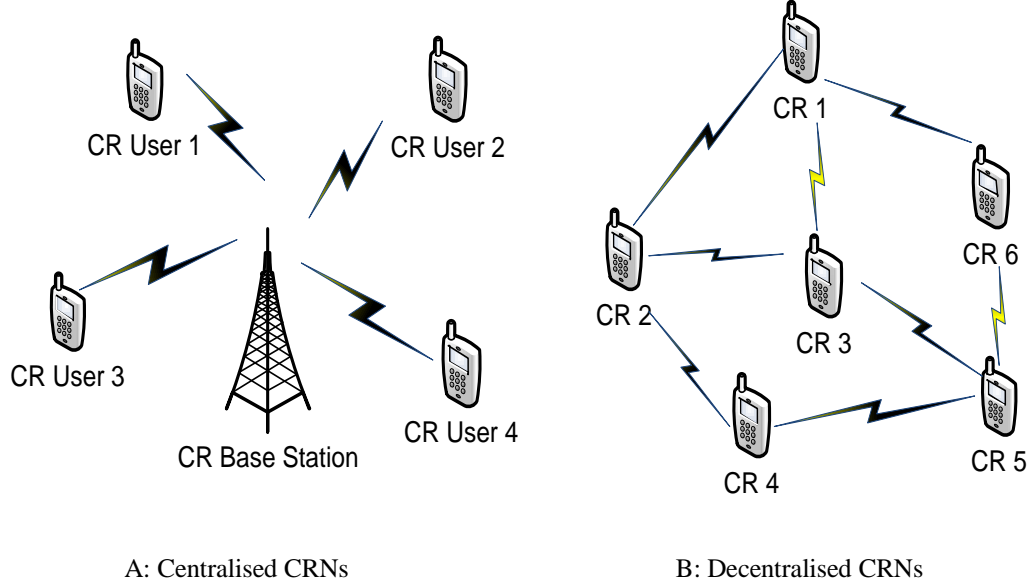


Figure 1-3: CRNs Architecture

### 1.3.3. Access technology

The last classification is access technology whether it is *overlay* or *underlay* (Ji & Liu, 2007) (Arkoulis, et al., 2008) (Zhang, et al., 2008) (Jinhyung & Wan, 2010) (Umamahesw, et al., 2012). In the overlay approach a CU utilises the spectrum without sharing with a LU. This is in contrast to the underlay approach in which both LUs and CUs utilise the licensed spectrum at the same time (Zhao & Swami, 2007) (Wyglinski, et al., 2010) with strict power control implemented by the CUs not to interfere with the LUs.

## 1.4. Research Background

As discussed in section 1.1 that the CRN is a novel approach of wireless communication and is completely different from the traditional wireless network. The main objective of deploying CRNs is the ability of offering substantial wireless communication that effectively improves the unused spectrum for gaining better connectivity through occupying the white spaces dynamically. This dynamic operation requires cognitive ability and re-configuration capability that

CRNs perform to gain dynamic access with the help of the unique CR functions and characteristics that distinguish it from the conventional wireless networks (Chauhan & Sanger, 2014). However, this would not be successful and accomplish the demand of maintaining the network and CUs' needs without incorporating security factors and validating the communication security requirements namely; authentication, authorization, availability, data confidentiality, privacy, and registration (Rizvi, et al., 2014). These security requirements have been emphasised and highlighted in several recent surveys, such as in (Khasawneh & Agarwal, 2014) (Li, et al., 2015) (Girraj & Ritu, 2015) (Sharma & Rawat, 2015), that have been discussed in the literature review and related to the CR security, for the need of addressing the security factors leading to achieving the demand of successful communication among CUs in the CRNs.

Therefore, CRNs should ensure the same security level as that of conventional wireless networks. However, due to the sophisticated characteristics and dynamic operation of CRNs that were discussed in section 1.1, CRNs present new security threats (e.g. primary user emulation attack, primary user interference attack, falsifying data, denial of service attack, etc. (Li, et al., 2015) (Girraj & Ritu, 2015)) that guarantee achieving malicious users' goals for compromising the network communication and its resources. Therefore, this issue becomes more critical in a cooperative approach, where CUs require exchanging a set of available channels that are not occupied by licensed users. Consequently, malicious users can easily exploit this opportunity by targeting the CUs' activities for malicious and selfish purposes such as gaining unauthorised access, making the exchanged channels unavailable, creating interference over the selected channels, modify or replacing the transmitted channel information. Accordingly, malicious users terminate the communication and increase the possible damages to the licensed users' activities over the licensed channels. Thus, CRNs strongly need to incorporate the security by all possible means for providing successful communications among CUs requiring the meeting of their demands.

### **1.4.1. Security requirements in CRNs**

In order to maintain the network performance, several security aspects must be considered and addressed in CRNs. These are explained as follows:

#### **1.4.1.1. Access control**

As access control provides the guarantee to access the network only if CUs meet and follow the defined policy, it coordinates the CUs' spectrum access to avoid collisions that may occur due to utilising the same band. Thus, the security property of the physical layer plays a major part to ensure the correct and unmodified spectrum sensing information (Xiang, et al., 2010) (Parvin, et al., 2012).

#### **1.4.1.2. Confidentiality**

Here the information is accessed only by the intended authorised users and it is transmitted in unintelligible form to the unauthorised users. Confidentiality is considered as a significant security requirement element in CRNs as the available channels are not guaranteed (Mathur & Subbalakshmi, 2007) (Parvin, et al., 2012) (Hanan, et al., 2014) (Rizvi, et al., 2014).

#### **1.4.1.3. Authentication**

Authentication schemes are widely considered to be the best solution to ensure data is transmitted amongst authorised users and that only those legitimate users can access the transmitted data (Zhu & Zhou, 2008) (Alhakami, et al., 2012) (Hanan, et al., 2014). This requires that data integrity is preserved from any modification, as information messages propagate through a number of users in order to arrive at their destination. This is particularly important when wireless technology permits the injection of adversary packets in multi-hop environments, which increases the level of threats (Alhakami, et al., 2012). Therefore, the application of an authentication mechanism is intended to protect the network from eavesdropping, and the saturation of the CCC making it prone to a DoS attack. Usually adversary users have their own targets and interests to affect the network and its performance. Encrypting the negotiation/control information phases help to maintain the whole network by hiding decisions from the adversary

users (Zhu & Zhou, 2008). For instance, once the Free Licensed Channels List (FCL) has been determined between two CUs, an encryption mechanism will hide the FCL information from any malicious users once they need to switch to a different channel. The use of cryptography techniques for exchanging control channel information is essential to prevent potential misbehaviour (Zhu & Mao, 2011) (Baldini, et al., 2012) (Alhakami, et al., 2012).

During the negotiation phase, the authentication mechanism and encryption algorithm function to ensure secure communication between the CUs. As discussed in (Zhu & Zhou, 2008), a network vulnerability can be opened for attackers if insecure transmission is launched, in which an attacker easily exploits this chance to launch DoS attacks. However, due to the absence of a centralised node to act as a base station in multi-hop environments, an authentication scheme should be relatively simple in order to save energy for CUs. This means that complexity can be a drawback in some cases due to the greater energy and time required to process the security algorithms. Nevertheless, the authentication in a multi-hop environment will avoid the most common threat in centralised networks, which is having a single point of failure. This type of threat is common among all types of centralised networks such as IEEE 802.11, IEEE 802.15 and IEEE 802.16. However, this problem is lessened in multi-hop networks, where the authentication mechanism takes place locally between CUs (Alhakami, et al., 2012).

### **1.4.1.4. Availability**

This is the process of ensuring the authorised access to resources at any time. The security purpose here is to make the stored information and resources available to, or being processed by, the authorised user (Sazia, et al., 2012). In centralised networks such as IEEE 802.22 cognitive radio, a base station governs and senses the free channel information from the neighbour's nodes within the range. Although the IEEE 802.22 standard (Stevenson, et al., 2009) establishes that the final decision on the availability of a channel must be performed at the base station for both CUs and LUs, in decentralised networks there is no central entity to collect the information for the available channels. Therefore, security features are required to be equipped with CUs for maintaining the network,

achieving the procedure on how nodes securely update their information with their neighbours (Alhakami, et al., 2012) (Hanen, et al., 2014) and preventing DoS attacks while making the spectrums available for both LUs and CUs.

### **1.4.1.5. Authorisation**

Authorisation is the ability of the system to allow the access to the network. It requires authorised parties to be allowed to configure and manage the spectrum without the base station. Cognitive nodes must successfully authenticate their encrypted configuration and information among the nodes by using an efficient algorithm.

As long as the main focus of this thesis is the MAC layer security which considers the core point that deals with data transmission between two different CUs, the availability of the CCC is the most essential part to allow for the negotiation and transmission of data among CR users. However, the CCC is mainly targeted by a malicious user to launch the DoS, and Selfish behaviours aiming to maximise their performance interest or saving energy instead of cooperating in communication between two nodes through itself (Leon, et al., 2010). The MAC layer is particularly vulnerable due to existing weaknesses within itself in terms of poor authentication in multi-hop networks. Additionally, the lack of an encryption mechanism for exchanging frames in the control channel creates easy access for any malicious behaviour. Once the control channel becomes saturated by an attacker, the service can be compromised by a DoS attack. Since CR ad-hoc networks do not have any centralised entity, the authorisation becomes more challenging (Alhakami, et al., 2012).

### **1.4.1.6. Integrity**

Integrity refers to the assurance of transmitting data from any modification, insertion and/or deletion. It is significantly important as the technology uses wireless medium for transmitting data and permits the injection of adversary threats. Therefore, using advanced cryptographic techniques assist to achieve data integrity in CR technology (Parvin, et al., 2012) (Hanen, et al., 2014).

#### **1.4.1.7. Non-repudiation**

Non-repudiation aims to achieve the transmitted message from being denied by either the sender or receiver CUs (Hanan, et al., 2014). Hence, it provides the assurance of the transmitted message from the right user and can then be used as a proof against themselves if they attempt to misbehave (Zhu & Mao, 2011) (Goyal, et al., 2011) (Rizvi, et al., 2014).

### **1.4.2. Cryptographic schemes**

As long as cryptographic schemes play significant roles to secure and ensure the authenticity and integrity of the transmitted information within a network, they are different in their functionalities and operations of managing their keys that are employed for the encryption/decryption procedures and message authenticity. For example, both symmetric and asymmetric key algorithms function to guarantee secure transmission while the Message Authentication Code (MAC) algorithm provide the integrity and authenticity assurance of the transmitted messages within a network (Toldinas, et al., 2011) (Koopman & Szilagyi, 2013). Therefore, these algorithms are discussed in details as follow:

#### **1.4.2.1. Asymmetric-key algorithm**

This is also referred to as Public Key Cryptography in which two different keys known as private and public keys are applied. Each user has a pair of these keys for encryption and decryption purposes. The public key is used to encrypt the transmitted data and does not require a secure system for the secure key distribution while the private key is kept securely by the user to decrypt the received information. The Public Key Cryptography algorithm is more secure and supports another efficient security technique known as digital signature which provides message authenticity. However, the limited energy of the devices is affected by the usage of the key size which is required to be considered to provide the demand of the security. RSA is an example of public key cryptography algorithm (Krishna & Doja, 2011) (Kaur, 2013).

#### **1.4.2.2. Symmetric-key algorithm**

It is also known as shared key, where a single, secret key is shared between two or more entities for encryption and decryption purposes (Kaur, 2013). Each user can encrypt or decrypt the transmitted information using the same key and this also can be applied to other users who have the same shared key. This has lower complexity than the public/private key pair, thus making it more energy efficient (Krishna & Doja, 2011). However, it requires a secure system in order to distribute the shared key among the participating users within the network. The AES algorithm is an example of a Symmetric-key system.

#### **1.4.2.3. Message Authentication Code (MAC)**

MAC has been used widely in different networks due to the efficient functionality that can be provided within such communication. It is used in a situation that requires integrity assurance and message authenticity (Koopman & Szilagyi, 2013). An attacker can modify the transmitted message through applying bit flipping of that original message before it is received by the intended destination. Therefore, the receiver is not able to detect any modification occurred on the original transmitted message unless a shared secret key is used to key message coding in order to generate a Message Authentication Code Key (MAC Key) for the assurance of message integrity and authenticity (Capkun, et al., 2008).

### **1.5. Motivation**

The CRN MAC layer functions in sharing the physical medium for establishing the communication among users wirelessly within the same range. However, achieving a successful communication in CRNs is a challenging task and considered one of the most critical issues, since the CRN suffers from various presented security threats that lead to DoS attacks due to its inherent characteristics (Hananen, et al., 2014). These threats target all the CR functions; spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility for the aim of preventing CUs from using the available white spaces (Zhang & Lazos, 2013) (Sharma & Rawat, 2015). Consequently, the overall network operation and performance is easily affected in a DoS attack. Therefore, performing security at the MAC layer of the cooperative decentralised CRNs is

essential for providing defence against the MAC layer security threats related to the channels availability and successfully leads to achieving the CUs goal of successful and efficient communication over the unused spectrum (Rizvi, et al., 2014).

Moreover, maintaining secure communication is another crucial aspect to guarantee the exchange of control information and data between CUs. However, the primary security concerns in decentralised CRNs are authentication and data confidentiality (Alhakami, et al., 2014). Compromising on these elements can potentially lead to the modification, forgery, or eavesdropping of the MAC frames in CRNs, which could, in turn, increase the chance of DoS attacks that would adversely affect the performance of the network. However, these security factors in distributed CRNs have received relatively little attention in the literature, perhaps due to their complex nature and dynamic topology (Goyal, et al., 2011) (Alhakami, et al., 2014). These must be investigated properly in order to meet the security needs of the CRNs technology. Further research is required in order to support the security requirements, especially to provide authentication assurance for the authorised access. These requirements assist in maintaining secure communication and enable the provision of available resources in distributed multi-hop CR environments, while simultaneously avoiding external threats. Moreover, an encryption method is required to support secure communication between end users, and considering the inherent power limitations of the devices (Goyal, et al., 2011). This issue is also important because of the lack of a central entity that provides security and key management to end users. Thus, the simulation of a secure CR MAC protocol must involve the design and simulation of a robust, secure system that can achieve authentication, availability, confidentiality, integrity, non-repudiation, anonymity, and authorisation to achieve the security demands (Attar, et al., 2012) (Alhakami, et al., 2014).

### **1.6. Problem statement**

The MAC layer of decentralised CRNs is more exposed to security threats and attacks such as eavesdropping, forgery, DoS, and selfish behaviours. These vulnerabilities represent the main security concerns in CRNs (Hanan, et al., 2014)

(José, et al., 2015). A compromise on authentication and data confidentiality can lead to the modification and forgery of MAC CR frames resulting in potentially increasing the chance of DoS attacks (Zhu & Zhou, 2008) (Tang & Wu, 2012) (Attar, et al., 2012). For this reason, an authentication and secure communication mechanism in decentralised CRNs is strongly needed due to the absence of a trust entity among CUs. Unlike in traditional wireless networks, such as Wi-Fi and WiMAX, where base stations and access points function as central and core entities that provide security key management to end users, CUs need to incorporate security by all possible means in order to protect the network components. However, the authentication mechanism in decentralised CRNs has not received much attention (Yu, et al., 2010) (Tan, et al., 2011), and the related vulnerabilities are likely to remain unsolved due to the discrepant unique environment (Jhaveri, et al., 2012). Further research is essentially required for the demand of achieving strong authentication to maintain a secure communication in distributed multi-hop CR environment.

The control channels selection in decentralised CRNs decreases the probability of successful communication among the cognitive nodes due to authenticity and validity of the CUs. As discussed in (Sanyal, et al., 2009), CUs are the non-licensed users and attackers easily exploit the CUs, escalate their privilege, and might damage the spectrum and the traffic of the LUs as well. Moreover, without security, this issue becomes more critical when cognitive nodes use the spectrums in the absence of the LUs or not using their licensed bands. Moreover, selecting data channels for exchange of data among the cognitive nodes without the authenticity of the CUs is another issue that needs to be addressed in CRNs especially for maintaining the links if the LU returns to the licensed data channel. A number of research has been conducted in developing security in centralised CRNs (Cordeiro, et al., 2005) (Wang, et al., 2008) (Shin, et al., 2010). However, the issue is that there is little intention being given for investigating and developing a complete secure MAC protocol for providing authentication, confidentiality, non-repudiation, and integrity in decentralised CRNs (Zhu & Zhou, 2008). For example, the authors in (Zhu & Zhou, 2008) investigated and analysed DoS and greedy attacks of the MAC layer in decentralised CRNs, but

they do not consider such a mechanism to protect the network from these attacks. Moreover, there are some recent publications that theoretically highlight the importance of addressing the security challenges and its requirements such as in (Attar, et al., 2012) (Hanan, et al., 2014) in decentralised CRNs environment. Furthermore, some researchers have introduced individual security techniques that assist in the detection of a malicious user based on a timing parameter technique and puzzle punishment through the control phase (Rakhshanda, et al., 2008) (Huayi & Baohua, 2011). These techniques are useful in some circumstances for controlling selfish attacks which target to maximise attackers' throughput, or to saturate the channel by sending frequent packets. However, these techniques do not identify misbehaving users from being internal or external in the CR MAC protocol.

Therefore, there is a strong need of deploying a complete secure MAC protocol to ensure the successful communication among the intended CR users and maintain the network operation in decentralised CRNs. According to (Wang, et al., 2010) and (Rizvi, et al., 2014), the integration of security precautions should be at the MAC layer for ensuring the authenticity and integrity among CUs in distributed CRNs environment. Consequently, this research attempts to detect malicious behaviour and protect the channel sensing results from adversary users who target the spectrum management in the cooperative approach leading to a DoS attack. Another aspect considered in this research is related to improving the network efficiency and connectivity by utilising effective security algorithms. In addition, the main security requirements that were discussed in section 1.4.1 especially authentication, is taken into account as the primary element, and develops two hybrid secure MAC protocols with a dedicated server being involved for authentication purposes and for providing security keys to only the registered CUs. These secure protocols should operate with minimum handshaking frames between CUs as required to address the main security requirements in decentralised CRNs. The research also aims to investigate and analyse the malicious behaviours' impact on the network performance.

## 1.7. Research aim and objectives

This research aims to develop a novel secure MAC protocol for decentralised CRNs. The objectives of this research are:

- ❖ To investigate existing secure MAC protocols in CRNs (both decentralised and centralised) and the different types of attacks that are possible in CRNs in order to identify the security flaws in the existing MAC protocols
- ❖ To propose, and design a novel hybrid secure MAC protocol for CRNs (SMCRN)
- ❖ To perform security analysis of the proposed protocol using the BAN formal logic
- ❖ To implement and analyse the performance of the proposed hybrid secure MAC protocol through simulations
- ❖ To evaluate the performance of the proposed hybrid secure MAC protocol against other secure protocols.

## 1.8. Research Contributions

- Accomplishing an efficient decentralised CRNs MAC protocol that performs minimum handshaking frames to increase the network performance.
- Deploying two versions of secure MAC protocols to provide strong defence against MAC layer security threats.
- Reducing the communication time of malicious users' activities over the CCC. Thereby, the detection of transmitted fake control frames, which aim to increasing the network and server overload in SSMCRN, leads to increasing the CCC availability to other CUs and then resulting in achieving higher network throughput.
- Limiting the transmitted secure control information to only a single pair of CUs to protect the SLDCH from being targeted by internal and external malicious users to make the SLDCH unavailable or launch a jamming attack.
- Protecting the sensing result information (FCL) and the SLDCHs availability from launching DoS attacks that can be resulted by modifying

the transmitted control information. Thus, both of the secure protocols ensured the integrity and authenticity of this transmitted information to enable spectrum management taking the correct decision based on the data channel selection criteria.

- Investigating and analysing the impact of both the unauthorised access and modification attacks on the transmitted information in each of the secure protocols.

## 1.9. Research methods

Due to their adaptive nature, cognitive nodes are difficult to authenticate without any centralised entity like a base station (BS). Although, there is a number of published work that attempted to address the security issues in CRNs (Sanyal, et al., 2009) (Sazia, et al., 2012) (Parvin & Hussain, 2011) (Zhu & Mao, 2010) (Zhu & Mao, 2011) (Minho, et al., 2013), most of these studies focus on the security in centralised CRNs where BSs are involved in the communication (Zhu & Mao, 2010) (Zhu & Mao, 2011) (Parvin & Hussain, 2011) (Sazia, et al., 2012). However, few published work on the security in decentralised CRNs have only addressed the selfish attack which is one of the existing security issue in CRNs (Minho, et al., 2013), while others such as (Sanyal, et al., 2009) simply provided a theoretical approach instead of simulating the network to show any results to confirm their work. Therefore, authentication, data integrity, and secure communication are strongly needed in a cooperative approach within a CR environment in order to limit the transmitted data to authorised and legitimated users only (José, et al., 2015). This leads the work carried out in this research and discussed in this thesis to design and implement a novel secure MAC protocol for decentralised CRNs with the minimum handshaking of frames between a pair of CUs in order to compare and evaluate against an existing well-known MAC protocols on performance terms.

This study, therefore, proposes to explore the generic security mechanisms of authentication, authorisation, and integrity for wireless decentralised networks. Based on the desired security requirements in CRNs, a selection of security

features will be incorporated within the proposed MAC protocol for decentralised CRNs.

Particular attention will be given to the private/public key pair, and secret (shared) key cryptography mechanisms, Message Authentication Code algorithm, and digital signature with the aim of investigating the possibility of these algorithms being used by two CR nodes and addressing the security issues related to the MAC layer in CRNs. This will be achieved by selection, analysis, and testing of the proposed MAC protocol in terms of security flaws.

The above mentioned security features will be incorporated within two benchmark protocols for comparison with the proposed secure MAC protocol on their overall performance.

### **1.10. Scope and limitations of the research work**

Since the CR is completely different from the conventional wireless network (section 1.1 details the differences between CR and traditional wireless networks) the scope of the current research is to address the authentication, authorisation, confidentiality, and non-repudiation procedures for ensuring secure data transmission amongst authorised CUs in only CRNs. Thus, the security in conventional wireless networks is excluded from this research due to the different operations and subsequent security approaches for the secure communication in the context of these networks. Therefore, the current research maintains the security in the CRNs by utilising an authentication server and cryptographic symmetric and asymmetric keys to maintain a secure communication among the CUs. Moreover, the proposed protocol in its two versions based on the type of keys used will address several malicious behaviour attacks such as eavesdropping, spoofing MAC address, forgery, DoS, and masquerading, and provide mitigation procedures against Spectrum Sensing Data Falsification attacks and Jamming attacks. These threats are taken in consideration and prevented from attacking the network. Some other attacks such as PUE and selfish attacks are not addressed in this work, since the PUE belongs to the physical layer and analyse LUs and other users' signals with a number of work already conducted and published on it, while the selfish behaviour where selfish users intend to maximise their throughput has

also been addressed in (Huayi & Baohua, 2011) (Minho, et al., 2013). These selfish behaviour detection mechanisms can be applied in the proposed Digital Signature based Secure MAC Protocol for Cognitive Radio Networks (DSMCRN) and Shared Key based Secure MAC Protocol for Cognitive Radio Networks (SSMCRN) protocols for selfish users' detection. Thus, there is no significant reason to address the selfish behaviour detection in the proposed protocol while the existing schemes effectively work against this type of attack and can be incorporated in the DSMCRN and SSMCRN.

On the other hand, the main reason of deploying two different versions of secure MAC protocols is to investigate and analyse the authentication mechanism by applying different security approaches, digital signature and shared key, and how these different security algorithms can affect the network time performance and throughput. It is necessary that the all the security requirements required to be addressed to provide strong security against any malicious behaviour.

### 1.11. Thesis organization

The following chapters of the thesis can be summarised as follows:

**Chapter 2:** This chapter details work that has been done by other researchers in CRNs and is categorised in two main parts belonging to the common features of CR MAC protocols for utilising and improving the spectrum efficiently and the security threats. These common features include the spectrum sensing techniques, spectrum access techniques, and number of associated transceivers that are equipped by a CU. However, the security part introduces the details of the common security threats in conventional wireless and CRNs, the specific security threats in CRNs with more attention given to the protection and detection mechanisms that have been done by researchers in spectrum sharing security in CRNs.

**Chapter 3:** This chapter discusses the design and simulation of the proposed MAC protocol without involving the security features. It introduces the protocol's architecture and features such as the number of radios in each CU, CCC access technique, spectrum sensing, and licensed data channel selection criteria. Moreover, the protocol's evaluation in terms of the communication time and message delivery

rate along with the LUs activities and its impact on the protocol performance is analysed and introduced in this chapter.

**Chapter 4:** This chapter introduces a framework of the two versions of the proposed secure MAC protocol for CRNs. It also details the protocols' frames exchanges and the associated security algorithms for securing the data transmission among the intended CUs. In addition, the chapter introduces the analysis of the frames' transmissions among the contributed entities in the format of the formal BAN logic, which mainly considers the security features, to validate the proposed secure MAC protocols.

**Chapter 5:** This chapter presents the simulation stage of the associated security features in the two versions of the proposed secure MAC protocol that were discussed in Chapter 4. It highlights the security execution time of each applied security algorithms such as RSA, AES and MAC, for encrypting and decrypting the transmitted information, verifying and ensuring the integrity of the transmitted messages, and generating and verifying of the digital signatures for the authentication procedure.

**Chapter 6:** This chapter focuses on the simulation of the communication part of two versions of the proposed MAC protocol with the associated security features. Both versions are analysed and compared to each other in order to investigate their operations time, and throughput analysis. Furthermore, the impact of malicious users' behaviours in terms of modification on the transmitted messages, and unauthorised access are analysed along with their defence against these malicious activities. The chapter also investigates the LUs activities and its impact on the network performance of the proposed secure MAC protocols.

**Chapter 7:** This chapter presents the comparative analysis of the proposed and benchmarks protocols with and without security in terms of the operation time and network's throughput as network performance factors. In addition, the influence of the LUs activities on the communication time and throughput of both the proposed and benchmark protocols are analysed and compared to investigate their extent on each protocol.

**Chapter 8:** This chapter introduces the conclusion part of the thesis along with the future work suggestions.

## **Chapter 2 LITERATURE REVIEW**

This chapter introduces two different main parts belonging to networking and security. It highlights the common features of MAC protocols for CRNs in which they lead to successful data exchange among users. Moreover, in addition to the well-known security issues in wireless networks, CRNs introduce new classes of security threats and challenges, such as LU emulation attacks in spectrum sensing and misbehaviours in the common control channel (CCC) transactions that degrade the overall network operation and performance. This chapter briefly presents both the common security threats in conventional wireless and CRNs. It also outlines the security challenges in CRNs. However, the chapter will mainly focus on spectrum sharing security and its related challenges. Since spectrum sharing is enabled through the use of the CCC, more attention is paid to the security of the CCC by looking into its security threats as well as protection and detection mechanisms. Finally, the pros and cons as well as the comparisons of different CR-specific security mechanisms are presented. Figure 2-1 presents the common features of the CR MAC protocols while clearly highlighting the features of this research's proposed Cognitive Radio MAC Protocol for CRNs (MCRN).

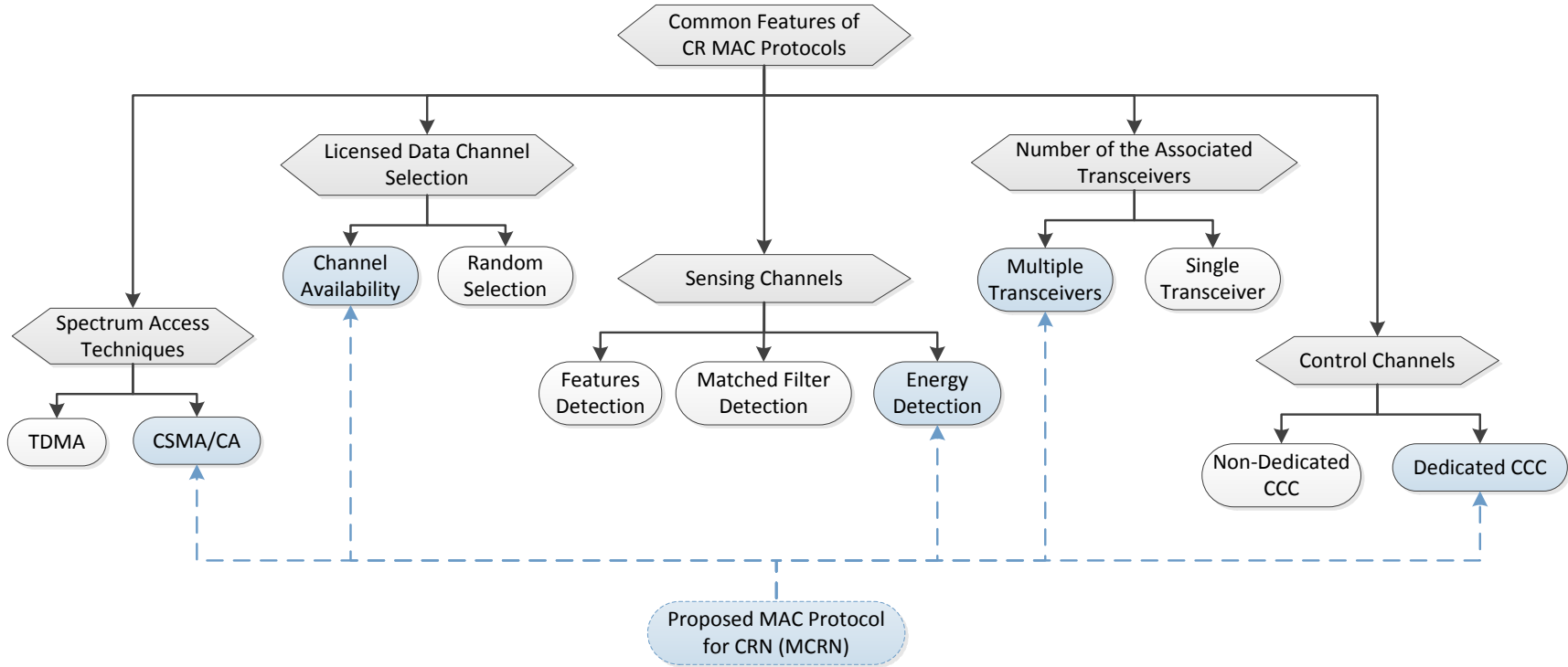


Figure 2-1: Spectrum sharing classification in Ad hoc CRNs and the current research direction

## 2.1. Common features of CR MAC protocols

MAC protocols are designed and implemented to provide the functionality of coordinating the spectrum access among a set of CUs. Several aspects and mechanisms are involved to achieve the aim of a successful data exchange between a sender and receiver. These include the criteria of spectrum sensing to find the spectrum hole, the types of mechanism used being either underlay or overlay for coordinating channel access by multiple CUs, data channel selection, and the number of available radio equipment for each CU.

### 2.1.1. Control channel

The most significant part of the CRNs MAC protocols is the exchanges of the control information among CUs in order to determine the criteria of switching to the appropriate Selected Licensed Data Channel (SLDCH) before initiating the data transmission. This part has received remarkable research that proposed different mechanisms for exchanging control information (Ma, et al., 2005) (Kondareddy, et al., 2008) (Haythem, et al., 2009) (Lin, et al., 2011) (Romero, et al., 2012) in the CRNs. Thus, the control channels can either be static or dynamic. The use of the Industrial, Scientific and Medical (ISM) or underlay ultra-wideband band for exchanging control information is considered as a static approach where CUs are assigned a control channel of unlicensed band such as IEEE 802.11b/g spectrum (2.4-GHz) spectrum (Salameh, et al., 2008) (Haythem, et al., 2009) (Song & Xie, 2012). However, the dynamic channel approach can be classified into two types known as *dedicated* and *non-dedicated* CCC. Only the *dedicated* approach is considered in this work for several reasons that will be discussed later in section 3.2.1.

### 2.1.1.1. Non-dedicated CCC

In this approach, a non-dedicated CCC is assumed among a set of CUs. Hence, a number of CRNs MAC protocols are designed for the exchange control information without a dedicated CCC. Instead, CUs necessitate finding the spectrum hole based on the spectrum sensing of the licensed channels, then they are required to agree about the reliable channel for exchanging their control information. This process necessitates successful completion before initiating their data transmission process over the selected data channel. However, this approach requires stringent time for selecting the control channel and channel synchronisation between CUs.

The work stated in (Joshi, et al., 2009) proposed a MAC protocol for decentralised CRNs with an improved network throughput. Their protocol does not consider a dedicated CCC and instead it deploys a stable control channel for control information exchange among CUs. This is achieved when every CU maintains a status table of channels and indexes these channels frequently. Therefore, the channel that has the highest stability is determined to be the control channel for exchanging control information between a pair of CUs. The work of (Carlos & Kiran, 2007) proposed a Cognitive MAC (C-MAC) protocol for decentralised multi-channel CRNs. The communication process among CUs is based on Rendezvous Channel for selecting the available slot of time to coordinate CUs in discrepant channels. Also, the Communication Rendezvous technique is used in (Theis, et al., 2011) (Zhang, et al., 2014) for the negotiation procedure between two CUs. Thus, a pair of CUs is required to agree and find an available channel to exchange certain control information that belongs to the selected channel for data transmission and its data rate before they initiate data transmission. However, the Rendezvous approach requires additional time for CUs synchronisation and leads to delay occurrence that effect the throughput performance as the network resources are not used efficiently.

Another approach of MAC protocols such as in (Lee & Kim, 2012) requires a predefined channel hopping sequence that is determined among CUs in order to achieve the hopping process over the existing licensed channels (Song & Xie, 2012). Both the cognitive sender and receiver necessitate time and channel

synchronisation (Zhao, et al., 2007). During this process, a proper channel is determined to be utilised to transmit data through exchange of control information between both the sender and receiver cognitive nodes. Once successful control information is exchanged between the sender and receiver, they end the hopping process and start with the second phase of transmitting data. After the completion of the data transmission phase, the synchronisation requests are recurred with the hopping sequence (Haythem, et al., 2009) (Domenico, et al., 2012). Since this approach is achieved over the existing licensed channels (Song & Xie, 2012) both the sender and receiver necessitate time and channel synchronisation (Zhao, et al., 2007).

#### **2.1.1.2. Dedicated Common Control Channel**

In traditional distributed wireless networks, the CCC is one of the existing licensed channels (Ren, et al., 2012) while in centralised CRNs, a dedicated channel can be assigned as a CCC by the central entities whether base stations (BSs) or access points (APs) for exchanging the control information (e.g. channel availability resulting from spectrum sensing) among the central entities' controllers and CUs (Ren, et al., 2012). However, it also can be employed for facilitating the spectrum sharing process between two CUs in distributed cooperative CRNs thus a CCC is established between both the sender and receiver for handshaking control information frames. Due to these effective functionalities, a number of researchers (Kondareddy, et al., 2008) (Safdar & O'Neill, 2009) (Haythem, et al., 2009) (Kahraman & Buzluca, 2010) (Huayi & Baohua, 2011) (Attar, et al., 2012) believe that CCC designed procedures can play a major role in promoting the initiation of the exchange of information processes among cognitive nodes. However, this approach of allocating a CCC for CUs in a distributed CR environment is a major challenge due to the absence of the central entity that provides the management part for determining the CCC channel, and the time difference of the spectrum resources. Therefore, there are two categories of MAC protocols which consider the assumption of the existence of a single dedicated control channel that is available and reliable all the time for CUs to exchange their control information. The first type used is the licensed dedicated CCC to exchange the control information among cognitive CUs (Su & Zhang,

2008) (Yoo, et al., 2009) (Chen, et al., 2011) (Yin, et al., 2011), while the second assumes unlicensed dedicated CCC to be utilised by CUs to exchange their control information. Generally, the dedicated CCC assumption is commonly known for deployment since it is a convenient place where all the CUs can launch and observe the ongoing packets of control information and efficiently simplify the architectures of the MAC protocols (Ren, et al., 2012).

In the work reported in (Zhang & Su, 2011), a MAC protocol called Cognitive Radio Enabled Multi-Channel MAC (CREAM) for decentralised CRNs is proposed. Two types of channels were considered among CUs to achieve successful data exchange. The first was known as the control channel, which is assumed to be dedicated, reliable, and permanently available for the contributing CUs to exchange their available channel lists. Whereas, the second type recognises the data channels for data exchange between CUs.

The protocol operates based on four handshaking control frames over a dedicated control channel. The first two frames are called Ready-to-Send (RTS) and Clear-to-Send (CTS), and are designed to reserve the CCC and solve the hidden node problem, while the other two control frames are known as Channel-State-Transmitter (CST) and Channel-State-Receiver (CSR), and are responsible for exchanging the list of available channels and agreed licensed channels between the sender and receiver. Moreover, two different frames, known as Data and Acknowledgment (ACK) are exchanged between both the sender and the receiver over the selected data channel.

CREAM is based on contention-based mechanism technique for controlled channel access and IEEE 802.11 standard for Distributed Coordination Function (DCF) algorithm backoff time. Moreover, each CU is equipped with a single transceiver for both control and data channels. However, the licensed data channel selection criteria is based on random selection for transmitting data. When the LU appears (ON) to utilise the licensed channel, the CUs necessitate restarting the process of exchanging control information to switch to different available licensed channels for transmitting data. Therefore, due to the use of both dedicated CCC among CUs to exchange control information, and multiple Licensed Data Channels (LDCHs) for data transmission the protocol is considered as the first

benchmark for its comparative analysis with the proposed MAC protocol for decentralised CRNs (MCRN).

The work reported in (Qian, et al., 2013) introduced a cognitive-radio-based carrier sense medium access with collision avoidance (CR-CSMA/CA) MAC protocol for CRNs. The protocol uses the CSMA/CA technique to access the channels utilised by CUs, and can be applied in three different scenarios, where a single channel, multiple channels, and a realistic CCC are used to exchange data among CUs. However, only the realistic CCC scenario is considered and applicable to this thesis, since it has the same feature as the proposed MCRN protocol, wherein a CCC is adopted for the exchanging control information. Therefore, the CR-CSMA/CA operates based on three handshaking frames over the CCC named as PTS, RTS and CTS. The Prepare-To-Sense (PTS) frame aims to ask neighbouring nodes to keep quiet for the next duration. Then spectrum sensing takes place to detect the channels states and determine the available channels. However, Request-To-Send (RTS) and Clear-To-Send (CTS) aims to exchange control information and update the NAV of the CUs. Due to the operational characteristics that are integrated with the CR-CSMA/CA in terms of using a realistic CCC to exchange control information among CUs and multiple LDCHs for data transmission, the protocol is considered as the second benchmark for its comparison with the proposed MCRN, as they have common features for their operations.

In the work reported in (Joe & Son, 2008), a Dynamic Spectrum Allocation MAC Protocol (DSA-MAC) based on Cognitive Radio for QoS Support is designed. The protocol is based on ZigBee channels with multiple transceivers assigned to each CU for accessing multiple channels simultaneously. Although the ZigBee channels have a range from 0 – 26, the proposed protocol specifies channel 0 as a dedicated CCC for adapting four handshaking frames whereas the rest of the channels (1 to 26) are used for transmitting the data. If a LU appears to use the licenced channels, CUs are required to restart the process for selecting both CCC and data channel for transmitting procedures.

The work reported in (Hussein, et al., 2013) proposed a MAC protocol for centralised and decentralised CRNs. The protocol required a control channel to

exchange the control frames for determining the selected available channel for data transmission. Each CU is equipped with a single transceiver and performs 802.11 DCF technique for the control channel access.

The authors in (Jia, et al., 2008) designed a MAC protocol called Hardware-Constrained Cognitive MAC (HC-MAC) for decentralised CRNs in which the assumption of common control channel is available any time for CUs to exchange three different pairs of control frames. The first group includes C-RTS and C-CTS frames which are designed for reserving the control channel while the second group involves S-RTS and S-CTS which aim to exchange the available channels for data transmission between the sender and receiver. Thus, as soon as the data channel is determined both CUs switch to that channel and initiate the data exchange process after that another two frames known as T-RTS and T-CTS are launched over the control channel after the successful data exchange to notify other CUs about the end of the communication process by the current pair of CUs. This would enable contentions among other CUs for the control channel access to exchange C-RTS and C-CTS frames.

The work reported in (Iyer & Limt, 2011) proposed a Multi-channel MAC Protocol for CRNs. The assumption of an existing centralised controller recognised as Spectrum broker is made for obtaining the CUs' information and then determining channel allocation for those CUs. The protocol uses a dedicated control channel for transmitting spectrum sensing information and communication with the spectrum broker, this requires a single transceiver that is tuned for the control channel. Nevertheless, a number of periodic time-slots is used to divide the control channel and assumed to be synchronised with the licensed channels. Thus, each CU is equipped with two transceivers recognised as a control transceiver tuned for the control channel and a software defined radio transceiver tuned to any licensed channels. However, the main issue is that the protocol requires and relies on a Spectrum broker as a central controller for channel management and provides the necessary information for determining efficient channel allocation for those CUs, this method is not considered performing the cooperative approach in which channel sensing results necessitate to be shared

among CUs to perform the agreement of selecting a licensed channel for data transmission.

The authors in (Kamruzzaman, et al., 2015) introduced an Energy efficient Cognitive Radio multichannel Medium Access Control (MAC) protocol recognised as ECRMAC. The assumption of a dedicated CCC is made in order to reserve segments for exchanging data and this is done through exchanging three handshaking frames over the control channel. These control frames recognised as ad hoc traffic indication message (ATIM) which includes both the number of the packets that needs to be transmitted and a list of use segment (LUS). The received LUS is compared with the receiver's LUS to link between both CUs. Thus, the receiver requires updating the LUS by selecting a random number of segments and making the state of this list as Tentatively Assigned that is launched with ATIM-ACK frame. Once the ATIM-ACK is received, the sender requires to update its LUS based on the received selected segments and change their status to 'occupied' which then need to be transmitted with ATIM-RES frame. Thus neighbouring CUs necessitate updating their LUS information. By doing this handshaking frames, the multichannel hidden node problem can be solved. Therefore, both sender and receiver initiate data transmission which is time slotted and two types of frames are exchanges in the reserved specific timeslot on a licensed channel.

### **2.1.2. Spectrum Access Techniques**

Spectrum access techniques play a significant role in channel utilisation in CRNs. They can be classified into two different methods to utilise a channel: Time Division Multiple Access (TDMA) which is based on time slots and CSMA/CA technique which is based on random access.

#### **2.1.2.1. TDMA technique**

The first approach is based on time slots in which a particular slot is assigned to a single user to be enable them to transmit the data. Every time slot has two different periods belonging to the listening period for CUs synchronisations and a communication period for control and data frames exchange. TDMA is a technique that is used by CUs to access the CCC for control information exchange

or over the selected data channel for data transmission. The authors of (Carlos & Kiran, 2007) (Iyer & Limt, 2011) applied the same technique in which bacon intervals have been designed for adjusting both listening period and communication period. The control frames and selected data channel and synchronisation take place during the sensing interval while the data exchange is initiated during the communication period.

#### **2.1.2.2. CSMA/CA technique**

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is considered as a random access mechanism for channel utilisation in WLANs and also in CR technology, where a set of CUs attempt to perform the wireless medium channel access based on a contention process (Chong, et al., 2009) (Liu, et al., 2010). However, this brings an issue related to the collision occurrence which is resulted from multiple CUs who attempt to use the same CCC for their control frames exchange that enable them to determine the most reliable licensed channel for data transmission. However, this issue can be solved by applying a random backoff time to seize the channel without possible collision occurrence.

This technique is employed by different researchers in CR MAC protocols (Chong, et al., 2009) (Zhang & Su, 2011) for coordinating CUs when to access the control channel and transmit to avoid any collision that may occur. Thus, a CU requires checking the availability of this control channel before launching the RTS frame, this process requires listening to the control channel for a period of time. If the control channel is busy, then CUs apply a random backoff time.

#### **2.1.3. Sensing channels**

Sensing channels is a crucial aspect in CRNs to provide significant information belonging to the channels' availability and the LUs' signals over the licensed channels. Based on the sensing technique, the decision of the most reliable channel selection can be determined. Three different techniques belong to the LUs detection over the licensed channels are used by different researchers (Lee & Akyildiz, 2008) (José, et al., 2015) (Li, et al., 2015). The first approach concerns energy detection, in which the CUs are required to sense the licensed channels for a short time, to detect LUs activity using energy detection techniques. This

approach is used widely, due to its low complexity and the lack of necessity for prior information about the LU's transmission characteristics and particular designs to detect spread spectrum signals (José, et al., 2015). For these reasons, this technique is selected for detecting signals in the proposed protocol explained in this thesis. However, the second approach is based on the matched filter detection technique, which is considered an optimal approach for detecting LUs' signals and for delivering computations at a low cost. However, the technique demands prior knowledge of LU for the CUs. The third technique is based on features detection, which has both high computational costs and provides only partial knowledge of LUs compared to others, in order to determine the LUs occupancy by investigating the associated specific features of LUs modulated signals.

#### **2.1.4. Licensed channel selection**

However, in terms of licensed channel selection, there are two different approaches described in the literature. The first is recognised as random selection of a channel in which all the licensed channels are assumed to be equally in good condition to CUs such as in (Jia, et al., 2008) (Zhang & Su, 2011). In this manner the licensed data channels are different in terms of their availability as soon as the LUs have their right and priority to utilise these channels at any time compared to CUs. However, the other approach is based on the availability of the channel predictions based on the future of the channel status. This significantly assists the CUs to make the decision of the appropriate selected licensed channel for data transmission. Therefore, the network performance would be improved especially when the throughput factor is considered to measure the successful message delivery among CUs (Wang, et al., 2011). Thus, the proposed protocol considers the best licensed channel that has the highest available time as licensed channel selection criteria between CUs.

### 2.1.5. Number of associated transceivers

The existing MAC protocols can be classified into two categories based on the number of transceivers that are assigned to each CU. For example, the authors of (Ma, et al., 2007) (Carlos & Kiran, 2007) (Su & Zhang, 2008) (Kim & Kang G. Shin, 2008) (Kamruzzaman, 2010) (Zhang & Su, 2011) (Hussein, et al., 2013) (Kamruzzaman, et al., 2015) use a single transceiver for each CU. In this case, a big challenge has risen when a CU attempts to sense and observe the activities of both the transmitted control frames over the control channel and data frame over the data channel simultaneously. This results in causing the hidden node problem since the CU is able to listen a single channel whether control or data channel at a time.

However, another category of MAC protocols (Joe & Son, 2008) (Kondareddy & Agrawal, 2008) (Salameh, et al., 2009) (Salameh, et al., 2010) (Iyer & Limt, 2011) (Qian, et al., 2013) is based on using at least two transceivers for each CU. This approach functions in improving the network throughput and performance from different sides. For example, a CU who has multiple transceivers is able to sense different channels at the same time, this leads to an increase in the network throughput by fast switching to the desired channel, and also in case if there is a necessary switching to different licensed channel due to the appearance of LU. Moreover, CUs equipped with multiple transceivers can observe and listen to the on-going packets over multiple channels including the control channel at the same time. This leads to the reduction of potential packets' collisions that resulted from the hidden node problem.

Therefore, the multiple transceivers approach is significantly important for multi-channel MAC protocol since CR is a smart and intelligent technology for improving the spectrum utilisation. It is impossible to deny the fact that less energy is consumed with a single transceiver compared to the multiple transceivers approach. However, the energy consumption is not addressed in this thesis since it is out of the scope of this research. Thus, the nature of CRNs requires effective and efficient functionalities of the spectrum utilisation and applying multiple transceivers significantly contribute in observing the on-going packets transmission in both CCC and data channels. Therefore, each CU is

equipped with a pair of transceivers in the proposed protocol for different reasons (see section 3.2.2.1 for further discussion). By considering multiple transceivers, not only the hidden node terminal issue (Kondareddy & Agrawal, 2008) in a single channel would be solved but also being an effective approach for solving the hidden node in a multi-channel environment, and increasing the spectrum efficiency. In addition, it enables the dynamic fast switching to different data channel called a backup data channel as soon as the LU appears to utilise the licensed channel. However, the backup data channel is left for the future work since it is out of the scope of this research.

Table 2-1 summarises and compares different characteristics of the discussed existing MAC protocols in literature review for decentralised CRNs.

Table 2-1: Characteristics of some existing MAC protocols

Protocols	Control Channel	Number of control frames	Spectrum Access technique	Number of Transceivers	LDCHs selection Criteria	Sensing Technique
CREAM (Zhang & Su, 2011)	Dedicated	4	802.11 (DCF)	Single	Random	Energy detection
CR-CSMA/CA (Qian, et al., 2013)	realistic CCC	3	802.11 (DCF)	Multiple	Not discussed	Energy detection
DSA-MAC (Joe & Son, 2008)	Dedicated	4	802.11 (DCF)	Multiple	Based on SINR	Energy detection
P-MAC (Hussein, et al., 2013)	None dedicated	2	802.11 (DCF)	Single	Not discussed	Energy detection
ECRMAC (Kamruzzaman, et al., 2015)	Dedicated	3	TDMA	Single	Time slotted	Assumed to be any
HC-MAC (Jia, et al., 2008)	Assumed	6	802.11 (DCF)	Single	Assumed all channels are same	Not discussed

Since the aim of this work focuses on the deployment of a secure MAC protocol for CRNs, the network overhead can be affected by the associated security information and frames for providing defense against the related malicious activities to the MAC layer. Therefore, there is a need of a MAC protocol that

efficiently provides a successful communication with respect to minimum handshaking frames that would result in fast switching to the SLDCH for data transmission. Moreover, the existence of a dedicated CCC to only CUs considers the best medium channel for providing security and significantly leads to increasing the chance of reliable, efficient, and successful secure communication among CUs (More discussion about the reason for considering a dedicated CCC is provided in section 3.2.1). Thus, despite the existing MAC protocols discussed beforehand accomplish successful utilisation of the unused white spaces by CUs, they are not considered as the best choice for deploying the security on top of them. The performance of CRN's time and throughput can be improved if the number of handshaking frames are minimised since most of these protocols such as CREAM, and CR-CSMA/CA, which are used as benchmark for different reasons discussed in section 6.2, exchange more than two control frames over the dedicated CCC. However, although two control frames are exchanged in Performance Evaluation of Cognitive Radio Network Predictive MAC (P-MAC) protocol (Hussein, et al., 2013), it uses non-dedicated CCC, which is not considered as the best channel for ensuring the reliable and successful communication among CUs since the chance of the disturbing the CUs communication can occur by LUs, who have the priority to utilise the channel. Consequently, CUs require allocating a different control channel to avoid the interference due to the LUs' activities.

## **2.2. Security Threats**

Although a CRN is similar to the traditional wireless network, it faces similar and some additional vulnerabilities that has resulted in the discarding of the communication process among end users (Leon, et al., 2010) (Fragkiadakis, et al., 2013). These vulnerabilities can lead to varied threats, which can be classified into two categories: the first relates to common security threats in both conventional wireless and CR networks, and the second category is specific to CRNs.

Figure 2-2 presents the challenges and security in CRNs while clearly highlighting the main area of this research.

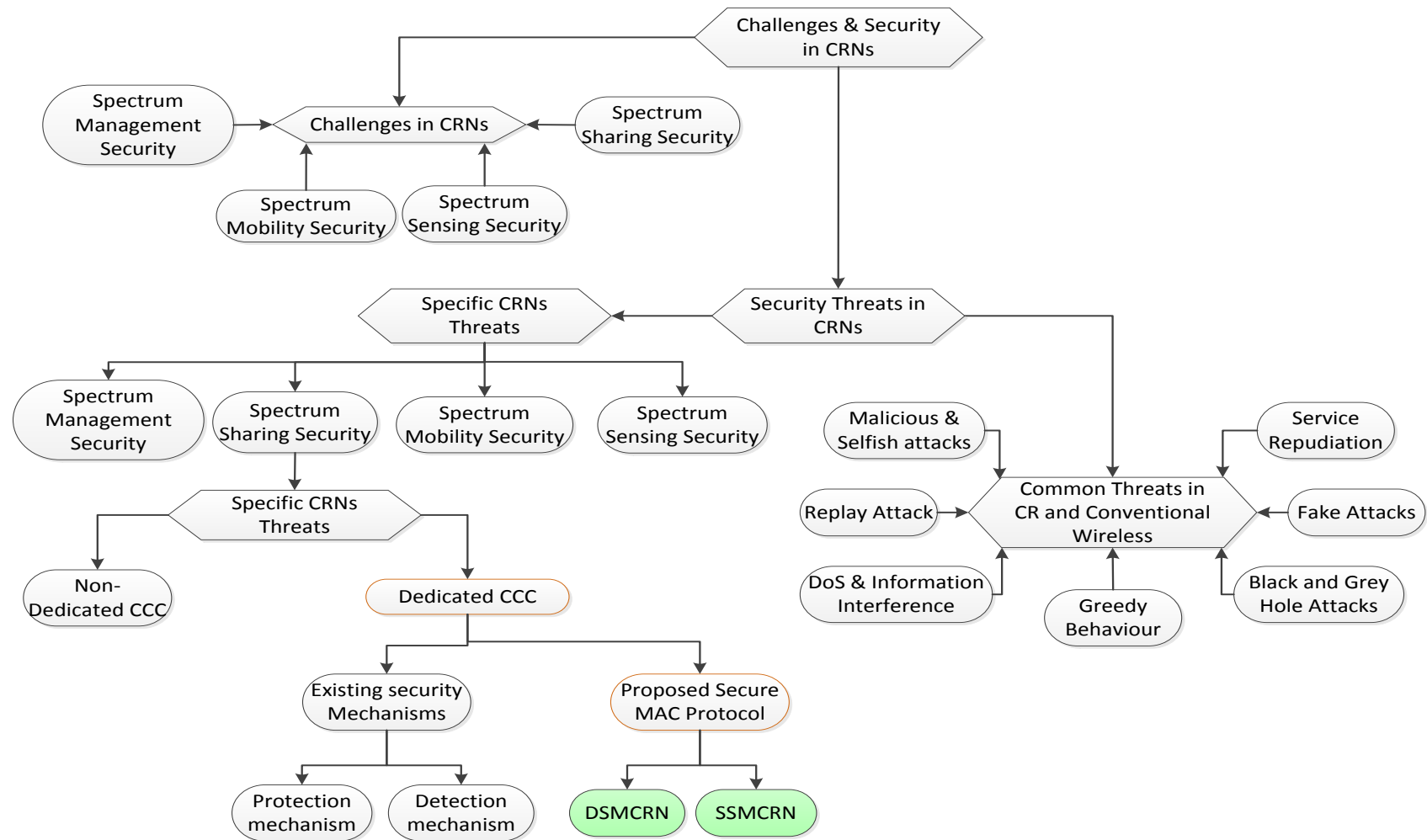


Figure 2-2: Challenges & Security in CRNs

### 2.2.1. Common security threats in conventional wireless and CR Networks

In traditional wireless technology, a radio channel is used to establish communication and transmit information between communicating nodes and AP or BS. It is also being used in cognitive networks to address several similar functionalities. The transmitted information can be sensitive such as user identity, allocation, signalling, and key information. However, an attacker using a range of techniques such as eavesdropping, forgery, and masquerading attacks can easily intercept the communication during the transmission process (Zhang & Li, 2009) (Tang & Wu, 2012). An effective security mechanism must be applied to protect data transmission from malicious behaviour like eavesdropping, and information tampering (Soleimani & Ghasemi, 2011). Therefore, as far as data protection is concerned, different security measures can be used for the protection, detection and countermeasures based on wireless security protocols such as WEP, WPA and WPA2 in conventional wireless networks and EAP, AES and 3DES in WiMAX. These security protocols are designed with various levels of encryption of different strength being used according to the importance level of the information being secured. Figure 2-3 shows the most common threats in both traditional wireless and CRNs.

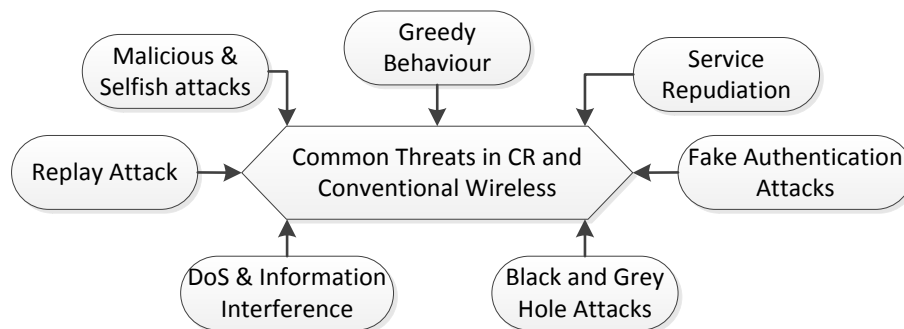


Figure 2-3: Common Security threats in conventional wireless and CRNs

#### 2.2.1.1. Fake Authentication Attacks

In the infrastructure-based wireless networks, the communication between terminals and BSs is accomplished through the wireless medium. Thus, a malicious user may exploit this opportunity to obtain the identity information belonging to the network control information, network services, and network access through tapping on the

wireless channel to pose as a legitimate user. Therefore, this grants a malicious user access to the network and to obtain a network service free of charge, or to launch an attack against the network (Sampath, et al., 2007) (Tang & Wu, 2012) (Song, et al., 2012). Therefore, cryptographic encryption schemes are generally used to protect the transmitted messages (Guo, et al., 2010).

#### **2.2.1.2. Information Tampering**

This is a serious attack that causes change, modification, replacement, or deletion of the information before it is received at its intended destination (Sampath, et al., 2007), and that result in misleading the receiver, who can thus make a wrong decision. Alteration significantly affects message integrity, which is unacceptable for legitimate users and network policies. However, this type of attack generally occurs in a situation where a cooperative terminal is needed to forward the information (Robles, et al., 2010) (Terence, 2011) (Tang & Wu, 2012).

#### **2.2.1.3. Service Repudiation**

In this attack, when the connection is achieved between two nodes, one user denies transmitting their information for two reasons: repudiation for the communication service to deny usage of the network, which requires payment for the network usage, and repudiation for the communication content to refuse the transmission of their content. For example, when transactions are made in a commercial process, the user refuses to pay. To overcome these issues, proof-of-origin evidence can be used against a particular individual for sending or receiving messages. Identity, authentication, and cryptography encryption schemas are presently used to prevent unpredictable or hidden issues arising (Rai, et al., 2010) (Tang & Wu, 2012).

#### **2.2.1.4. Replay Attack**

The key purpose of this attack at the MAC layer is to obtain effective information by intercepting and retransmitting the same signed information sent to a particular node over a period of time in order to build trust with the receiver. This gives an advantage to the attackers, granting them access to new useful information like user passwords, which then enables unauthorised access to

resources and control network licenses, etc (Goyal, et al., 2010) (Li, et al., 2011) (Enneya, et al., 2011) (Goyal, et al., 2011) (Tang & Wu, 2012) (Baayer, et al., 2012). Therefore, in order to overcome this attack, the timestamp procedure is recommended because of the message validation involved (Baayer, et al., 2012).

#### **2.2.1.5. Denial of Service and Information Interference**

While electromagnetic waves are essential in order to gain wireless information from users, recent advanced hardware technologies can involve a higher transmitted power in the communication process at the physical layer. It is, therefore, possible for an attacker to use this transmitter power to block the ordinary transmission and create interference and noise in the communication procedure, thereby decreasing the capacity of the wireless BS resources and equipment. This can also lessen user access through a BS terminal. Therefore, the interference of information procedures is likely to have a critical social impact (Jakimoski & Subbalakshmi, 2008). An example of this occurred in 2001, when the satellite communication service was interrupted due to the high power caused by locating a VSAT terminal (Jakimoski & Subbalakshmi, 2008) (Tang & Wu, 2012).

Another approach of DoS can be launched by greedy behaviour attack. For instance, during the channel negotiation process in both centralised and decentralised multi-hop networks, an attacker intends to maximise their throughput of using a spectrum through manipulating and changing the parameters of the MAC layer protocol (Zhu & Zhou, 2008) (Djahel, et al., 2009) (Attar, et al., 2012) (Zou & Yoo, 2015). This is achieved by reporting false information regarding the available channel, which causes throughput collapse for other users. For instance, in decentralised networks, if a greedy user attempts to misbehave by starving the neighbouring node, the intermediate user will be affected and banned from transmitting its messages (Tang & Wu, 2012).

#### **2.2.1.6. Malicious and Selfish behaviour attacks**

In malicious behaviour, the attacker makes other CUs to make handoff from the current channel. This generally causes degrading of the network performance (Leon, et al., 2010) (Chaczko, et al., 2010) (Soleimani & Ghasemi, 2011) (Zou

& Yoo, 2015). However, in selfish behaviour, the attacker intends to maximise their throughput and disturbing the normal process (Akkarajitsakul, et al., 2011). This happens when the selfish user collaborates in the process of the routing discovery with other users, and then avoids forwarding other users' packets and drops them. This brings an advantage to the selfish node to maximise their throughput by preserving their resources and uses the received resources belonging to other users (Soleimani & Ghasemi, 2011).

#### **2.2.1.7. Black and Grey Hole Attacks**

Both black and grey holes' attacks exist in decentralised networks and the rate of dropping the transmitted packets is used to distinguish between these two attacks. In a black hole, the malicious user intends transmitting forged routing packets and pretending to be the destination node to deceive users for starting their packets transmissions. This provides the misbehaving chance to the malicious user to launch DoS by dropping all the received packets (Abusalah, et al., 2008) (Soleimani & Ghasemi, 2011) (YI, et al., 2012). However, in the grey behaviour attack, a malicious user drops part of these transmitted packets in order to interrupt the routing discovery procedure that results in deteriorating the overall network performance (Xiaopeng & Wei, 2007) (Jiwen, et al., 2010) (Joshi, et al., 2011) (Kariya, et al., 2012) (Anon., 2012) (Jhaveri, et al., 2012) (Jhaveri, et al., 2012).

#### **2.2.2. Specific security threats in CRNs**

Generally the DSA is considered as a big challenge to implement because of:

- 1- The dynamic behaviour and nature such as different frequency, geographical location and time of operation (Datla, et al., 2009) (Li, et al., 2009).
- 2- In comparison to known security issues that exist in wireless networks, CRNs are more exposed to threats from targeted intelligent malicious strategies (Jack, 2008) (Zhang, et al., 2008) (José, et al., 2015). This poses security challenges in preventing any definite or predictable risks from occurring.

Due to the key differences in their specifications when compared to conventional wireless networks, CRNs face certain unique challenges and security issues in

terms of their continued effective use and their vulnerability to outside attacks. These particular characteristics of CRNs involve the need for additional implementation of specific functions, such as proper sensing protocols, correct decision making, appropriate switching, and the provision of sufficient access for the sharing of the resources required to operate each particular function. Several potentially serious threats to network performance have been highlighted by researchers investigating CRN technology (Zhang & Li, 2009) (Mao & Zhu, 2011) (Tang & Wu, 2012), which increase spectrum availability to malicious users. As long as the CRN is similar to a conventional wireless network in utilising a spectrum as a medium for the transmission and receiving of information, it is more exposed to security threats which are usually not faced by conventional wireless technology. Therefore, security mechanisms play an important role in maintaining the network that is potentially affected by different kinds of threats (Tang & Wu, 2012). Malicious attacks are well-known threats that target all layers in the CRNs (Zhang & Li, 2009) (Tang & Wu, 2012), with their own behaviour, which can affect network performance by attacking a particular layer. Thus the main security threats and challenges related to CRNs can be identified in Figure 2-4 below and described in more detail in the following sections:

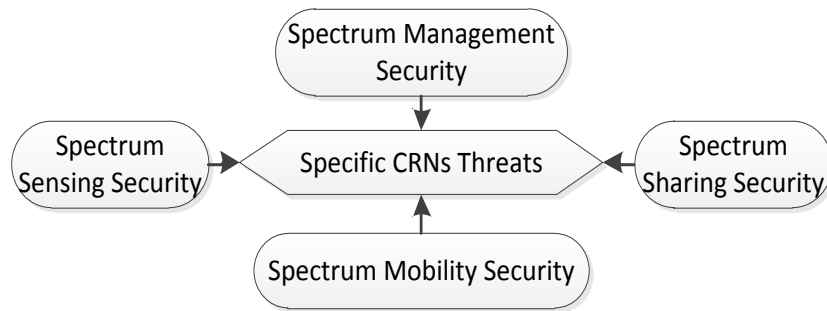


Figure 2-4: CRNs specific security threats

### 2.2.2.1. Security in spectrum sensing

Spectrum sensing is a major aspect of CRNs, providing the spectrum information about the appearance of the licensed incumbent user and the available channels (Ucek & Arslan, 2009) (Wang, 2009) (Chen, et al., 2010) (Ejaz, et al., 2011). The challenge broadly pertains to the ways in which a CU detects and differentiates between LUs and CUs. This is of great importance as attackers may

be able to emulate the signals of the LUs, thereby increasing the likelihood of false alarms being triggered. In addition, the hidden node problem may be another issue that can lead to a failure to detect the LUs, which would result in unacceptable shadow fading (Chen, et al., 2008) (Akyildiz, et al., 2008). Therefore, it is subjected to the most prevalent attack that brings the network performance down by reporting the false results of the LU detection. As long as the security in spectrum sensing is concerned with controlling the network operation, attackers have their own malicious behaviours strategies, focusing instead on degrading the network spectrum performance by causing collisions or occupying the spectrum. This can result in potential security vulnerabilities that enable DoS attacks to be launched easily (Mao & Zhu, 2011). Thus serious attacks can occur in this level of the spectrum, which are called Primary Users Interference (PUI) and Primary User Emulation (PUE).

In PUE, an attacker has a chance to focus on the physical layer to simulate a signal that resembles the signal of the LU, thereby misleading and deceiving other CUs (Chen, et al., 2008) (Anand, et al., 2008) (Ucek & Arslan, 2009) (Shin, et al., 2010) (Chaczko, et al., 2010) (Huang, et al., 2010) (Zhou, et al., 2011) (Jin, et al., 2012) (Yuan, et al., 2012) (Alahmadi, et al., 2014). This would result in increasing the availability of the spectrum to the malicious user. The authors of (Chen, et al., 2008) (Wan, et al., 2009) proposed a simulation technique used by a malicious user, which involves a multiple stage attack that demonstrates the general influence on the network performance and other special effects on the CUs. Additionally, the simulation experiment results showed how the relationship between the performance improvements can be associated with the bands' availability and vice versa.

However, in PUI, the attacker breaks the rules of the CRN mechanism by affecting network performance through interfering with LUs within the network. This forces the LU to use the spectrum with noise and unavailable frequency band (Tang & Wu, 2012). This is also called a Jamming Message attack or Lion attack where the attacker transmits high signal power to disturb the LU through TCP connection (Sampath, et al., 2007) (Zhang & Li, 2009) (Leon, et al., 2010) (Wu, et al., 2012). Several researchers have investigated and proposed algorithms to detect malicious

behaviours in cooperative sensing of the spectrum in order to improve security in this stage. A detection scheme based on a past test report obtained through calculating the suspected point of CUs, and computing the value of trust behaviour mechanism, is proposed in (Wan, et al., 2009). The algorithm is able to distinguish malicious from honest users within a network. However, (Li & Han, 2010) presented a data mining technique without needing priori information about a CU to detect misbehaviours. In addition, (Mao & Zhu, 2011) explained that changing the spectrum modulation system strategy and protecting the location information of the LU, and using proactive techniques in transmission, can help to prevent DoS attacks at this stage.

#### **2.2.2.2. Security in spectrum management**

Spectrum management is considered to be the second task after obtaining the result from spectrum sensing the decision of the appropriate available spectrum is crucial aspect to maintain the link between a pair of CUs for data transmission. This decision is mainly based on the desired characteristic of the current channel in terms of the local observation by CUs and the activity of the LU over that channel (Zhang, et al., 2008). However, the appropriate channel decision is a challenge task as soon as CRNs should be capable for supporting two different types of bands, licensed and unlicensed (Parvin, et al., 2012).

However, this stage cannot be safe from attacks. It is possible for an attacker to easily forge or tamper the transmitted information that belongs to the channels' availability, which will affect the correctness of any decisions made by the spectrum management. This is a significant issue that could arise relatively easily (Hanan, et al., 2014) (Parvin, et al., 2012) and has influence on the networks' resources in terms of identifying the channels availability to CUs and can result in launching a DoS. CUs can be deceived and will not be able to utilise the channel with its adaptive purpose (Mao & Zhu, 2011) (Tang & Wu, 2012). In this case malicious users (e.g. selfish) can maximise their throughput through the use of these channels for their data transmissions. Therefore, the inherent complexity of the protection techniques is a key requirement to provide reliable and secure transmission of information among CUs.

### **2.2.2.3. Security in spectrum mobility**

This stage refers to the mandatory process of seamlessly switching (handoff) from the current channel to another available one due to channel occupancy by the LU. With the appearance of the LU to utilise their assigned channel, a CU must vacate and select another available channel to initiate a new connection, resulting in greater energy consumption (Feng, et al., 2009) (Mao & Zhu, 2011) (Tang & Wu, 2012) (Song & Xie, 2012). This process also constitutes a significant challenge for CUs when an attacker launches a threat to hinder or prevent this integral and flawless switching by occupying the available channels. When there is a large number of malicious users the channels availability is reduced, and affect the entire network resources including other legitimate CUs, who are required to find available channels (Jakimoski & Subbalakshmi, 2008) (Song & Xie, 2012). Moreover, this kind of attack could also potentially increase the waiting time involved over a licensed channel in achieving a proper handoff and this increase is certainly unacceptable to the LUs, who have priority need to utilise their assigned channels (Parvin, et al., 2012). Also, a failed handoff to a proper channel may occur when an attacker forces CUs to vacate the channel by pretending to be the LU. As a consequence, it results in slower communication and requires additional time to resume the process of the communication (Zhang, et al., 2008) (Chen, et al., 2008) (Jin, et al., 2012).

### **2.2.2.4. Security in spectrum sharing**

The dynamic environment in a MANET network architecture leads to show more challenges and security issues due to the lack of the central entity which usually provides security and key management among users (Yu, et al., 2010). Since CRNs are self-organised and self-configured and CUs have the capability of reconfiguring the transmission specification, a great opportunity is presented to malicious users who have this flexibility to get any advantageous for launching their attacks (Attar, et al., 2012).

From a security point of view, no spectrum sharing classifications, which are discussed in section 1.3, are secure against any malicious behaviour while they are not supported with security mechanisms for protection and detection (see

Table 2-2). Generally the attackers' intention is to determinate an effective strategy that exposes a predictable risk. For instance, when CCC is used in the cooperative method of decentralised CRNs for exchanging information about the available channels and the selected channel for data transmission between SUs, the CCC is more prone to various attacks based on selfish and malicious behaviours (Leon, et al., 2010) (Fragkiadakis, et al., 2013). Because the CCC is regarded as a valuable structure for the attacker to access the channel and gain the most sensitive information, a key approach for some attackers involves applying a PUE attack. Moreover, it is more exposed to other attack types such as eavesdropping and DoS, which can be launched easily due to existing weaknesses within the MAC layer, where poor authentication and an existing lack of encryption mechanisms enable an attacker to detect available channels that they can occupy to forge or drop MAC frames (Zhu & Zhou, 2008) (Safdar & O'Neill, 2009) (Leon, et al., 2010) (Hanan, et al., 2014), as shown in Figure 2.5.

Another vulnerability in a CCC is where an attacker forges the transmitted packets to another path and causes collisions. As a consequence, this impedes the network performance and launches a DoS attack. Once a CCC is saturated by attackers, a large number of forged packets are generated to block the exchange of the control information, enabling DoS attacks to be easily launched against the network, hence affecting its performance (Hanan, et al., 2014). Moreover, the author of (Zhu & Zhou, 2008) suggests that encryption must be applied between legitimate SUs for the exchange of control information; otherwise, it can be readable by attackers of other CUs. Also, it can protect the exchanged control information over the channel from predictable control channel hopping sequences, thereby preventing itself from being saturated (Bian & Park, 2006) (Tang & Wu, 2012).

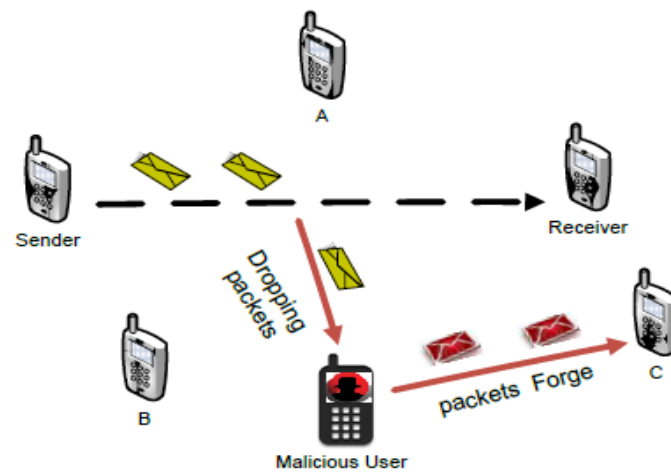


Figure 2-5: Malicious activities in decentralised CRNs

Therefore, Table 2-2 summaries the potential attacks that can be launched by adversary users in CRNs.

Table 2-2: Overview of the attacks occurring at different CR functions

Attack Name	CR function	Description
Forgery & Data tamper	Spectrum Sensing	Spectrum Management system makes wrong decision by receiving the attackers' sensing information
Overlapping		An attacker impacts other networks by transmission to a specific network
Denial of Service		An adversary user decreases the availability of the spectrum bandwidth by blocking the communication, through creating noise spectrum signals which cause interference with PUs
Lion or Jamming Message		An attacker transmits high signalling power to disturb the PU or the CU which results forcing the CU to hop to different channel to utilise
Spectrum Sensing Data Falsification		In collaborative spectrum sensing, a collaboration technique used among CR nodes to generate and utilise a common spectrum allocation for the exchange of information about available channels. However, an adversary node gives false observations information to other users.
Eavesdropping	Spectrum Sharing	Weaknesses within the layer due to the poor authentication and no existing encryption mechanisms
Denial of Service & masquerade		Repetition of the frequent packets that result in overcrowding the channel which is being busy to be utilised by legitimated users
Selfish behaviour or selfish masquerade attack		An attacker does not follow the normal communication process for maximising their throughput, saving energy or gaining unfair beneficial access of using spectrums through injecting frequent anomalous behaviour
Key depletion		An attacker attempts to break the cipher by repetition of the session key
Forgery attack		Lack of authentication mechanism leads to the occurrence of modification and forgery on MAC CR Frames which result in the launch of DoS attacks
Biased utility	Spectrum Management	An attacker tries to reduce the bandwidth of other SUs in order to obtain more bandwidth by changing the spectrum parameters
False feedback		An attacker secretes the incidence of the PU in order to disturb the information sensing of other SUs

### 2.3. Secure Communication Scheme in CRNs

Since each layer within CRNs has its own characteristics and parameters (Ci & Sonnenberg, 2007) (Wan, et al., 2009), they are vulnerable and allow an

attacker to make a decision to launch a specific attack for the purpose of deteriorating the whole network performance. In MAC layer frames, an adversary has a variety of aims to misbehave and launch such an attack. For instance, a denial of the channel service is one of the serious threats that lead to the network degradation between both sender and receiver. This attack happens when the attacker saturates the control channel until it becomes weak for attacking (Baldini, et al., 2012). In addition, selfish behaviour is another example of attack that can also exist in MAC layer in which an attacker does not follow the normal process of communication. Therefore, in order to provide defence against these threats, security mechanisms are required in MAC layer to provide authentication, authorisation and availability (AAA) in CRNs. Thus, incorporating these security features can lead to the exchange of complete and reliable secure MAC frames among CUs (Prasad, 2008) (Zhang & Li, 2009) (Tang & Wu, 2012). Several studies have been conducted for secure communication in CRNs (Mathur & Subbalakshm, 2007) (Prasad, 2008) (Sanyal, et al., 2009) (Parvin, et al., 2010) (Zhu & Mao, 2010) (Sorrells, et al., 2011) (Zhu & Mao, 2011) (Huayi & Baohua, 2011) (Parvin & Hussain, 2011) (Zhu & Mao, 2011) (Parvin & Hussain, 2012). They are classified into two categories based on protection and detection techniques for addressing the security requirements and to define the existing security issues in MAC protocols in CRNs.

### **2.3.1. Protection mechanisms in CRNs**

In general, the authors of (Mathur & Subbalakshm, 2007) (Prasad, 2008) (Sanyal, et al., 2009) (Zhu & Mao, 2010) (Parvin, et al., 2010) (Parvin & Hussain, 2011) (Zhu & Mao, 2011) (Parvin & Hussain, 2012) aim to provide a secure communications among CUs by applying different security mechanisms, such as authentication and authorisation access by different techniques within a CRN. Their proposed procedures include digital signatures, certification authority, trust based and third party entities like BSs. Although, these solutions attempt to be effective in some ways, they fail in demonstrating any results and focus only on providing a theoretical approach with poor clarity in their work for the full

entire operation. Their discussions have significant limitations in terms of lacking of security aspects belonging to the security requirements and their failure to evaluate the approaches. While in (Mathur & Subbalakshm, 2007) (Sanyal, et al., 2009) (Parvin & Hussain, 2011) efforts have been done in order to perform the authentication within CRNs. However, their operation approaches were all limited to infrastructure CRNs.

#### **2.3.1.1. Digital signature and certificate authority**

A technique based on applying digital signatures in order to obtain a secure communication and protect the network from DoS attacks is proposed in (Sanyal, et al., 2009) (Parvin & Hussain, 2011). Their approaches involve the activities of a CA, PUs, and both PUs' and LUs' BSs. However, the main differences of these mechanisms are that the BSs are connected to the CA using wire links in (Mathur & Subbalakshm, 2007), while in (Sanyal, et al., 2009) the approach used was to have an asymmetric key scheme applied instead of BSs.

#### **2.3.1.2. EAP-SIM**

Another approach of authentication mechanism is presented in (Zhu & Mao, 2011). However, the presented scheme requires a BS which is connected to a CA and uses both EAP-TLS for establishing a secure connection and EAP-SIM for authenticating the user.

#### **2.3.1.3. Trust values procedures**

Other techniques based on trust values are proposed in (Parvin, et al., 2010) (Parvin & Hussain, 2012) to address and analyse the issues within CRNs. The trust value calculated to lead to the decision that will either allow the current user to utilise the available licensed channel or not.

#### **2.3.1.4. Other framework architectures**

Security for authentication and authorisation architecture frameworks have been proposed in (Prasad, 2008) (Zhu & Mao, 2011). Both techniques require third-party entities for appropriate access policies to the spectrum. The authors of (Prasad, 2008) use a technique based on processing user identification in the

system and providing the user preferences to third parties according to privacy rules. Based on this, the user is authenticated and then determined whether or not a data port would be used. However, the subsequent architecture in (Zhu & Mao, 2011) consists of two layers, which are up-layers for authentication purposes and encryption techniques, while the physical layer is for securing and protecting the spectrum.

Overall, while these proposed mechanisms are effective in some ways in protecting the networks from forgery and DoS attacks, they are not applicable in a decentralised environment because a BS is needed and incorporated for verifying the identity and providing secure communication. Moreover, the work focusses theoretically on discussing the security challenges and needs in CRNs and failed to produce results and poor clarity in their proposed framework operation.

Another security framework is proposed in (Safdar & O'Neill, 2009) for providing security in the MAC layer of decentralised CRNs. However, the framework has significant limitations related to security mechanisms and simulation parts and discussed as follows:

- The work is introduced theoretically and lacked both necessary information such as the frames sizes and sensing techniques which require different time over the CCC and lead to subsequent effect on the throughput rate, and demonstrated results for validating their approaches.
- There is lack of clarity in achieving the authentication mechanism without identifying and highlighting the authentication process, and for the reasons for having a trusted terminal to provide the secret information to validate CUs. The authors do not consider the process of how the authentication takes place and registering CUs for receiving the secret information that belongs to validation of those CUs. Instead they only stated that the authentication must take place between both senders and receivers over the CCC. This is a most critical point that needs to be evidently addressed in decentralised CRNs, since there are different verification schemes that can be used such as digital signatures, IDs, and shared keys. These schemes have different operation requirements for the need of registering CUs and the relevant number of the security frames that are required to be

exchanged for the demand of completing the registration process and the secret information exchange. This subsequently affects the entire network's operation and performance.

- Each pair of CUs necessitates exchanging three control frames over the CCC and they recognise as Free Channel List (FCL) frame, Channel Selection (CH-SEL) frame, and Channel Reservation (CH-RES) frame. However, the number of control frames can be reduced for the aim of improving the network's efficiency and performance related to the communication time and throughput. This reduction is also essential for reserving the CCC for less time and subsequently allowing CUs to perform fast switching to the selected data channel and making the current CCC available for the next pair of CUs.
- After selecting a licensed data channel, the sender sends CH-RES frame to its neighbouring for channel reservation. However, this will lead to increasing the potential threat targeting the announced data channel by the internal malicious users for launching a DoS attack through creating interference to disturb the communication. Therefore, making the selected data channel hidden from other CUs is essential for increasing the chance of exchanging data successfully between CUs, without occurring interference made by internal and external adversary users.
- Moreover, CUs are required to exchange their public keys to secure all the communications including the exchanging of the available channel list, selected data channel, and the actual data. However, this is not considered as an efficient approach since it leads to increasing the communication time and reserving the CCC for a longer time by two ways; the number of the transmitted frames for the purpose of public key exchange, and the execution security time of asymmetric key to encrypt and decrypt the secure control information and the transmitted data. Consequently, the network performance will be affected and especially in the situation where a large number of CUs need to access the control channel for establishing their communication. Moreover, the licensed data channel's availability can also be affected by slowing the switching time from the CCC to the

data channels. Therefore, this approach causes the decrease in the network throughput due to the long communication time over the CCC and subsequent lowering of the throughput. Thus, the proposed security protocols intended to avoid the use of asymmetric key by replacing it with a symmetric key algorithm to secure the control and data communication between CUs over the CCC and data channels for the purpose of improving the network performance. This point has been proved in the proposed protocols in sections 4.3.1 and 4.3.2, in which the RSA and AES algorithms are used to encrypt a single frame, is transmitted to the dedicated server for authenticating CUs in DSMCRN and SSMCRN respectively. Thus, it has been found that the execution time of the asymmetric key algorithm necessitates significant time leading to reserving the control channel for longer time. Therefore, the avoidance of asymmetric key algorithm is highly recommended and considered in the proposed protocols for securing both sensing results and data exchange among CUs over both CCC and selected licensed data channels.

Therefore, the security and challenges in decentralised CRNs still arise and require defensive techniques for securing communication among CUs. Table 2-3 demonstrates the pros and cons of the proposed protection mechanisms.

Table 2-3: Protection mechanisms in CRNs

Proposed Mechanism	pros/cons	Description
User identification	Pros	Low complexity by generating two virtual ports for secure transmission: the first is for control traffic information and another is for data transmission which is blocked by default unless the user has been authenticated.
	Cons	It requires a third party to provide information like user preferences
Digital signature & certificate authority	Pros	Low complexity and using the basic architectures of symmetric and asymmetric key infrastructures.
	Cons	It has not been simulated and tested to proof the security. It also does not work in Ad-hoc environment due to being based on centralised entities.
Certificate authority	Pros	Effective security mechanism due to identifying and verifying the user and the server respectively.
	Cons	Requires a third-party to verify the user identity. Also the mechanism has not been simulated and tested to ensure security against malicious behaviours.
Trust values	Pros	It is an additional procedure that can be built on the top of other security techniques to increase the level of the protection and detection in term of secure communication.
	Cons	Requires a third party procedure is to provide previous information of a node. Moreover, when a new node joins the network, the CA will not be able to provide reference for that particular user. Hence the mechanism does not operate in strong fixed level of the authentication for all CUs equally.

### 2.3.2. Detection schemes in CRNs

The authors of (Rakhshanda, et al., 2008) (Huayi & Baohua, 2011) (Zou & Yoo, 2015) have focused on the detection mechanisms in CRNs. Their proposed techniques address a variety of attacks caused by malicious and selfish behaviours, and the pros and cons of these mechanisms are illustrated in Table 2-4.

#### 2.3.2.1. Selfish behaviours

Selfish behaviour detection techniques for the CCC are proposed in (Huayi & Baohua, 2011) (Minho, et al., 2013), where a puzzle punishment model (Huayi & Baohua, 2011) is applied for bad behaviour activities in a situation

where a receiver is asked for a new hidden channel that has not been included previously. Thus, the sender would be a suspicious case. Therefore, the receiver applies the puzzle punishment to detect whether the sender is a selfish node or not. If the sender node solves the puzzle, they will be considered as a legitimate user and communication will be resumed normally; otherwise, the communication will be disconnected. Another technique called Cooperative neighbouring cognitive radio Nodes (COOPON) (Minho, et al., 2013) is applied among a group of neighbouring users to detect selfish nodes who broadcast fake channel lists. Consequently, neighbouring users can detect the selfish users by comparing the transmitted channel list of the target user with their lists. In addition, a similar mechanism called cooperative attack detection scheme (CADC) is proposed in (Zou & Yoo, 2015) in which CUs transmit their FCLs over the CCC to determine the final status of the availability of these channels. Thus, the scheme detects both greedy attackers, who transmit a part of authentic available channels and hide the other part for occupying them selfishly and malicious attackers, who transmit lists of occupied channels by LUs to deteriorate the network's performance.

#### **2.3.2.2. Timing parameter**

Another detection mechanism was proposed in (Rakhshanda, et al., 2008). They presented a mechanism that relies on timing parameters at MAC layer. When the negotiation phase is taking place, the node, which receives a request, sets up timing parameters for controlling the time interval. This forces the sender to transmit data without getting a higher rate. If the sender does not obey and sends packets more frequently, the receiver node takes action against the sender. Then the receiver node analyses the sender's misbehaviour and broadcasts the information over the current network.

#### **2.3.2.3. Anomalous Spectrum Usage Attacks (ASUAs)**

The authors of (Sorrells, et al., 2011) presented a cross-layer technique for CRNs for detecting ASUAs. Collecting the information on both the physical and network layers provides an awareness of the current spectrum. It operates against the PUE and jamming attacks to provide successful access to the

spectrum. Table 2-4 shows the advantages and drawbacks of the existing detection mechanisms in CRNs.

Table 2-4: Detection mechanisms in CRNs

Proposed Mechanism	pros/cons	Description
Selfish activity	Pros	Applied in both CCC and data channel which decreases the potential of misbehaviour in different stages of the network
	Cons	Focuses only on detecting selfish behaviour and does not provide the complete secure communication between sender and receiver
timing parameter	Pros	Detecting misbehaving nodes during the negotiation phase. It helps to maintain the channel from getting saturated.
	Cons	Theoretical and has not been simulated and tested to provide the detection scheme results. Weak against eavesdropping and forgery attacks especially once the FCL is not hidden which is exploited to launch Jamming attacks.
Anomalous Spectrum Usage Attacks	Pros	Combining both physical and network layers for detecting malicious users give a better achievement instead of selecting only a layer
	Cons	Focuses only on the detection approach and does not consider a significant protection scheme against both jamming and PUE attacks mobility.

### 2.3.3. Comparisons of the presented schemes against MAC layer attacks

Incorporating the security requirements; authentication, confidentiality, non-repudiation, and data integrity in CRNs can lead to the exchange of complete and reliable secure MAC frames among CUs (Bian & Park, 2006) (Zhang & Li, 2009) (Tang & Wu, 2012). The proposed digital signature, trust value and, CA procedures are different in terms of their operations (see the protection schemes in section 2.3.1), the security requirements are considered to provide the necessary defence against most of the MAC threats such as DoS, Forgery, eavesdropping and replay attack in centralised CRNs. However, the presented schemes require licenced and CU's BSs that are connected through a wired link to the CA.

In contrast, both puzzle punishment and COOPON approaches consider only the selfish behaviour among the other MAC attacks such as DoS, forgery, eavesdropping, and spoofing in decentralised CRNs. However, they are

effective in selfish behaviour detection due to the cooperation between a group of CUs which involve identifying selfish users in the COOPON technique and demand of solving the puzzle to resume the communication in puzzle punishment system. Moreover, the timing parameter procedure easily addresses DoS attack due to the presence of the centralised entity that controls the CUs' communication. In addition, the cooperative attack detection scheme (CADC) focusses on detecting only greedy attackers who hide a part of authenticated licensed channels for occupying them selfishly, and malicious attackers who intend to deteriorate the network performance by sending a list of occupied channels by LUs.

Despite these published research, which have been discussed in details in sections 2.3.1 and 2.3.2 attempt to provide solution for either protection or detection schemes in CRNs, none of them specifically introduced a clear vision of providing a complete secure MAC protocol for the cooperative approach of decentralised CRNs and incorporating most of the security requirements namely; authentication, confidentiality, non-repudiation, and data integrity in CRNs with full simulation and validation of the work such as in (Rakhshanda, et al., 2008) (Sanyal, et al., 2009) (Parvin & Hussain, 2011). Instead they just introduce theoretical approaches that are not possible to be validated without simulation and testing or using formal logic method techniques such as BAN, GNY, etc.

## **2.4. Summary**

Security is a crucial aspect needed in CRNs in order to achieve successful communication between sender and receiver CUs. Due to some unique characteristics in CRNs, different new threats exist to attack CR functions such as PUE and PUI in spectrum sensing, Tampering attack in spectrum management, failed handoff in spectrum mobility and MAC threats like eavesdropping, forgery and selfish behaviour attacks in spectrum sharing. A major portion of the chapter has been dedicated to this part for being the main motivation behind this overview work. It introduced details of challenges and security mechanisms in spectrum sharing that is based upon two criteria; a Dedicated Local Control Channel also

known as Common Control Channel (CCC), and a Non-Dedicated CCC. However, only the CCC is chosen to investigate and highlight the potential existing threats and vulnerabilities. It is found that several sorts of attacks such as eavesdropping, selfish behaviour, forgery, DoS and masquerade is exposed to multi-hop CR environment. In addition, this chapter included several prevention techniques and countermeasures that are proposed by other researchers to solve the existing issues with secure communication mechanism in CRNs. They focus on protection and detection procedures in CRNs layers. Therefore, the advantages and disadvantages of the proposed methods have pointed and summarised.

## **Chapter 3 DESIGN OF THE PROPOSED MAC PROTOCOLS WITH AND WITHOUT SECURITY**

This chapter focuses on two main sections that introduce the design of MAC protocols for CRNs with and without security. The first part presents the design of a novel MAC protocol for decentralised CRNs abbreviated as MCRN. It clearly identifies the method of exchange of the control information among CUs over a dedicated control channel. Moreover, it provides the details of the main features of the MCRN protocol such as the number of the transceivers that are associated with each CU to observe the ongoing activities over both the CCC and data channel which is selected and agreed upon on the basis of the channel selection technique. The Second part considers exclusively the design of two different security protocols based on, Digital-Signature, and Shared-Key. These two are extended protocols based on MCRN for achieving the security requirements within the network. Thus, both the Digital-Signature based Secure MAC protocol for CRN (DSMCRN), and the Shared-Key based Secure MAC protocol for CRN (SSMCRN) are discussed in details through applying appropriate and robust framework architectures and the frames' transmission for achieving the security and communication in ad hoc CR environments. Moreover, the analysis of the frames' transmissions among the contributed entities are described in the format of the formal BAN logic, which mainly leads to achieve the contribution of deploying and implementing the protocols through considering the security features defined and analysed within messages' exchange in the DSMCRN and SSMCRN protocols.

### **3.1. Assumptions**

The following assumptions are adopted in the proposed protocols. Therefore, the assumptions from (1-4) are applicable for all proposed protocols with and without security while the rest (5-8) are applicable only to the security protocols DSMCRN and SSMCRN since they are related to security aspects.

- 1) CUs obey the MAC layer protocol and do not interfere with the licensed users activities over the licensed data channels.

- 2) CUs require sensing the licensed data channel before exchanging their control information to detect LUs activities using an energy detection technique.
- 3) The common control channel is assumed to be dedicated, reliable, and permanently available for the contributing CUs.
- 4) Each CU is equipped with a pair of transceivers in the proposed protocols.
- 5) A dedicated server is engaged for the authentication purpose and providing the security key management to end users through registering CUs for controlling the entire network.
- 6) In the unauthorised access scenario, it has been assumed that a malicious user usually communicates with a valid CU, and this research do not consider the situation of two malicious users communicating with one another.
- 7) The dedicated server controls the network access information which namely the shared-keys and CUs' IDs for only the registered CUs.
- 8) CUs initiate exchanging the sensing results that belong to the licensed channels availability, selected data channel, and the transmitted data only after the server has validated both sender and receiver and provided the shared-key for control and data frames exchange after the successful authentication.

### **3.2. A MAC protocol for CRNs (MCRN)**

This section highlights the details of the proposed MCRN protocols in terms of its design and operation. The MCRN protocol permits the efficient utilisation of unused part of the licensed channels through considering the sequences of the different processes:

- Channel sensing to record the channels status; available or occupied by the licensed users, who have the priority to utilise these licensed channels.
- Determine and share only the available channels to select the highest available data channel for data exchange between a pair of CUs.
- Switching to the selected data channel and initiating data transmission.
- Vacating these channels in the case if the LUs activities are detected.

Therefore, the details of proposed MCRN are provided in the following sections.

### **3.2.1. Dedicated CCC for MCRN**

The need for a dedicated common control channel is essential in a cooperative approach of CRNs. Since it plays a major role and provides several advantages to CUs to guarantee the success of exchanging the control frames related to the spectrum sensing, sharing, management, and mobility. It also facilitates to provide coordination and cooperation among CUs to proceed the process of sharing the spectrum sensing results and making the decision of selecting a licensed channel for data exchange between both senders and receivers (Jia, et al., 2008) (Domenico, et al., 2012). Moreover, although, the CCC is simple in its design (Zhang, et al., 2014), it easily overcomes the issues related to the allocation, establish the link between CUs and monitoring of a secure communication (Gavrilovska, et al., 2014).

Since CUs initiate their communication process in the negotiation phase and require time over the control channel to exchange a number of control frames before initiating the data exchange. This time does not affect the LUs by occurring any interference while the control channel is dedicated to only CUs. As a result, there is no restriction in terms of the channel reserving time for those CUs and this will ensure the reliable communication between CUs. However, this time is not easy to be managed between CUs and LUs if the control channel is not dedicated and selected from the available licensed channels, because it is not possible to guarantee the successful communication between CUs due to the possible appearance of LUs, who has the priority of utilise the channel, at any time. Consequently, CUs necessitate vacating the channel which then leads to the failure of negotiation phase, which will be repeated and would result in affecting the network performance and throughput. This issue becomes more critical when security aspects are considered and require additional time that would lead to increase the chance of the interference with LUs. This issue is significantly taken into consideration, since the main aim of this research is to develop a secure MAC protocol rather than focusing on a network protocol, the security execution time

considerably affects the CUs' communication time and this has been proven and detailed in chapters 5 and 6.

Therefore, the dedicated control channel will contribute to overcome this issue by providing additional advantages and is considered as an efficient approach for addressing the security requirements (e.g. Authentication, confidentiality, integrity, secure communication and etc.) in decentralised CRNs. Since additional security frames and more time needed for the execution of different security algorithms are required, this leads to an increase of the time taken over the control channel. Thus, considering a dedicated control channel and avoiding a non-dedicated control channel will ensure the reliable and secure communication among CUs especially when the security execution time is not fixed among discrepant devices have different capability.

Therefore, the assumption of the dedicated CCC is made in the proposed protocol as according to the US Federal Communication Commission (FCC), most licensed bands are not utilised efficiently (Sood & Singh, 2011) (Bhattacharjee, et al., 2011) (Kanth, et al., 2013). It is calculated that 70% to 94% of these bands are unused, thus indicating that the greater part of the database of the whole spectrum is available to utilise. This fact has encouraged researchers such as (Joe & Son, 2008), (Zhang & Su, 2011) and also the author of this thesis to validate the assumption that dedicated CCC can be used for the proposed protocol. Therefore, the proposed protocol will be using a dedicated CCC to exchange control information. The characteristics of the CCC motivates all users to utilise the band as it provides a guarantee of reliable control information exchange for wireless communications systems and permits broadcasting and network synchronisation (Jha, et al., 2011) (Domenico, et al., 2012).

### **3.2.2. MCRN features**

The proposed MCRN protocol employs different features that lead to efficient utilisation of the unused spectrum. These include the number of radios in each CU, CCC access technique, spectrum sensing, and licensed data channel selection criteria. These features were highlighted in Figure 2-1 and are explained below:

### **3.2.2.1. Multiple transceivers in MCRN**

As discussed in section 2.1.5, there is a number of MAC protocols (Joe & Son, 2008) (Kondareddy & Agrawal, 2008) (Salameh, et al., 2009) (Salameh, et al., 2010) (Iyer & Limt, 2011) (Qian, et al., 2013) (Timalsina, et al., 2013) that considered multiple transceivers due to the effective functionalities related to improving the efficiency of spectrum utilisation and the network performance by tuning and accessing discrepant channels simultaneously. Therefore, it is assumed that each CU is equipped with a pair of transceivers in the proposed MCRN since it uses two different channels (control and data). A single transceiver is used over the CCC to transmit and receive the control frames while the second transceiver is used to sense the licensed data channel during the exchange of the control information and to enable the receiving and transmission of data and ACK frames over the selected data channel. This approach is being considered in this work because of the hidden node problem, which is a challenge that needs solving in distributed CRNs, since multiple channels can be available for utilisation by CUs. The multi-channel hidden node problem increases with the availability of these channels. These issues have been investigated by different researchers (Carlos & Kiran, 2007) (Liang Shan, 2009) (Zhang & Su, 2011) (Reddy, 2012) (Venkateswaran, et al., 2012) who found that they tend to come up when a CU needs to send a packet while the receiver is receiving different packets from a different sender. This causes collisions among the transmitted packets and results in a deterioration of the network performance.

It cannot be denied that single transceiver offers an effective and less energy intensive solution than multiple transceivers. However, the nature of CRNs requires effective functionalities to observe the on-going packet transmission in both control and data channels. Multiple transceivers not only solve the hidden node terminal issue in a single environment but also provide an effective approach to solving the hidden node issue in a multi-channel environment thus increasing the spectrum efficiency. This approach is expected to be considered in future studies because it enables dynamic and fast switching, that is, CUs can dynamically switch to different data channels (backup data channels) as soon as the LU appears to be utilising the licensed channel. This approach is also

considered in the design of the CTS frame in the MCRN protocol. However, it will not be implemented as part of this study, since it does not fall within the scope of this research.

### **3.2.2.2. Sensing channels and licensed channel selection in MCRN**

The assumption of energy detection technique for spectrum sensing that was discussed in section 2.1.3 is used in the proposed MCRN protocol. It is selected among the others, since it is used widely to detect signals and has low computational and implementation complexities, because of the lack of a need for the prior LUs' information over licensed channels and particular designs to detect spread spectrum signals (Li, et al., 2015). Thus, the adopted sensing technique is an energy detection technique that meets the demands and is the most appropriate for the proposed protocol, since it enables CUs to sense LU's activities over the licensed data channels before exchanging their control information within a short time. This is necessary to determine the channels' availability before adding it to the FCLs.

In terms of the Selected Licensed Data Channel (SLDCH) criteria, the proposed protocol considers the most appropriate and reliable licensed data channel for a pair of CUs to launch their data frames. It is entirely based on the channel that has the highest available time. This is important in CRNs to avoid any potential interference with the LUs over the SLDCHs and to increase the network throughput.

### **3.2.3. MCRN architecture**

The proposed MCRN is designed to accommodate decentralised CRNs where a set of CUs attempts to exchange their control information and data. This is a challenge in ad hoc networks because of the lack of an existing centralised entity that acts as a Base Station or Access Point to provide the control information to the CUs.

Figure 3-1 depicts the network scenario, in which a dedicated CCC is allocated only to CUs and used to exchange control information belonging to the available data channels (FCL) and the most reliable selected data channel (SLDCH), to exchange data between a pair of CUs within the same range. This process is shown in Step 1 of the same figure, in which a contention based technique is performed by CUs for accessing and reserving the CCC to exchange the FCL and SLDCH. Thus, two CUs exchange the control information while the third CU requires that the waiting CCC be vacated by the first group of CUs and switched to the selected data channel. Based on the data channels scan results, CUs can identify available channels not occupied by LUs. This stage must be completed before the exchange of the control information, which is shown Step 1. Although, both CUs can switch to any of the data channels included in FCL, and shared between the sender and receiver, such as data channels 2 and 3 in same figure, they only select a single data channel, which meets the applied data selection criteria requirement based on the highest channel availability. Once the SLDCH is determined and exchanged between both the sender and receiver, both CUs switch to the chosen channel and initiate the data transmission. However, data channel 1 is not included in the FCL, since the LU occupies it.

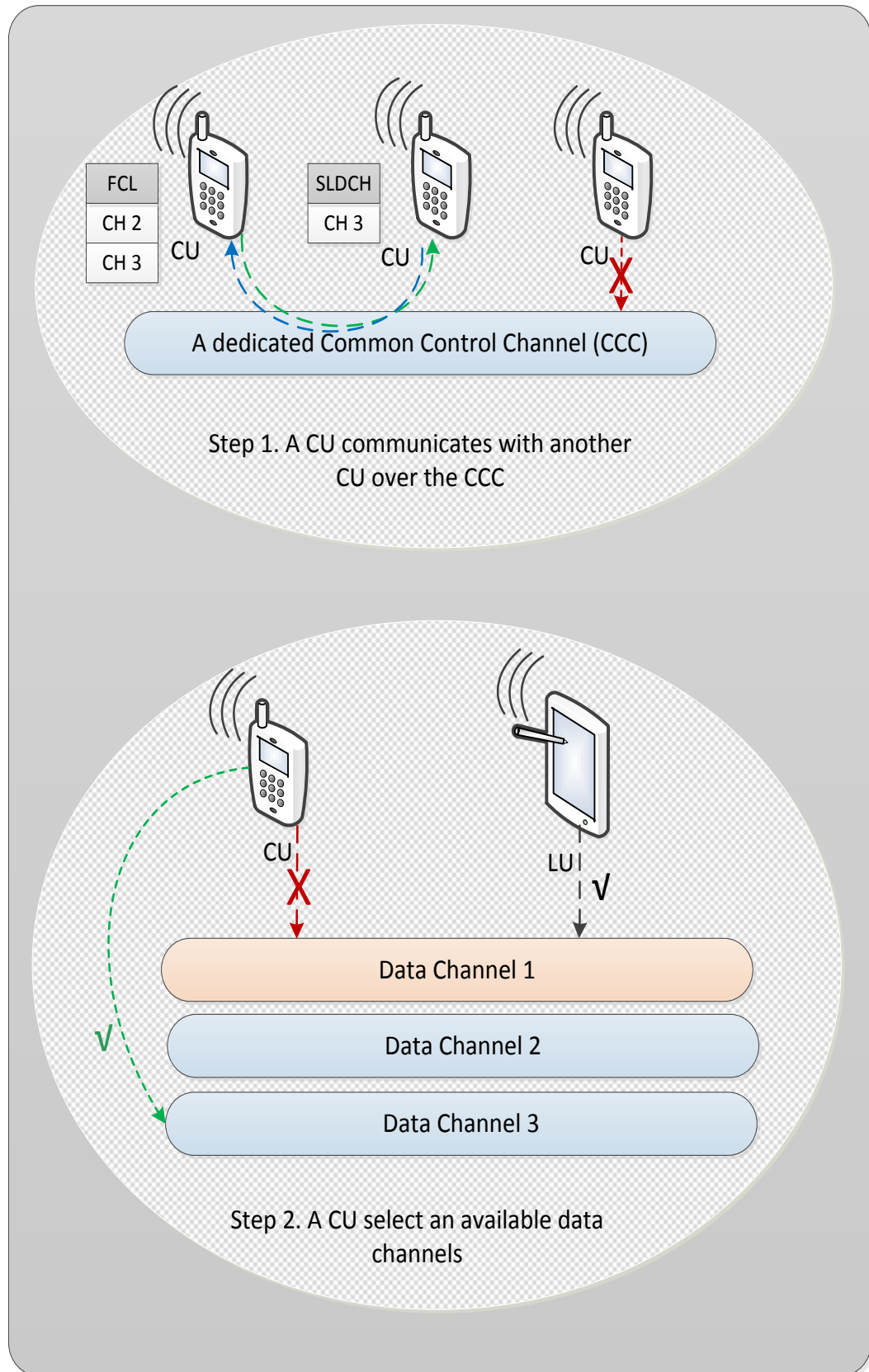


Figure 3-1: MCRN network scenario

### 3.2.4. Header fields in MCRN frames

Usually a frame's format in data communication and networking comprises constant management parameters (fields) such as; Header, Destination MAC address, Source MAC address, FCS, and other fields according to the frame's usage as shown in Figure 3-2. However, the frames sizes are different in this protocol and chosen according to their needs since there is no published standard for CRN frames' sizes but some fields like Destination MAC address, Source MAC address, and FCS remain similar to the IEEE 802.11 standard.

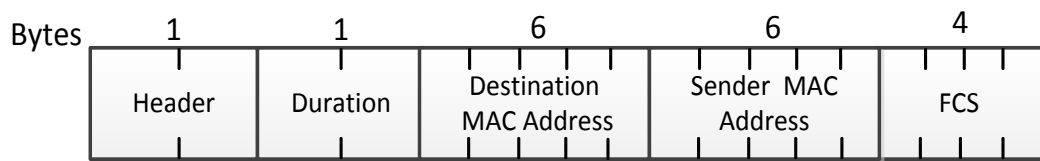


Figure 3-2: Frame structure

Therefore, the Header's 8 bits are allocated to determine several aspects belonging to the management procedure to indicate the following functions:

- **Protocol type** consists of 2 binary bits. It gives the details of the sender's protocol version e.g. IPv4 or IPv6.
- **Frame type** consists of 2 bits, the first specifies whether control or data frames while the second identifies the sub type of the frames. They are set as follows:
  - 0 0 in RTS frame of the control phase
  - 0 1 in CTS frame of the control phase
  - 1 0 in a data frame of the data phase
  - 1 1 in ACK frame of the data phase
- **Power management** bit specifies the status of sender power management after completing the exchange of the current frame.
- **Protected** bit specifies the encryption state of the information included within a frame. It is always set to 0 in the MCRN protocol since it does not consider the security and encryption techniques.
- **Retry** bit indicates the retransmission control or data frames.

- **Fragmentation** bit is usually associated with the frame type where it is set to 0 if the transmitted frame is a control frame, and 0 or 1 if it is a data frame. If the message needs to be fragmented it is set to 1, otherwise it remains 0.
- **Duration:** this field is based on 8 bits used to set the NAV value. When both the sender and receiver CUs are exchanging their frames, neighbouring CUs require suspending their communication for a period of time called NAV.
- **Destination MAC Address:** 6 bytes are allocated for the destination MAC address of the receiver.
- **Source MAC Address:** 6 bytes are allocated for the source MAC address of the sender.
- **Frame Check Sequence:** this field is based upon 4 bytes for the Cyclic Redundancy Check (CRC) process to identify the validity of the transmitted frame by checking their integrity.

### 3.2.5. MCRN Phases

The proposed protocol consists of two different stages using different channels; the first stage is called the *Control* phase which is designed for the exchange of a pair of control frames between two different CUs. These frames are known as RTS and CTS and facilitate the exchange of control information to determine the criteria of selecting an appropriate data channel for initiating the data transmission. The second stage is called the *Data transmission* phase, which is based upon multiple licensed channels that are sensed and determined in the previous control phase and are then used by CUs to launch their data and ACK frames. The frames' sequence in the MCRN protocol is shown in Figure 3-3.

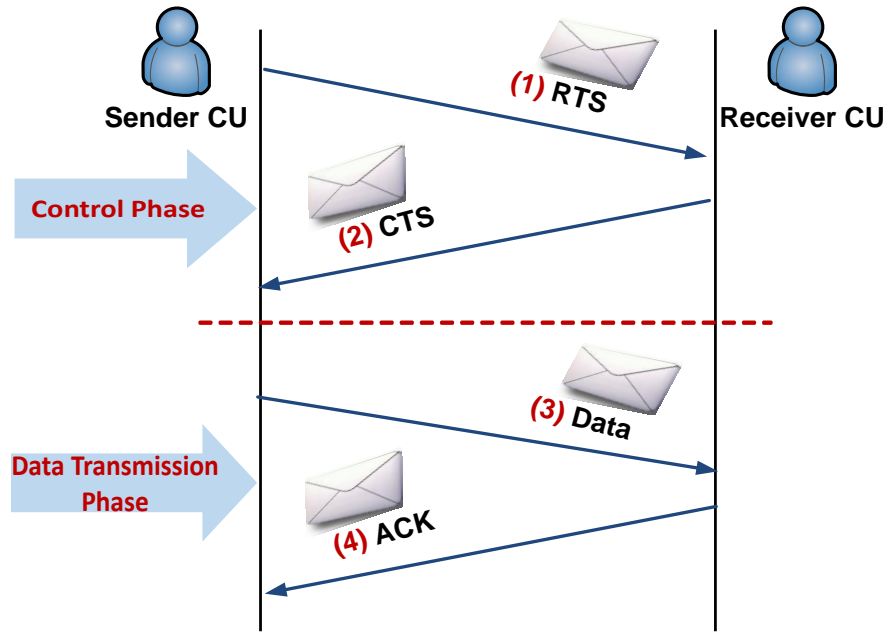


Figure 3-3: Control and data frames sequences in MCRN

### 3.2.5.1. Control Phase

Both the Request-To-Send (RTS) and Clear-To-Send (CTS), in the context of CR, are control frames which are used in the MCRN protocol based on Distributed Co-ordination Function (DCF). The format of the control frames, RTS and CTS, are shown in Figure 3-4 and Figure 3-5.

The RTS is a broadcast frame, in which an additional field of 2 bytes, called Free Channel Lists (FCL), is allocated to include a list of a maximum of four available licensed channels that are determined by the sender to enable data transmission. Each channel can be represented in 4 bits. However, in the CTS unicast frame, based on these attached channels, the receiver determines the best available channel according to channel selection criteria which are explained in section 3.2.2.2. Only the most reliable selected licensed channel based on the highest available time from the FCL is used by the receiver CU. This channel, called the Selected Licensed Data Channel (SLDCH), can be represented in 4 bits while the remaining bits are set to 0 in this thesis.

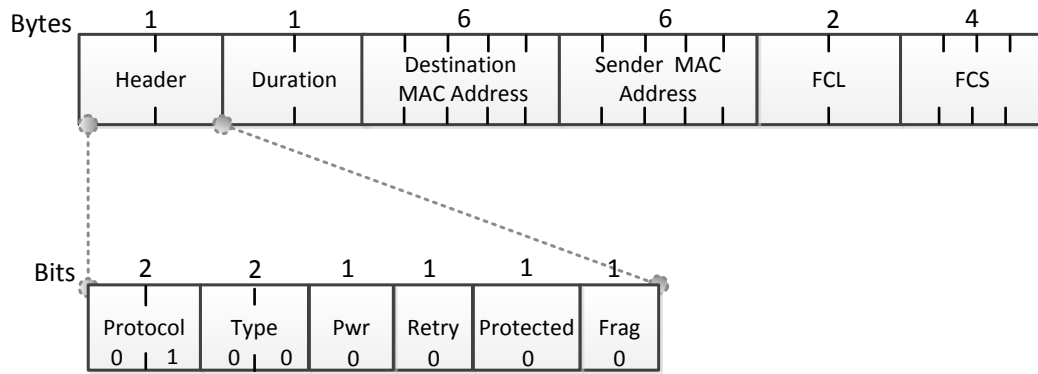


Figure 3-4: RTS frame format

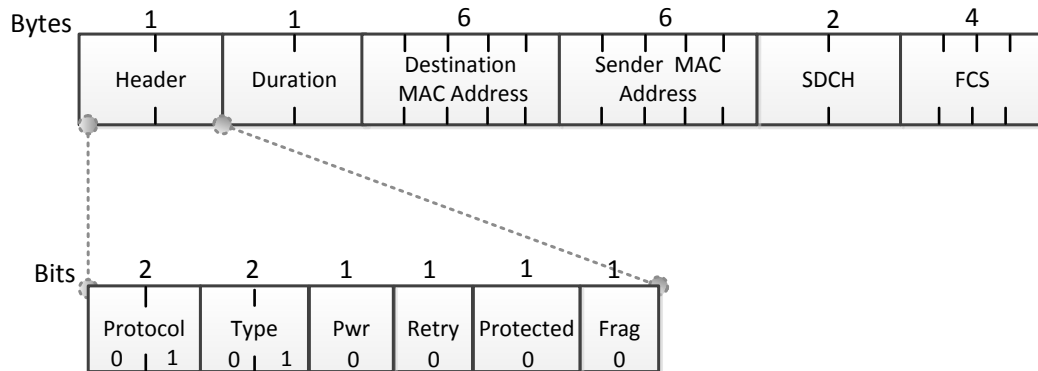


Figure 3-5: CTS frame format

### 3.2.5.2. Data transmission Phase

The data transmission phase takes place only if both the sender and receiver CUs successfully exchanged both the RTS and CTS frames and agreed on the licensed data channel for data transmission. Thus, both CUs switch to the selected licensed data channel as soon as the CTS frame is successfully delivered to the intended destination. Then the sender initiates the data transmission over the SLDCH without waiting time (DIFS) as the channel is available and has already been selected by both CUs. In contrast, the intended destination CU requires SIFS waiting time. The receiver therefore initiates the transmission of the ACK frame to notify the sender that the data has been delivered successfully. Based on the successful receipt of the ACK frame, the communication process between a pair of CUs is successfully completed and the entire process of frames exchange is terminated. The frame format of the Data and ACK frames are shown in Figure 3-6 and Figure 3-7 respectively. However, once the LU appears to be ON and able to utilise the selected licensed data channel during the data transmission,

then both CUs are required to immediately vacate the channel and restart the entire process to determine another SLDCH.

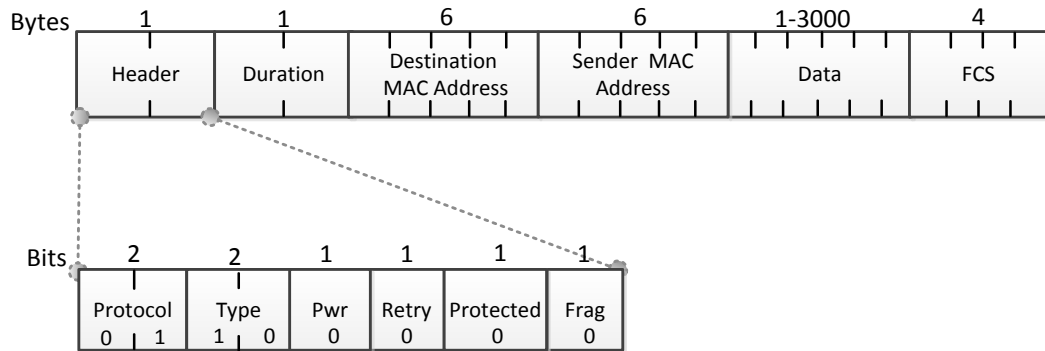


Figure 3-6: Data frame format

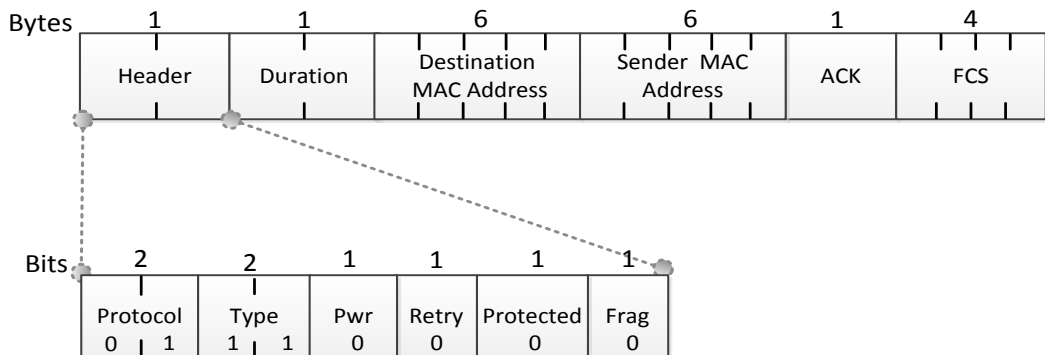


Figure 3-7: ACK frame format

### 3.2.6. Medium Access Control (MAC) for MCRN

The MAC layer which exists in the IEEE 802.11 wireless protocols to establish the communication process of the shared wireless medium among users provides the same functionality in CRNs to deliver reliable data among CUs. Therefore, two different types of channels are considered in the MCRN protocol, namely a CCC, which is a dedicated channel and is assumed to be available all the time for CUs to exchange their control information and licensed data channels that are determined by the CUs to exchange their data.

Figure 3-8 demonstrates the process of frame exchanges between CUs and highlights both DIFS and SIFS time as well as the Network Allocation Vector (NAV) during the frames' exchange.

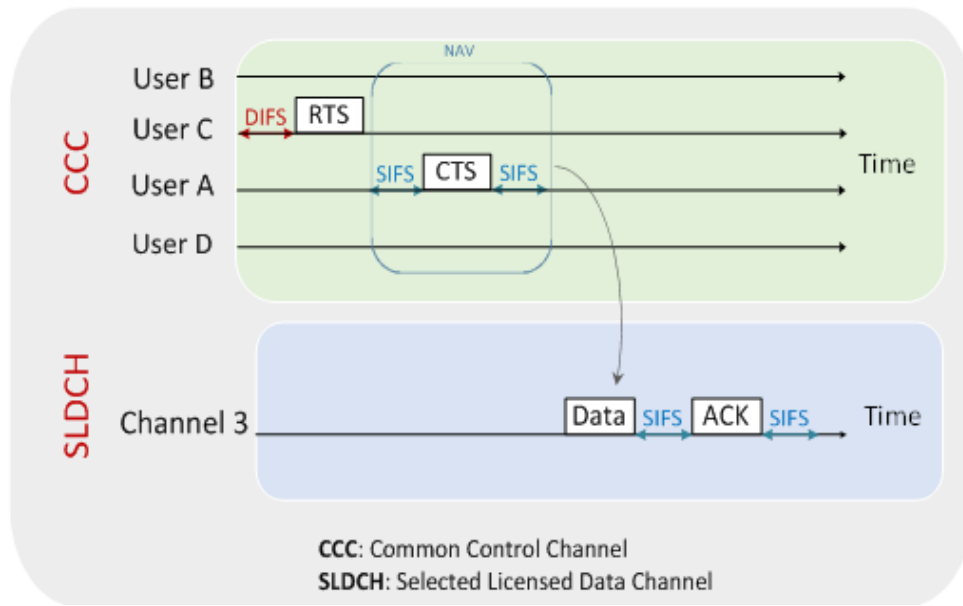


Figure 3-8: Timing and process of Medium Access Control (MAC) in MCRN

### 3.2.6.1. MAC access modes and timing

The DCF technique is applied in the MCRN protocol to provide the same functionalities in terms of accessing the CCC and exchanging the control frames between a pair of CUs before initiating the data transmission. Although only one CCC is located for multiple CUs to exchange their control frames, the DCF method offers the essential access and coordinates multiple CUs to utilise the same wireless channel to launch frame transmissions without the possibility of a collision. The DCF technique is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) (Taejoon & Jong-Tae, 2009) (Jie, et al., 2013) (Dappuri & Venkatesh, 2014) in which users are required to ensure that the CCC is clear for transmission before launching their control frames. This aims to avoid collisions and is achieved by applying channel access based on a contention technique and random backoff time. If the channel is marked busy, then a CU needs to set random back-off time to avoid collision.

Thus, in Figure 3-8 above, there are two pairs of CUs that need to launch their RTSs over the CCC for the purpose of data exchange. CU C needs to communicate with CU A. Therefore, the process of the prior CCC access is based on the contention technique and CU C requires checking of the availability of the CCC for a time equal to DIFS before launching the RTS frames. If the CCC is

busy then both CUs apply random backoff time to seize the channel without any collisions occurring. If the CCC is found to be available and assuming CU C wins access to the CCC, then CU C can launch the RTS frame because the channel is available for a period of time exceeding DIFS time.

Each intended destination CU requires waiting time measured in microseconds known as SIFS after receiving each control frame (RTS and CTS). Then, once the SIFS time has elapsed, a CU can reply over the CCC with CTS if the RTS has been received or switch to the selected data channel for data transmission if the CTS has been received. By exchanging these two control frames successfully, both CU C and CU A agree to select the SLDCH (Channel 1) to exchange data, therefore they switch to the SLDCH immediately as soon as the SIFS time to initiate data transmission has elapsed.

In terms of the data channels, two types of frames exist, namely, *Data* and *ACK*. CU C (sender) can launch the data frame without waiting time as the channel is sensed and determined to be available during the exchange of the CTS frame over the CCC. However, the receiver, CU B, requires SIFS time before replying with the ACK frame.

As soon as the first group vacates the CCC after the successful switching to the selected data channel, the CCC will be available for other CUs to exchange their control information. Thus, it can be utilised by different pairs of CUs after the contention technique of accessing the CCC. The second group of CUs exchange their RTS and CTS frames and then switch to different SLDCH (Channel 2) for data transmission. This process of using the CCC will continue as long as there are CUs willing to exchange data.

### 3.2.6.2. NAV period

According to 802.11 wireless frames (Sushma & Dijiang, 2010), a duration field is included within the transmitted frames to reserve of the channel for a specific time, which is measured in microseconds, required to complete the transmission process (Sushma & Dijiang, 2010). Therefore, the duration field in the RTS in MCRN has the same functionality for representing the Network Allocation Vector (NAV) time which aims to inform the other CUs within the same range that the

CCC is reserved (busy) for a fixed time. This resulted in barring of the utilisation of the current channel during that period by other CUs, otherwise the transmission process would be interrupted. This benefits wireless devices in terms of saving power as it enters into power saving mode until the NAV value reaches zero. Thus, the neighbouring CUs, who are within the same range, can recognise the transmitted control frames. They set their NAV according to what is provided in the duration field of the transmitted frame and then they count down the NAV timer to reach zero before attempting to transmit a frame. As soon as the timer of the NAV reaches zero, CUs are alerted that the CCC becomes available for utilisation.

### **3.3. Secure MAC Protocols for Cognitive Radio Networks (SMCRN)**

The MCRN protocol proposed and discussed in the previous section does not consider the required security features against the potential threats in CRNs. Therefore, this section focusses on the design of two different security protocols identified as, Digital-Signature based Secure MAC protocol for CRN (DSMCRN), and the Shared-Key based Secure MAC protocol for CRN (SSMCRN). These two security protocols are built independently on the proposed MCRN protocol to address the security requirements within CRNs. Therefore, the security protocols' frameworks which demonstrate the full operation and frames sequences related to security keys exchanges and communication are provided. In addition, the associated security features, aim in addressing the security requirements in CRNs, of each protocol are highlighted and explained in details.

#### **3.3.1. Symmetric and Asymmetric keys cryptography in SSMCRN and DSMCRN**

Two different types of cryptographic keys are identified in the security field as asymmetric (Public and private), and symmetric (Shared or Secret) keys. They not only aim to perform the secure communication in the DSMCRN and SSMCRN protocols respectively, but also other relevant security features such as

authentication, integrity, and confidentiality among incorporated users with the assistance of using different security algorithms.

Although, the proposed protocols can adopt any types of both asymmetric and symmetric key algorithms, both RSA and AES are considered among the other security algorithms. Since RSA is widely utilised for secure information exchange while AES is considered to be the strongest security approach in cryptography compared to the other related techniques. Despite, DES was the strongest security algorithm up to 1992, it failed to become so due to its vulnerability to threats resulted from its small key size. This failure led the National Institutes of Standards and Technology (NIST) to replace the DES algorithm with the AES that provides more security and has not been broken so far (Naidu & Joshi, 2015). Consequently, the U.S. government announced that the AES algorithm can be used for protecting information and became the default security algorithm to encrypt information. Thus, the associated features of AES like, gaining high throughput, flexibility, simplicity, and easiness of implementation has led AES adaptation by numerous organisations across the world (Kumar & Rajalakshmi, 2014).

### 3.3.1.1. Associated cryptographic keys in SSMCRN

In SSMCRN, three different symmetric (Shared) keys and an asymmetric (public/private) key are applied to provide different security features, these keys are classified into four groups:

- Group 1: **Network's Shared Key** shares between all registered CUs and server for gaining authorised access to the network.
- Group 2: **X-S-Shared Key** is shared between the user X and the Server only. It is generated by user X before transmitting IOR frame to encrypt/decrypt and ensure the integrity of the transmitted information between the server and user X.
- Group 3: **X-Y-Shared Key** is generated by the server after the successful authentication process for both users X and Y only. This ensures the confidentiality and the integrity of the transmitted information between this pair of CUs.

## Design of the proposed MAC protocols with and without security

- Group 4: **Server's public/private key**: the server public key is distributed to all users whom willing to register and gain authorised access to information to utilise the network resources. Its function is to exchange secret information belonging to the user at the initial stage of the registration process.

The primary reasons of using three different shared keys in SSMCRN are:

- 1- Different pairs of CUs are required to communicate securely with the demand of achieving the confidentiality.
- 2- Since CUs have the ability of misbehaving during the transmission, therefore if a group of CUs shares the same shared key, it will increase the chance of misbehaviour activities such as decrypting any encrypted transmitted messages. As a result the detection process will be difficult to achieve.
- 3- Through applying three different shared keys the following security requirements can be achieved.
  - Authentication through the use of **Network's Shared Key**
  - Secure frames' exchanges between the intended recipients through the use of **X-S-Shared Key** and **X-Y-Shared Key** at different security levels
  - Confidentiality with the help of applying the **X-S-Shared Key**
  - Integrity assurance through applying the **X-S-Shared Key** and **X-Y-Shared Key**

Table 3-1 below outlines the aims of using these keys and their relation to the required security features in SSMCRN.

Table 3-1: Security Keys in SSMCRN

Cryptographic Keys	Authentication	Integrity	Confidentiality	Secure Transmission
<b>Server's Public/Private Key</b>			Only the server can decrypt the IOR	Encrypt IOR
<b>Network's Shared Key</b>	To authenticate CUs	To ensure the integrity of ITA and RTA	Confidential communication	Encrypt ITA and RTA
<b>X-S-Shared Key</b>		To ensure the integrity of COR, CUA1 or CUA2	Only user X decrypt the COR and CUA1 or CUA2	Encrypt COR, CUA1 and CUA2
<b>X-Y-Shared Key</b>		To ensure the integrity of RTS and CTS and Data	Only users X and Y decrypt the RTS, CTS and Data	Encrypt RTS, CTS and Data

### 3.3.1.2. Associated cryptographic keys in DSMCRN

In DSMCRN, as part of the *Server's public/private key*, only two different shared keys are identified as *X-S-Shared Key* and *X-Y-Shared Key* along with the *User's Public/Private Key* are applied. These associated keys are classified into four groups as follows:

- Group 1: *User's Public/Private Key* is generated by the CUs during the registration process. Therefore, the public key is provided to the server to generate a unique ID that is associated with the user public key. This ID aims to have the registered CU gain the authorised access to the network resources and used for authenticating the CU through the associated public key for verifying digital signature procedure.
- Group 2: *X-S-Shared Key* is shared between user X and the Server only. It is generated by user X before transmitting IOR frame to encrypt/decrypt and ensures the integrity of the transmitted information between the server and user X.
- Group 3: *X-Y-Shared Key* is generated by the server after the successful authentication process for both users X and Y only. This ensures the confidentiality and integrity of the transmitted information between this pair of CUs.
- Group 4: *Server's public/private key*: the server public key is distributed to all users who are willing to register and gain authorised access information to utilise the network resources. Its function is to exchange secret information belong to the user at the initial stage of the registration process.

Table 3-2 highlights the associated cryptographic keys to incorporate in providing the required security features in DSMCRN protocols.

Table 3-2: Security Keys in DSMCRN

Cryptographic Keys	Authentication	Integrity	Confidentiality	Secure Transmission
<b>Server's Public /Private Key</b>			Only the server can decrypt the IOR, ITA and RTA	Encrypt IOR, ITA and RTA
<b>X Public/ Private Key</b>	Generate/verify digital signature	To ensure the integrity of ITA and RTA through DS	The private key is kept secret to sign messages	
<b>X-S-Shared Key</b>		To ensure the integrity of COR, CUA1 and CUA2	Only user X decrypt the message	Encrypt COR, CUA1 and CUA2
<b>X-Y-Shared Key</b>		To ensure the integrity of FCL and SLDCH and Data	Only user X and Y decrypt the messages	Encrypt RTS, CTS and Data

### 3.3.2. Secure keys exchanges in DSMCRN and SSMCRN

Each authorised registered CU has a unique ID which is associated with the user's public-key in DSMCRN while network's Shared Key and ID in SSMCRN. This is the authorised access information is generated by the server and obtained in the registration phase of the DSMCRN and SSMCRN protocols. However, the main security concern is that this information must be delivered to each intended registered CU in protected and unreadable format from other users. Because the received information is essentially used to identify the CU, whom this information belongs, to the server in DSMCRN and the CUs who are part of the network in SSMCRN. Also, the authentication procedure is mainly based on the public key of the registered CU in DSMCRN and the network's Shared Key and ID in SSMCRN. Without the encryption technique, this information is easily manipulated or obtained and used by different users or attackers. Therefore, the generated **X-S-Shared Key (Group2)** is considered to produce the ideal solution to encrypt and protect this transmitted information from other users before its transmission. However, the **X-S-Shared Key (Group2)** necessitates to be shared between both CU X and the server previously. Thus, in order to distribute it to the server in a secure manner, the use of the **server's public key (Group4)** provides a perfect consideration for encrypting the **X-S-Shared Key**. As the encrypted **X-S-Shared Key** can only be decrypted by the server which has the private key.

Furthermore, the *X-S-Shared Key (Group2)* is also used for encrypting the *X-Y-Shared Key (Group3)* in the CUA1 or CUA2 frames in both DSMCRN and SSMCRN. Thus, the overall secure exchanged keys are encrypted and decrypted by the right entities in both DSMCRN and SSMCRN. Figure 3-9 summarises the encrypted keys exchanges by involving different keys in DSMCRN and SSMCRN.

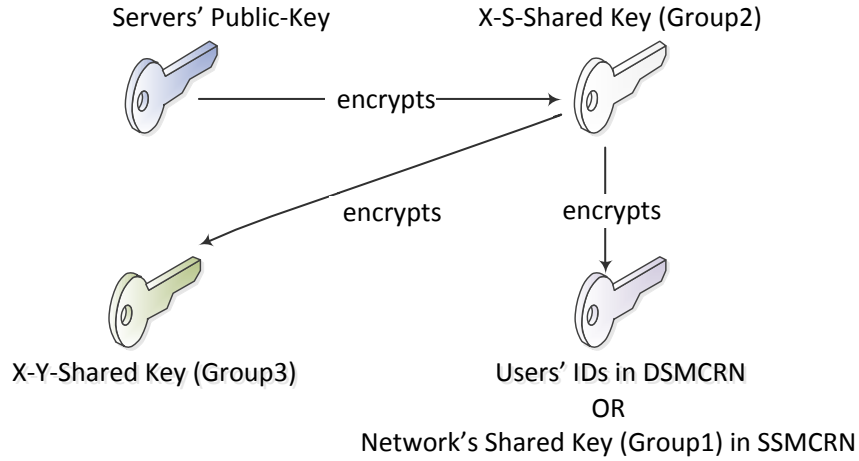


Figure 3-9: Secure keys exchanges in DSMCRN and SSMCRN

### 3.3.3. DSMCRN and SSMCRN architecture

Although the proposed MCRN protocol for decentralised CRNs was discussed in depth in chapter 3, it is entirely revisited in this chapter with some additional factors belonging to the security procedures. The additional aspects can be highlighted into two sides. The first is a cooperative dedicated server that is engaged for the authentication purpose and providing the security key management to end users through registering CUs for controlling the entire network. The second belongs to the additional security frames required to provide the necessary security demands, including the authentication and users' validation, as well as secure communications among incorporating entities. These additional aspects are applied to both DSMCRN and SSMCRN equally with the same added frames and server involvement. However, the main difference between them is that some of the frames have different sizes compared to each other in both protocols. This is because of the required security information exchanged between CUs and the server.

Thus in Figure 3-10, a dedicated server is incorporated within the communication over only the dedicated CCC, which is allocated to the server and CUs only for exchanging the security frames and control information belongs to the sensing channels results (Free channels List, FCL, or white spaces) and the most reliable selected licensed data channel (SLDCH) for the aim of exchange data between a pair of CUs within the same range.

Therefore, case 1 refers to two different situations in which the CUs perform the contention method to access the CCC in order to communicate with the server for the registration process to gain authorised access to network information, or authentication procedure to send a request for validating CUs. This case is only used for security purposes, and is considered an initial stage in which a CU exchanges registration and security frames before initiating the process of control information exchange. This aims to control the network, so that it can only be utilised by authorised CUs. Once the CUs are successfully authenticated and permitted to continue communicating with each other, then case 2 is begun to exchange the FCL and SLDCH information over the CCC, and to perform the switching procedure to the SLDCH. Therefore, the same discussion about the network scenario as raised in section 3.2.3 is applied in DSMCRN and SSMCRN protocols, to exchange control information and initiate data transmission. Thus, the complete framework of both DSMCRN and SSMCRN is demonstrated in Figure 3-11.

## Design of the proposed MAC protocols with and without security

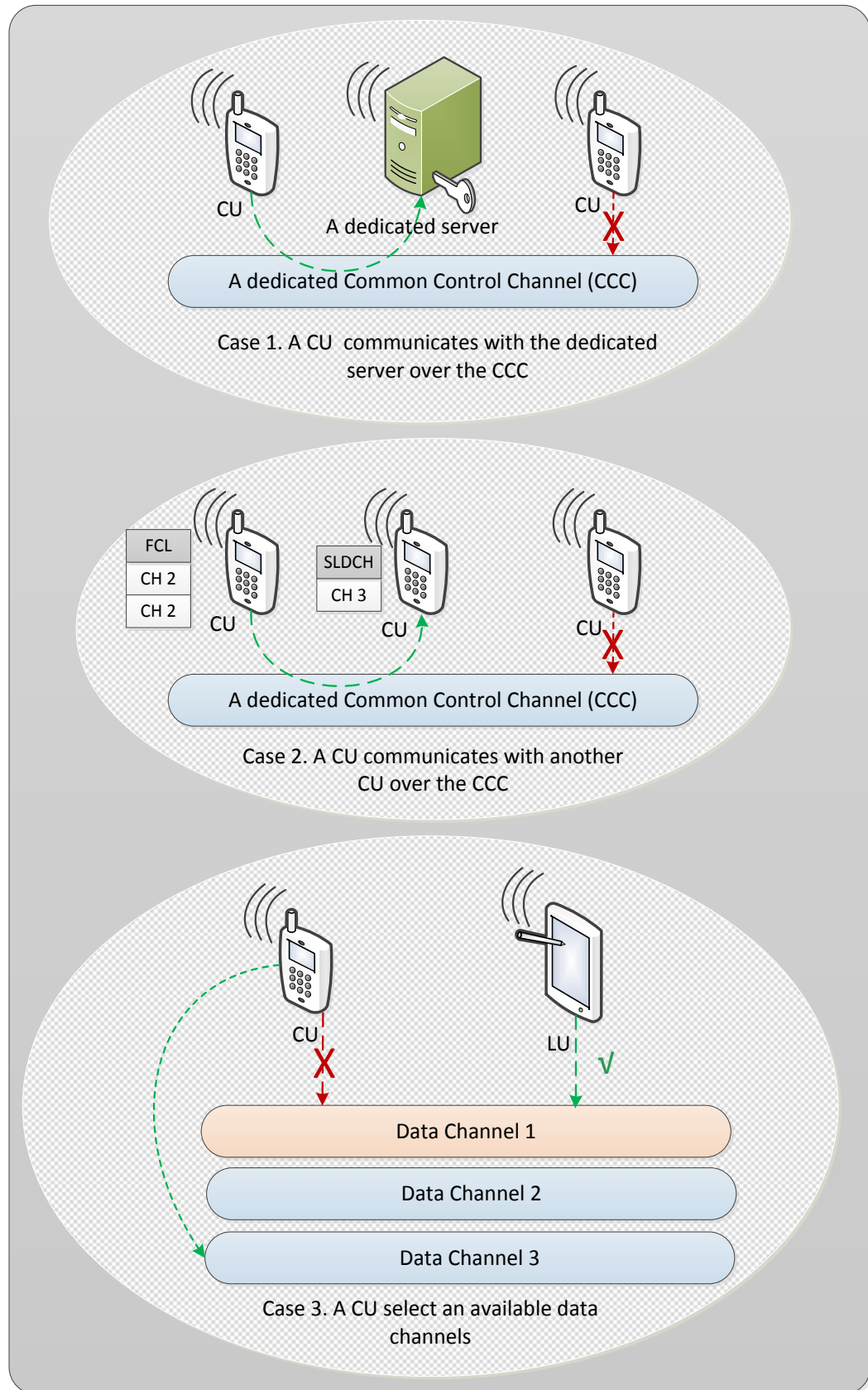


Figure 3-10: DSMCRN and SSMCRN Network scenario

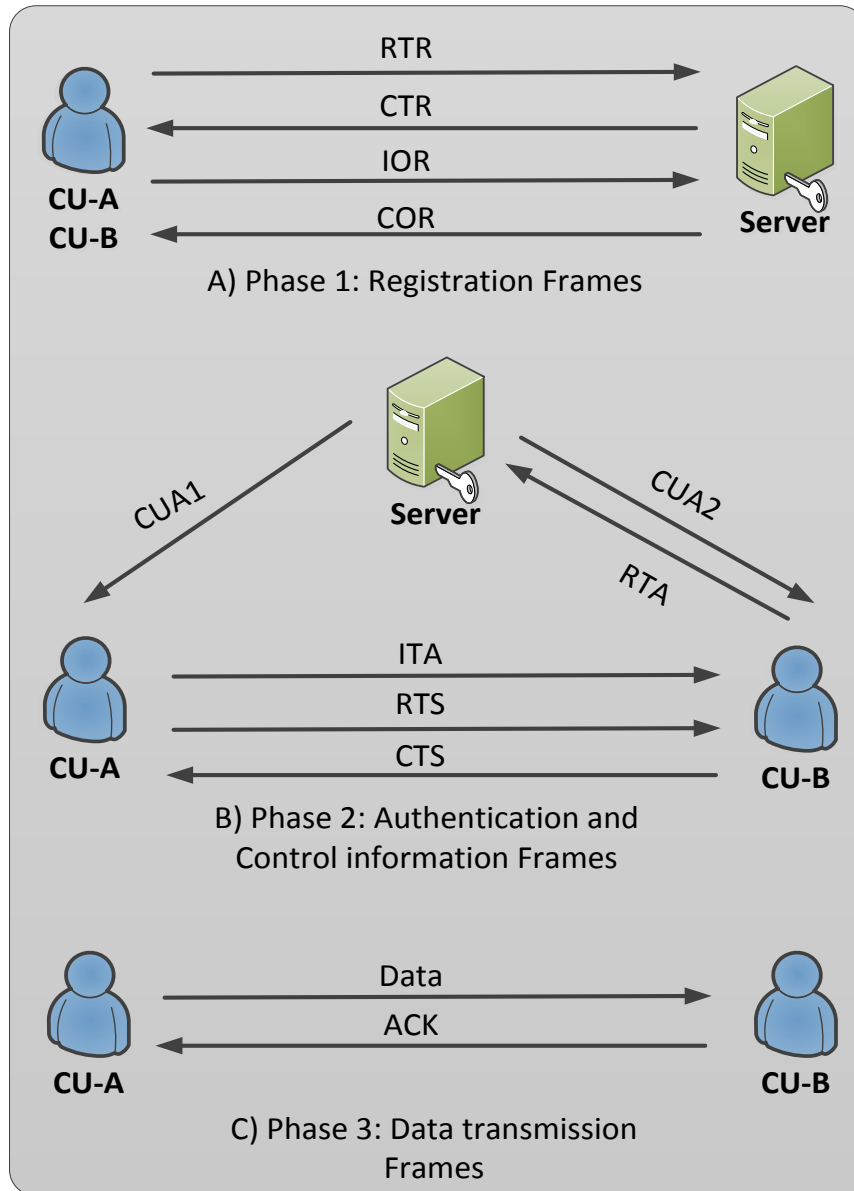


Figure 3-11: DSMCRN and SSMCRN architecture

The assumed authentication server involved in the network and shown in Figure 3-11 is a layer 2 device which can be an AP or a mobile device. It is assumed that the device is capable for providing the required associated transparent security functions related to the encryption and decryption. This differentiates the operation of the assumed authentication device in the proposed protocols from the other existing authentication servers that operate in the application and transport layers such as RADIUS and TACACS+ respectively. Therefore, the proposed protocols integrate all the required security features in a single layer instead of relying on multiple layers this avoiding complexity and

possible additional overhead that might occur that lead to the decrease in network efficiency. Accordingly, the proposed security protocols are simple in their structure and operation, since the assumed layer 2 authentication server has less complexity in terms of performing authentication processes without the need of access credentials which are required for RADIUS. Moreover, since the CRNs are self-organised, self-configured and can be deployed anywhere and anytime free of cost, the use of existing authentication server will have additional costs that can affect the deployment of CR technology. Therefore, the proposed security protocols use the authentication server for both registering CUs and authentication purposes. In addition, the use of the associated security at the MAC layer ensures the protection and confidentiality for the information presented in the MAC frames related to the message transmission between two CUs in decentralised CRNs. Thus, the security issues related to the PHY and MAC layers in decentralised CRNs, such as jamming attacks, Spectrum Sensing Data Manipulation/Falsefication, MAC address Spoofing, and Primary User Emulation (PUE) and Primary User Interference (PUI) attacks, are handled by offering the security at these layers.

### **3.3.4. Digital-Signature based secure MAC protocol for Cognitive Radio Networks (DSMCRN)**

DSMCRN is a Digital Signature based secure MAC protocol for CRNs (Alhakami, et al., 2013) designed to achieve the security requirements, such as authentication, authorisation and data confidentiality addressing most of the existing issues in decentralised CRNs. A cooperative dedicated server is engaged for the authentication purpose based on a digital signature procedure with the assistance of asymmetric-key cryptography for detection mechanisms against unauthorised access. The server also provides the security key management to valid CUs for maintaining a secure communication process. Therefore, the protocol accommodates two different cryptographic encryption mechanisms known as *symmetric* and *asymmetric* encryption techniques that are used to secure messages' transmissions (Alhakami, et al., 2013). It also consists of three different essential embedded phases that operate in sequence. Each phase has a

different task and relies on the completion of the previous phase. Table 3-3 demonstrate where the symmetric and asymmetric key algorithms are used in the DSMCRN.

Table 3-3: Encryption methods used in DSMCRN

Encryption Method	Type of encryption	Keys size	DSMCRN Phases					
			Registration		Control			Data
			Server to Node	Node to Server	Node to Node	Node to Server	Server to Node	Node to Node
RSA	Asymmetric Cryptography	1024		√		√		
AES	Symmetric Cryptography	128	√		√		√	√

In order to obtain the required security for achieving a successful data transmission among valid CUs, each user necessitates going through two different stages before transmitting data. These two phases are designed and applied for the security purpose. More details of the functions of each phase are discussed next:

#### **3.3.4.1. Registration phase of DSMCRN**

The registration process is considerably important to CUs for obtaining the security IDs to provide authorised network access. This security information is essential because it enables only the registered CUs in joining the network, and continuously communicate with the other valid users. Therefore, CUs who intend to use the network resources, are required to register their information with a dedicated server to obtain a user's ID. This is achieved through launching four frames; *Request-To-Register (RTR)*, *Clear-To-Register (CTR)*, *Information-Of-Registration (IOR)*, and *Confirmation-Of-Registration (COR)* over the CCC. Figure 3-12 shows the messages' sequence of the registration phase of both protocols.

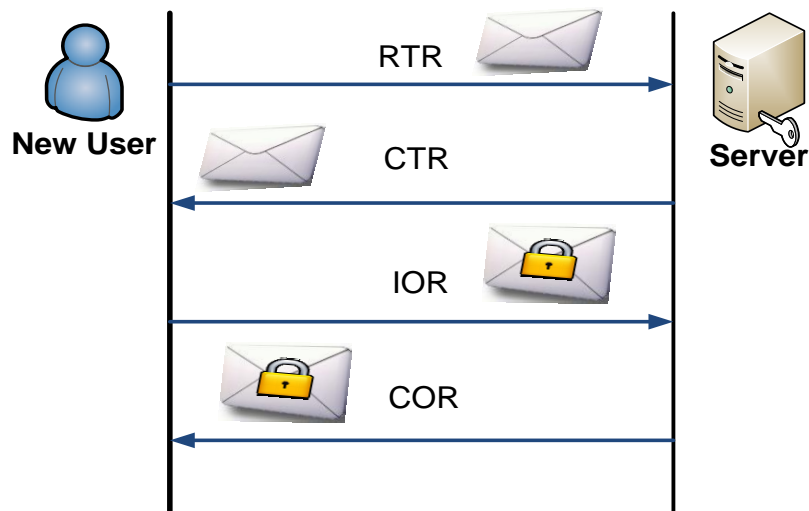


Figure 3-12: Messages' sequence of the registration phase

### 1) Request-To-Register (RTR) frame

The process of initiating the registration phase is established when a new CU transmits an RTR broadcast frame over the CCC. The frame's destination is the dedicated server which is the main controller of the network in terms of the security key management to end users, and the authentication procedure. Figure 3-13 shows the RTR frame contents.

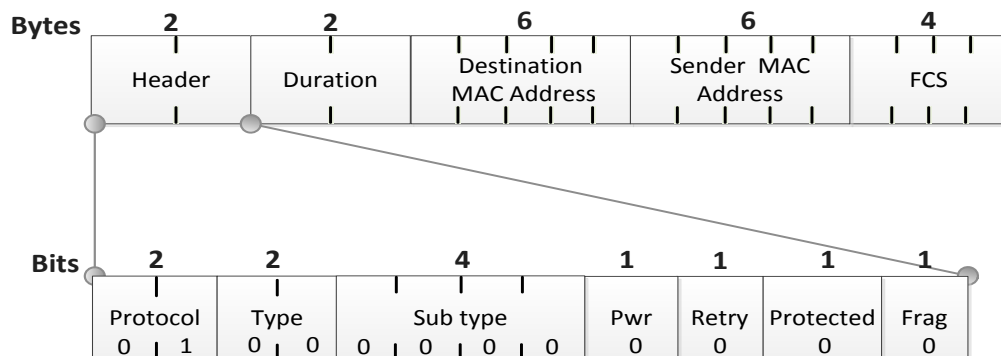


Figure 3-13: RTR frame format

### 2) Clear-To-Register (CTR) Frame

A CTR is a unicast frame that is sent as a reply by the server. It includes the public-key in order to encrypt any transmitted information between those two entities in the next frame. Therefore, the frame format is shown in Figure 3-14.

## Design of the proposed MAC protocols with and without security

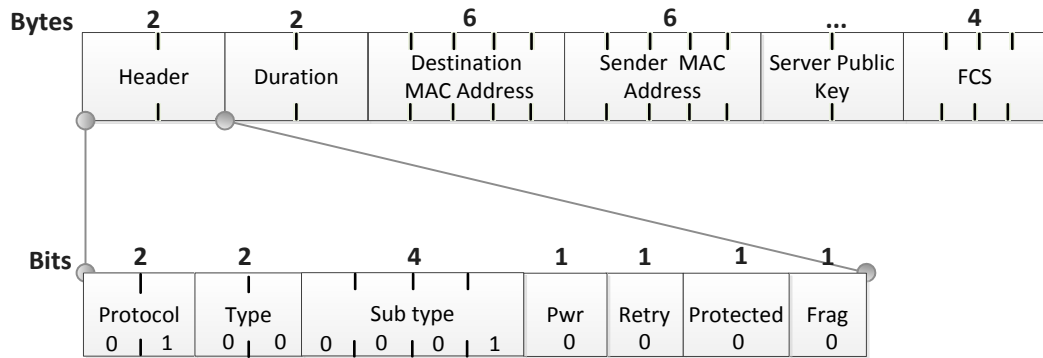


Figure 3-14: CTR frame format

### 3) Information-of-Registration (IOR) Frame:

After receiving the server's Public-Key, the CU requires generating security keys from both symmetric and asymmetric keys cryptography independently. A shared key is generated from AES-128 and a pair of public/private keys is generated from RSA-1024 algorithms. Only the public and shared keys will be distributed to the server in a unicast secure manner. Therefore, the CU requires generating a Message Authentication Code Key (MAC-key) to ensure the integrity of the transmitted keys to the dedicated server. Therefore, the CU encrypts MAC-Key, ID, Shared-key and Public-key using the server's public-key, which is received in the CTR frame. This encrypted information then is included in the IOR frame before its transmission to the server as shown in Figure 3-15.

As soon as the server received the IOR, it will decrypt the information through applying its Private-key. Then the server needs to verify the received information from any modification that has occurred during the transmission. Therefore, it generates a new MAC-Key through applying the MAC-Key algorithm with the use of the received Shared-Key, ID and Public-Key. If both the generated and received MAC-Keys are identical, then the IOR frame is accepted.

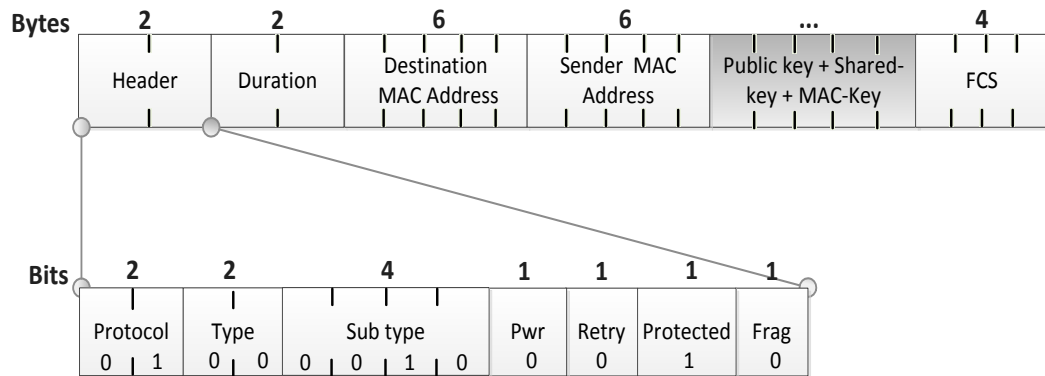


Figure 3-15: IOR frame format in DSMCRN

#### 4) Confirmation-Of-Registration (COR) frame

Once the server has accepted the IOR information, it stores both the user's Public-Key, ID and Shared-key and generates a specific ID for the CU. Therefore, the server sends a COR unicast frame that includes the generated ID and a new MAC-Key in an encrypted format using the same Shared-Key that received in the IOR frame from the user. Consequently the user obtains the required ID after decrypting and then verifying the received information using the same Shared-Key and MAC-Key algorithm respectively. This information indicates the complete successful registration process and offers the ability to the CU for joining the network. However, in case of MAC-Key verification indicates false which means the transmitted information has been modified during the transmission, the CU requires to launch the RES frame in order to let the server retransmit the COR frame. The content of the COR frame is demonstrated in Figure 3-16.

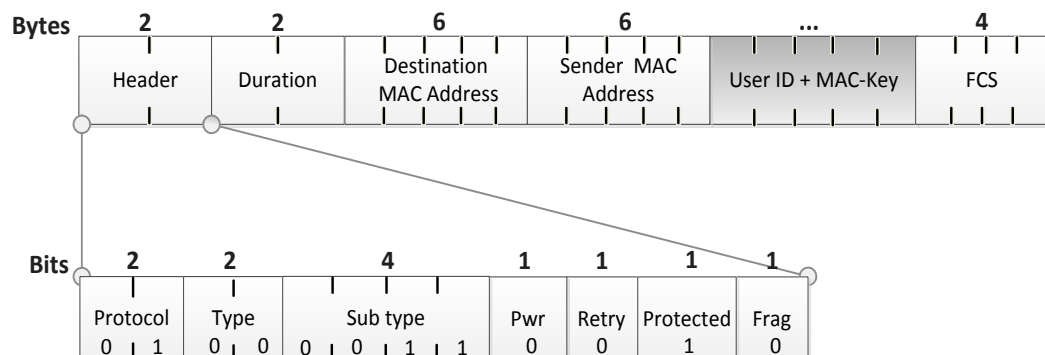


Figure 3-16: COR frame format

The flowchart of the entire registration process of both the DSMCRN and SSMCRN protocols is shown in Figure 3-17.

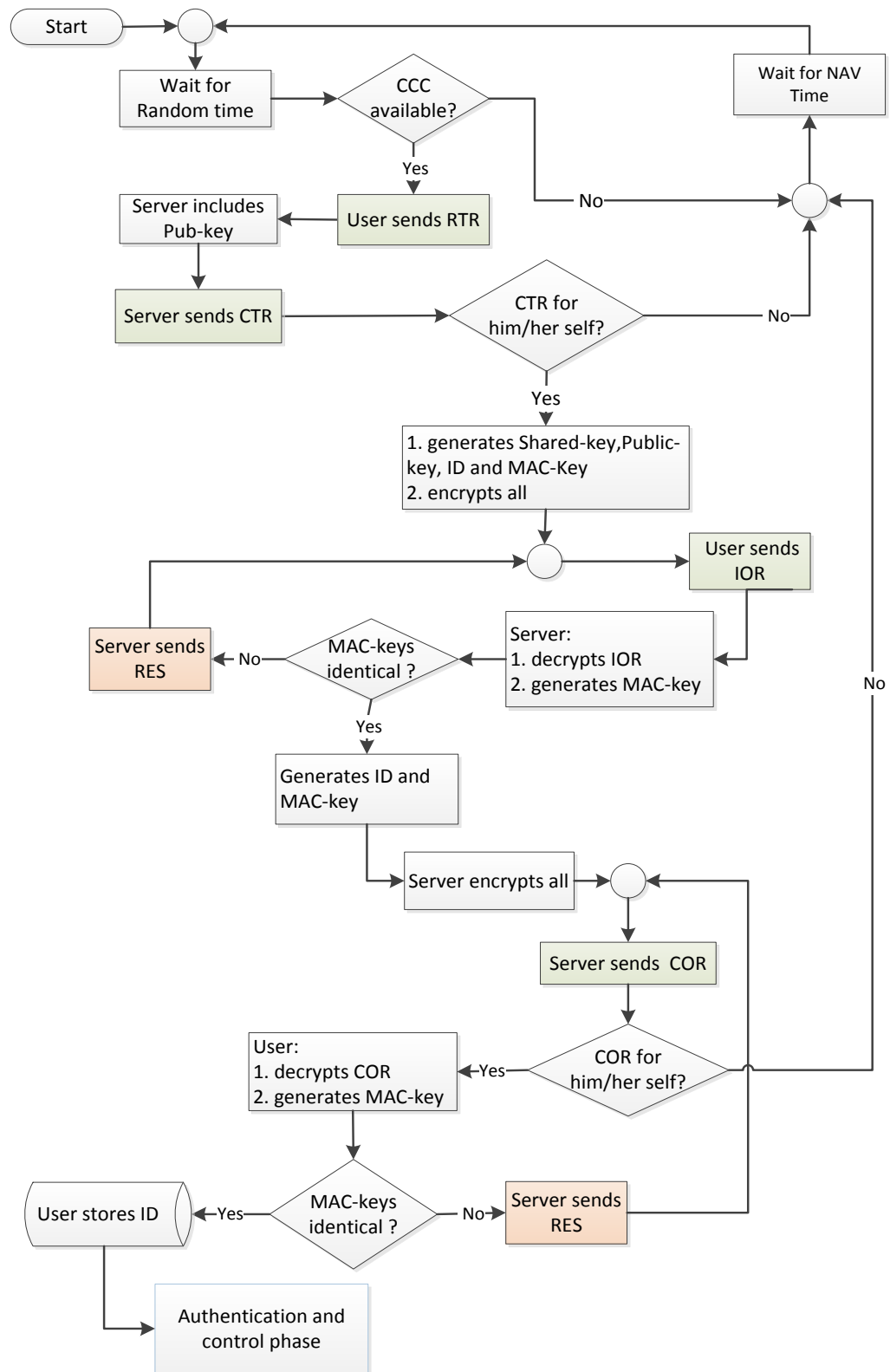


Figure 3-17: Flow chart of the registration process in DSMCRN

### 3.3.4.2. Authentication and control phase of DSMCRN

The current phase considers as the initial stage of applying the security techniques in the communication between the sender and receiver CUs. It is designed for exchanging six frames; *Information-To-Authenticate (ITA)*, *Request-To-Authenticate (RTA)*, *Confirmation-Of-Authentication1 (CUA1)*, *Confirmation-Of-Authentication2 (CUA2)*, *Request-To-Send (RTS)* and *Clear-To-Send (CTS)*. These frames are divided into two groups based on their functionalities. The first group is the security frames, which are ITA, RTA, CUA1 and CUA2, for achieving the task of authenticating both the sender and receiver CUs through applying a digital signature procedure and providing a shared-key for those users after they are authenticated in order to encrypt and decrypt the next frames. The second group is the control information frames, which are RTS and CTS, for control information exchange between the sender and receiver. Figure 3-18 below illustrates the sequence of the Authentication and Control phase frames' transmission among the sender, receiver and the server:

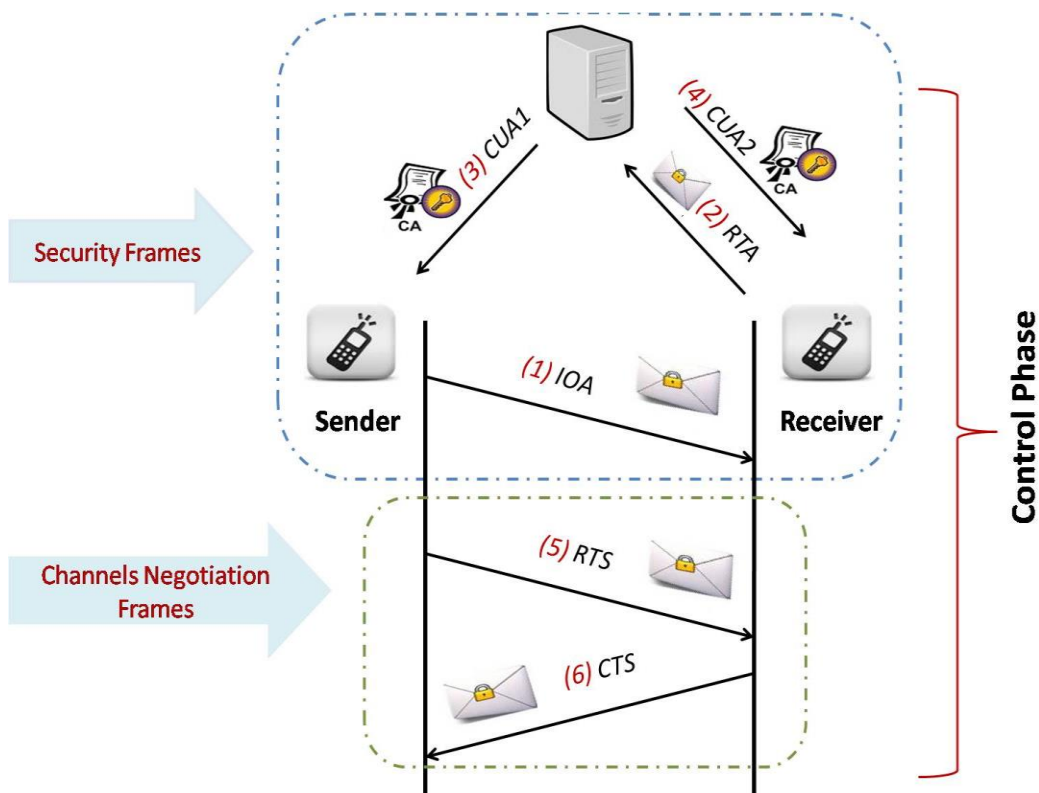


Figure 3-18: Authentication and control phase framework in DSMCRN and SSMCRN

### 1) Information-To-Authenticate (ITA) frame:

The process of the communication between a pair of CUs is initiated formerly when the sender CU signs its ID. This would result in generating a digital signature, which then is attached to the ID. The sender therefore encrypts both the generated signature and ID uses the server's public key (Group 4) that was received in a CTR unicast frame. This encrypted information is attached to the ITA frame which then is transmitted to the receiver CU. Figure 3-19 shows the ITA frame format after the encryption.

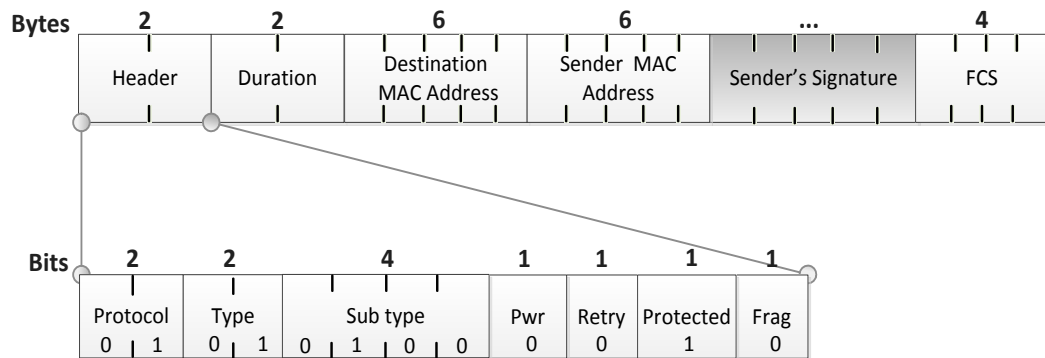


Figure 3-19: ITA frame format in DSMCRN

### 2) Request To Authenticate (RTA) frame:

As soon as the receiver CU received the ITA frame, it does the same process of signing its ID and then attaching to the generated signature that belongs to himself for authentication purpose. Then the receiver CU attaches both the received encrypted information from the sender CU and its information to the RTA frame which then is transmitted in a unicast form to the server. The frame format of the RTA, which includes two separate signatures belong to the sender and receiver CUs, after the encryption is shown in Figure 3-20.

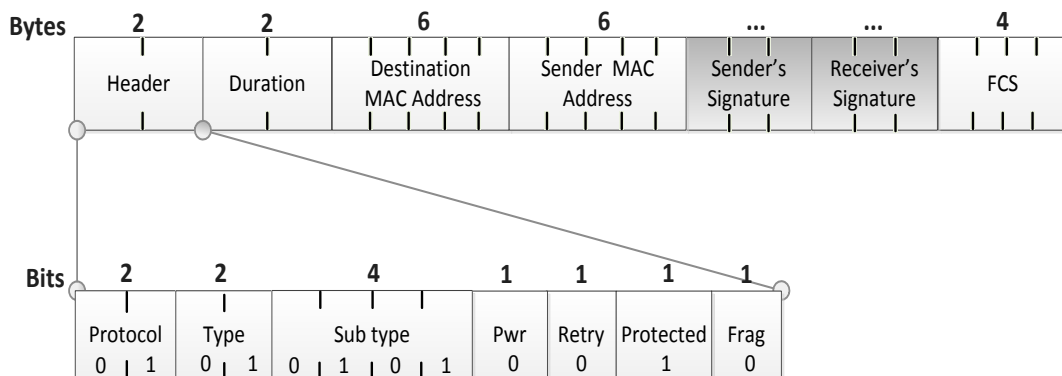


Figure 3-20: RTA frame format in DSMCRN

As soon as the server receives the RTA frame, it requires verifying both signatures individually after decrypting them using its private-key. Therefore, with the help of the received IDs, the server uses its database to retrieve the public-keys of the sender and receiver CUs and then verifies each signature through applying these public-keys separately. Based on the verification results, two possible actions will be taken by the server; if the result of the each signature verification is positive (True), it indicates that both users are authorised and allowed to continue the communication with each other. Thus, the server will generate a shared-key for both sender and receiver for encryption and decryption, this key is represented as ***X-Y-Shared Key*** (Group 3).

However, if the status of one of the digital signature verification refers to negative (False), this means that the user is failed to authenticate and treated as malicious or invalid users because of non-registration within the server to gain authorised access to the network. In this case, the server will eliminate the user who is failed to authenticate from gaining access and uses the resources of the network. In other words, suppose the sender is a malicious user or has not registered for obtaining an ID and contributed with the communication by sending ITA, if their signature is failed to be verified, then the server will update the receiver CU with this by sending a Fail-To-Authenticate frame indicates that sender is malicious. Thus, the receiver CU requires stopping the communication with the sender CU immediately. The failure of authentication process framework is shown in Figure 3-21 while the format of the FTA frame is shown in Figure 3-22. Therefore the entire process of the authentication flowchart of DSMCRN is shown in Figure 3-23.

## Design of the proposed MAC protocols with and without security

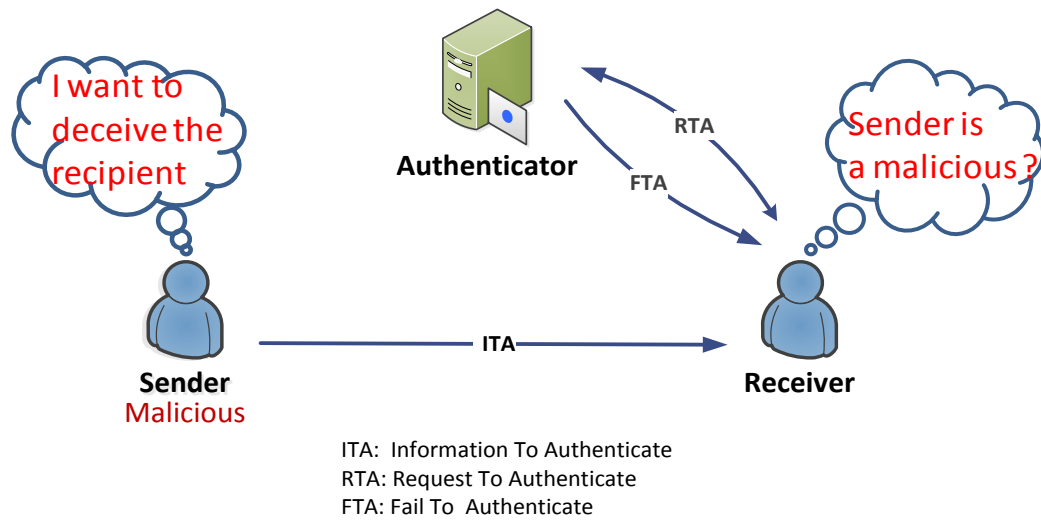


Figure 3-21: Failure of authentication process of the sender

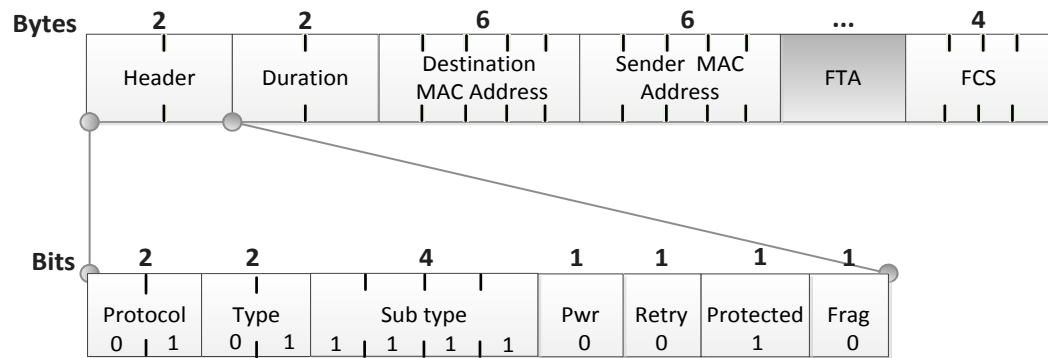


Figure 3-22: FTA frame format

## Design of the proposed MAC protocols with and without security

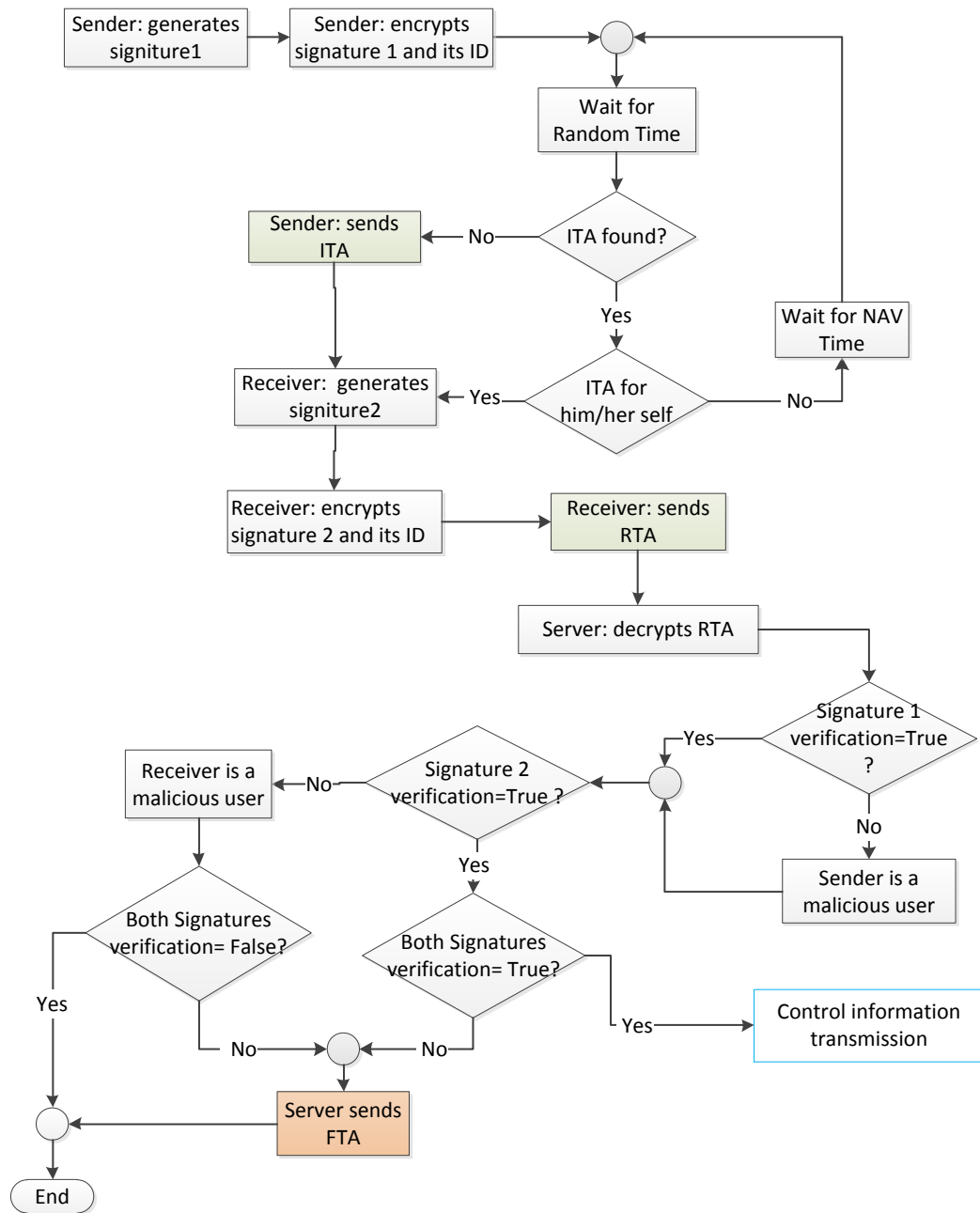


Figure 3-23: The authentication process flow chart in DSMCRN

### 3) Confirmation-Of-Authentication CUA1 & CUA2 frames:

Only after the successful verification of both CUs and generating a shared-key (group 3) for encryption and decryption procedure, the server launches two different unicast frames known as CUA1 and CUA2 for the sender and receiver CUs respectively. Each frame includes three pieces of encrypted information; *MAC-Keys*, *IDs* and *X-Y-Shared Key* belongs to Group 3 keys. The included

## Design of the proposed MAC protocols with and without security

information of the CUA1 which is intended to sender CU is encrypted using the sender's shared key, *X-S-Shared Key* (Group 2), that was generated previously by the sender in the IOR frame during the registration. Also for encrypting the content of the CUA2, the server encrypts the information using the receiver's shared key, *X-S-Shared Key* (Group 2), that was generated by the receiver during their registration. The format of the CUA1 and CUA2 are given in Figure 3-24 and Figure 3-25 respectively.

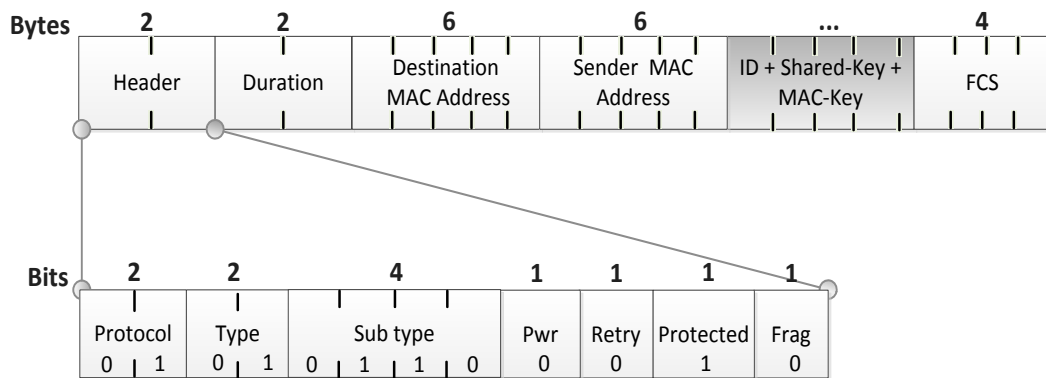


Figure 3-24: CUA1 frame format

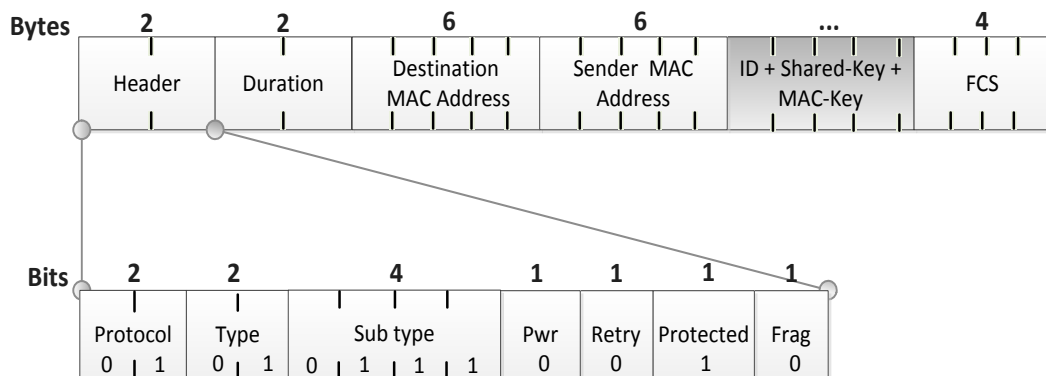


Figure 3-25: CUA2 frame format

When the sender received and then decrypted the CUA1 frame by the use of the same shared key (Group 2) they can verify the authenticity of the received message through using the MAC-Key algorithm. Thus, the comparison of the received and the new generated MAC-Key will confirm whether the received shared has been modified during the frame transmission or not. The same process applies to the receiver as soon as they received the CUA2 frame.

#### **4) Request-To-Send (RTS) frame:**

During the authentication process and before receiving both the CUA1 and CUA2, both the sender and receiver CUs sense the licensed channels to list the available channels that can be utilised for data transmission in the next phase. Therefore, after receiving the CUA1, the sender requires to launch an RTS unicast frame which includes both the authentic sensing results (Available/Free Channel List (FCL)) and a MAC-Key which is generated from applying both the received Shared-key (Group 3) and the FCL in the MAC algorithm. Therefore, both MAC-Key and the FCL are encrypted by applying the same shared key, *X-Y-Shared Key* (Group 3), and this is considered as a clear contribution point of this research since the encryption is essential to hide the FCL and SLDCH from both adversary users (external attackers) and other CUs (internal attackers), who aim to misbehave by switching to these channels and make them unavailable for both senders and receivers in CRNs and resulting in deteriorating the network performance through decreasing its throughput. Moreover, if the FCL is not encrypted then the malicious users can inject or modify the FCL which results in wrong decision is made by spectrum management to select the best channel for data transmission and this attack is recognised as Spectrum Sensing data manipulation/falsification attack that resulted from unauthentic sensing results. Thus, the attacker's aim is to give false observation information to the CUs in order to affect the communication process by launching DoS attack in terms of the available channel level or may to maximise his/her communication performance (selfish attack). Furthermore, not only the encryption mechanism is essentially considered in the RTS frame for securing the FCL but also MAC-Key for the attached FCL is generated in the sender side and then attached to the FCL for the encryption procedure. This significantly helps to authenticate the received information in the receiver side for the integrity assurance of the transmitted information. Thus, the format of the RTS frame is shown in Figure 3-26.

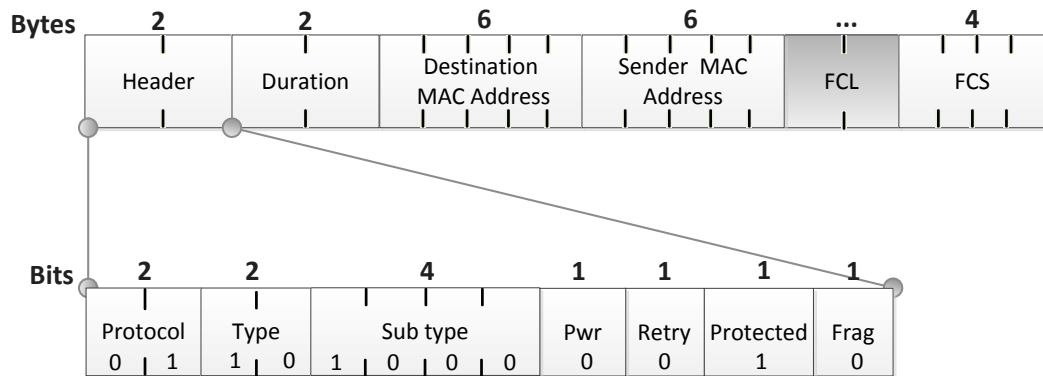


Figure 3-26: RTS frame format

As soon as the receiver received the RTS frame, he/she is able to decrypt it using the same shared-key (Group 3) which received from the CUA2 frame. Therefore, the CU requires ensuring the integrity of the received information through generating a new MAC-Key of the received FCL and the Group 3 shared-key. Once the integrity of the received information ensured then the receiver replies with the CTS frame as follow, otherwise the CU needs to reply with RES frame to leads to retransmitting the CTS frame again.

### 5) Clear-To-Send (CTS) frame:

As mentioned before in the RTS frame, both the sender and receiver perform the sensing mechanism to allocate the available licensed channel to transmit their data over. Based on the received FCL, the receiver needs to select the most reliable data channel based on the high availability from the FCL. Thus, the receiver launches a CTS unicast frame which is shown in Figure 3-27. The CTS frame includes both the Selected Data Channel (SLDCH) and a MAC-Key which is generated by running both SLDCH and the shared-key (Group 3) in the MAC algorithm. These two pieces of information are encrypted using the shared-key of group 3 (X-Y-Shared Key). Both the encryption and generated MAC-Key for the SLDCH are crucial in this stage to defend against a DoS attack, which can be resulted by launching a Spectrum Sensing Data manipulation/Falsification attack which was discussed in the RTS frame described earlier in this chapter.

## Design of the proposed MAC protocols with and without security

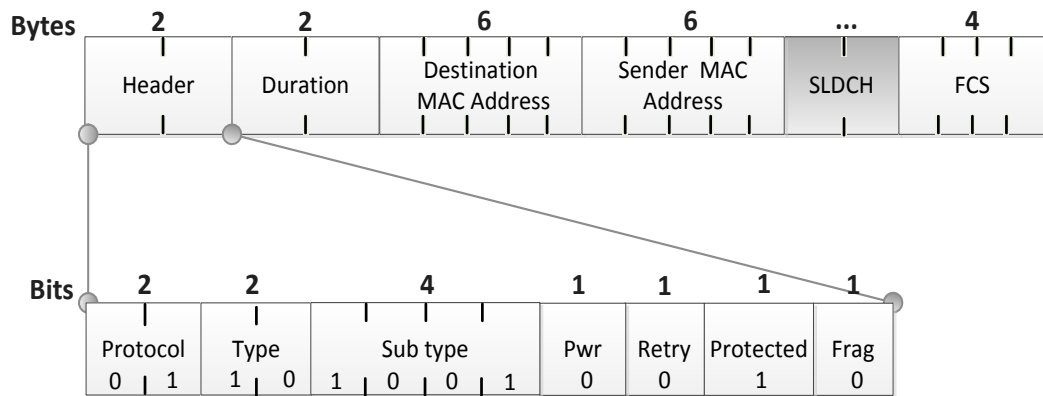


Figure 3-27: CTS frame format

On the sender side, the encrypted content of the received CTS frame can be decrypted through applying the same shared-key, X-Y-Shared Key (Group 3). Then the CU requires ensuring the integrity of the received encrypted SLDCH through generating a new MAC-Key and then compares it with the received MAC-Key. If these MAC-Keys are matched, then both CUs necessitate switching to the SLDCH for data transmission, otherwise, the sender sends RES frame to notify the receiver that the received information has been modified during the transmission and this leads to retransmitting the CTS frame again. Thus, the flow chart of the secure control frames transmissions is shown in Figure 3-28.

## Design of the proposed MAC protocols with and without security

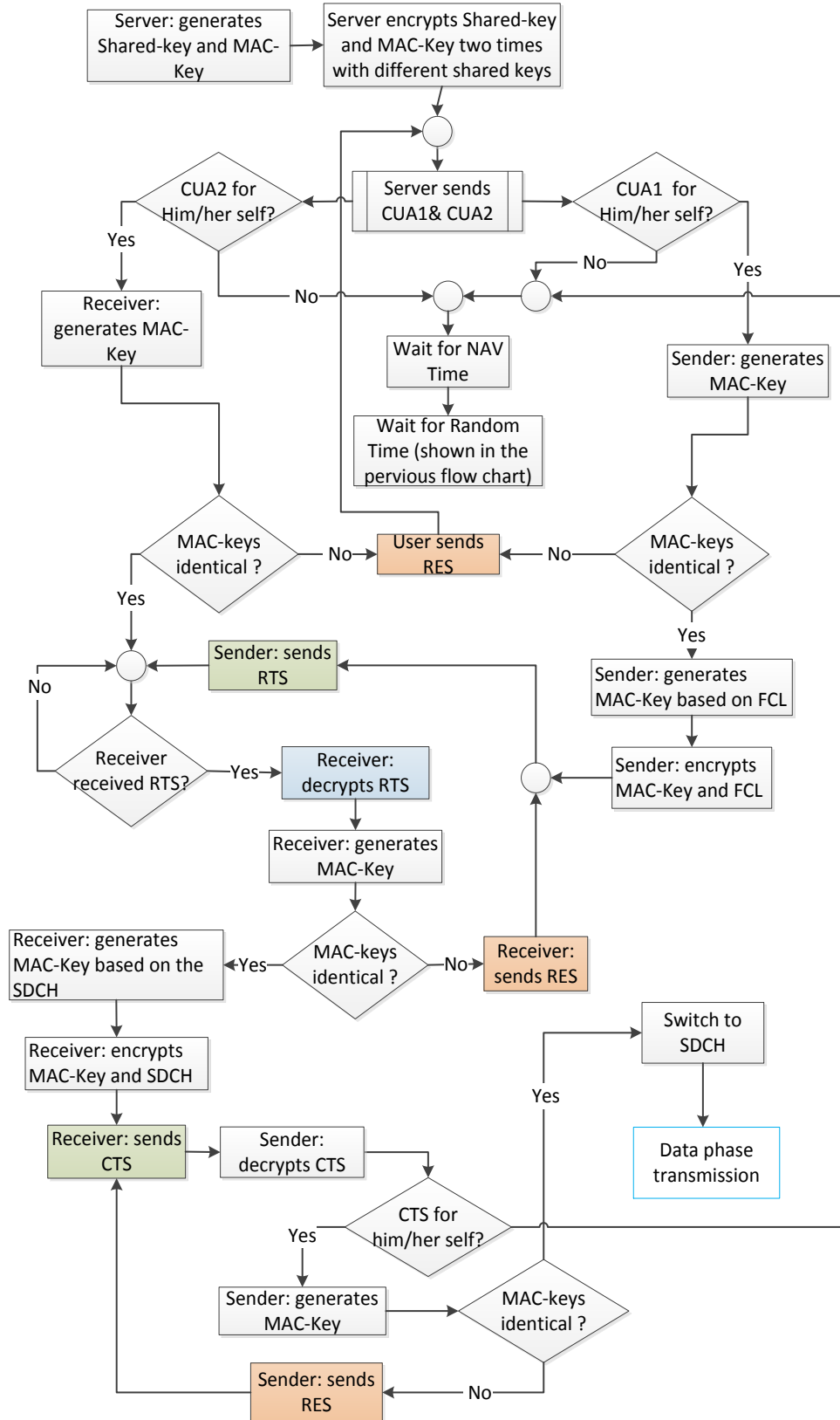


Figure 3-28: Secure control phase transmission in DSMCRN and SSMCRN

### 3.3.4.3. Data transmission phase of DSMCRN

Data and Acknowledgement frames are two main different frames, which are used in the current phase. Figure 3-29 demonstrates the data frames sequence between the sender and receiver CUs.

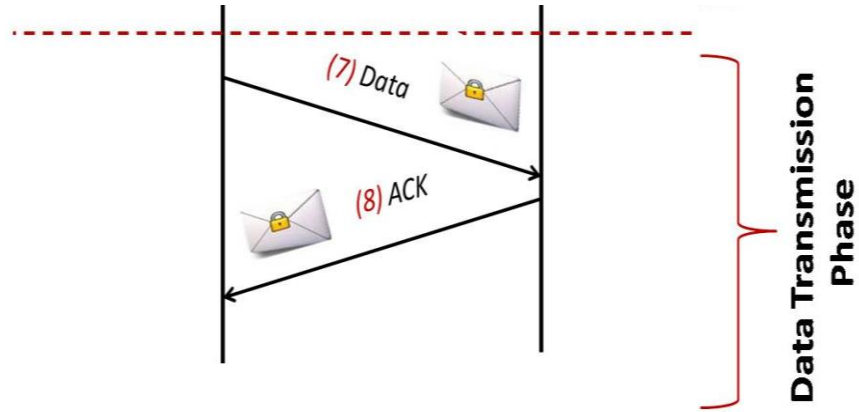


Figure 3-29: Data transmission phase

#### 1) Data frame

When both CUs are agreed and exchanged SLDCH over CTS frame successfully and then switched to the SLDCH, they can exchange both Data and Acknowledgement frames in unicast form over the SLDCH. Usually the data is transmitted in encrypted format uses the group 3 shared-key (X-Y-Shared Key) after the MAC-Key is generated and associated with the data for the integrity assurance. Thus, the receiver is able to decrypt the received information by using the same shared-key and then verify the data integrity through applying the same group 3 shared-key and the received data. This process indicates the secure data transmission and data confidentiality, which are considered as a clear contribution point of this research, since only the right legitimate intended receiver among other users, who either can be internal CUs (CUs attempt to misbehave) or external attackers, can decrypt and verify the integrity of the received data. The format of the data frame is shown in Figure 3-30.

## Design of the proposed MAC protocols with and without security

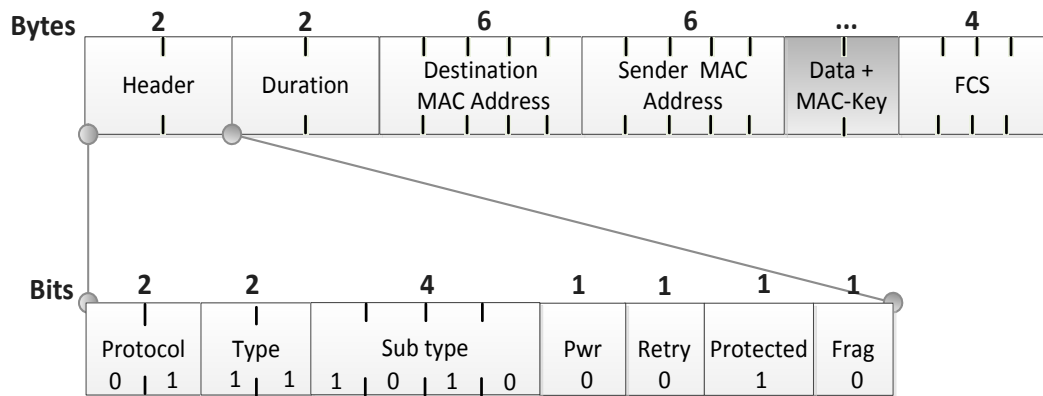


Figure 3-30: Data frame format

### 2) Acknowledgment frame

Once the integrity of the received data is ensured the ACK unicast frame is transmitted over the same channel. Only 1 byte is encrypted and known as ACK field in Figure 3-31 to confirm that only the intended receiver has transmitted the ACK frame. This encryption is important since the man in the middle attack can intercept the data transmission frame by causing modification or eavesdropping of the transmitted data and resulting in DoS attack. Therefore, only the encryption of the transmitted ACK frame is considered since it ensures and notifies the sender that the data has transmitted successfully to the intended CU and there is no need of ensuring the integrity of the encrypted information by the sender while the notification is done by the encryption procedure using the shared key is known to only a pair of CUs (sender and receiver). Therefore, once the ACK frame is received and then decrypted successfully by sender the entire process of the communication is ended and both CUs vacate the current licensed data channel.

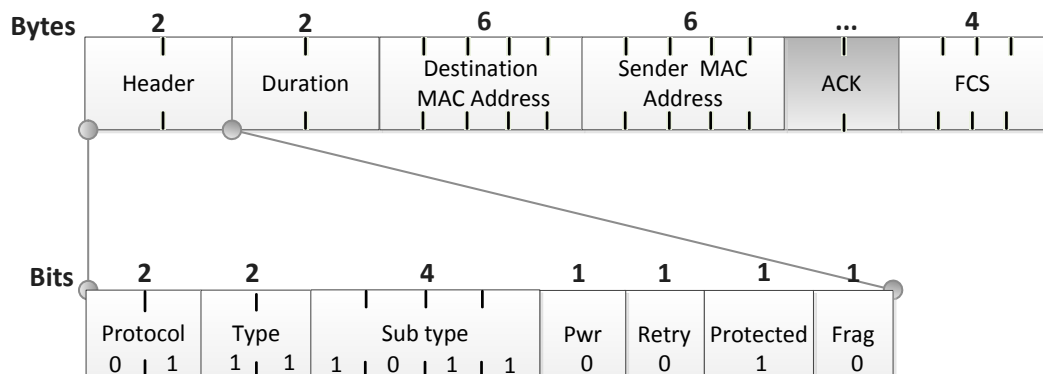


Figure 3-31: ACK frame format

## Design of the proposed MAC protocols with and without security

Note: Generally, the format of the RES frame remains same in all the protocols phases and is shown in Figure 3-32.

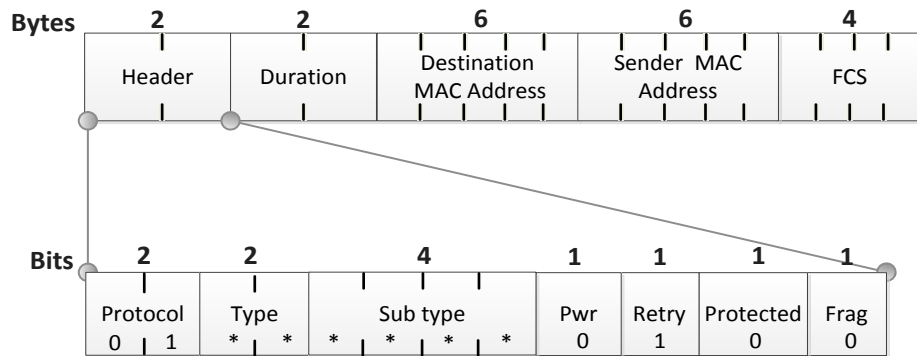


Figure 3-32: RES frame format

The flow chart of the data transmission process in both DSMCRN and SSMCRN protocols is shown in Figure 3-33.

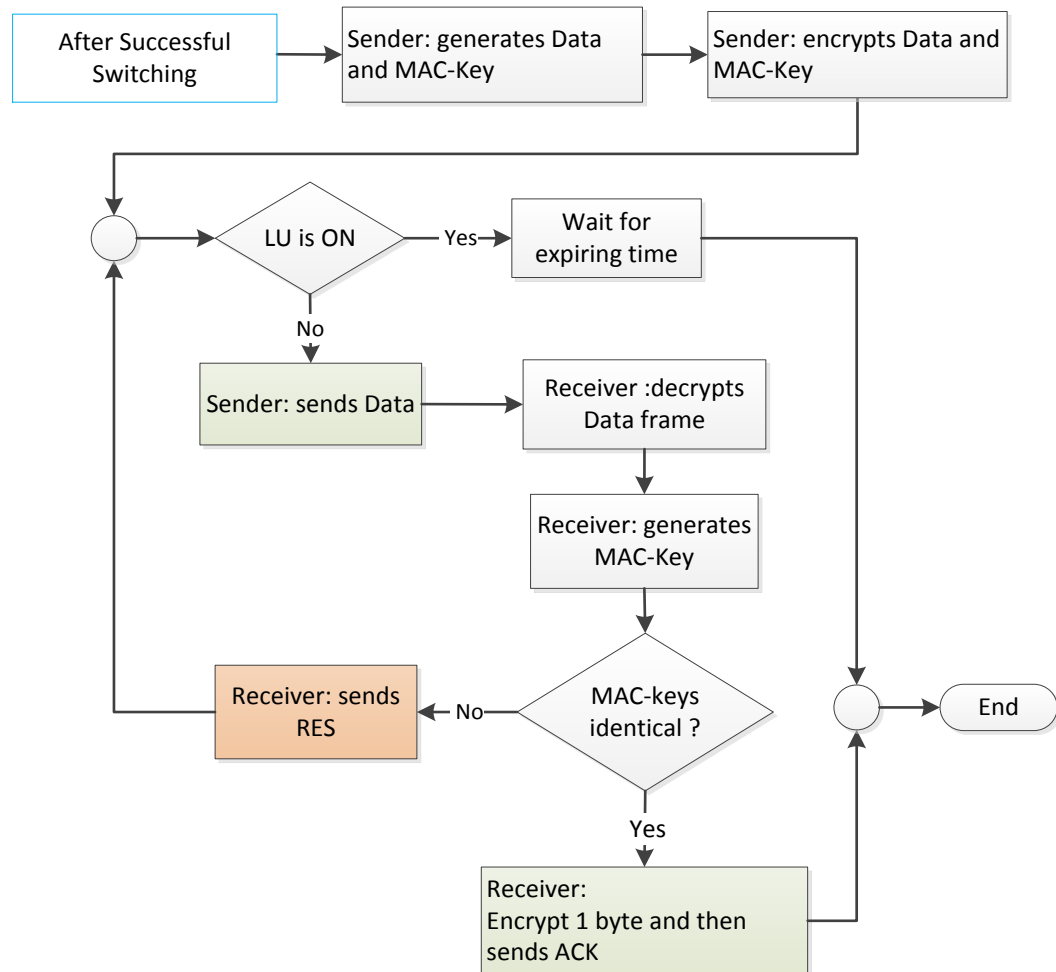


Figure 3-33: Data transmission phase flow chart in DSMCRN and SSMCRN

### 3.3.5. Shared-key based Secure MAC protocol for CRNs (SSMCRN)

The proposed DSMCRN protocol (Alhakami, et al., 2013) is analysed and addressed the security requirements to provide an authentication procedure among CUs using digital signature procedure with the assistance of asymmetric-key cryptography for detection mechanisms against malicious behaviour activities. However, it can also operate based upon symmetric-key cryptography for maintaining the same functionalities in terms of providing the necessary security features. The SSMCRN protocol (Alhakami, et al., 2014) maintains the same phases of the DSMCRN protocol in terms of registering the CUs' information to the dedicated authenticator server as a first stage, authenticating and exchanging the control information as the second stage and secure data transmission as last phase. However, its operation in addressing the authentication and CUs validation is different comparing to DSMCRN because of a shared key is used among the registered CUs instead of having an asymmetric key to generate a digital signature for authentication purpose. Table 3-4 demonstrates where the symmetric and asymmetric key algorithms are used in the SSMCRN.

Table 3-4: Encryption methods used in SSMCRN

Encryption Method	Type of encryption	Keys size	SSMCRN Phases					
			Registration		Control			Data
			Server to Node	Node to Server	Node to Node	Node to Server	Server to Node	Node to Node
RSA	Asymmetric Cryptography	1024		√				
AES	Symmetric Cryptography	128	√		√	√	√	√

The SSMCRN protocol consists of three sequential phases; registration, control and data phases that each performs a specific task to fulfil the secure data transmission among only the authorised CU recipients (Alhakami, et al., 2014). Thus, the phases of the SSMCRN operation are explained as follows:

### 3.3.5.1. Registration phase of SSMCRN

The registration phase of the SSMCRN protocol follows the same process of the registration process in DSMCRN in terms of obtaining the authorised security information access to join the network. Also, this is achieved through transmitting four frames; RTR, CTR, IOR and COR frames between both the CU and the dedicated server. Therefore, RTR and CTR frames are discussed in details in section 3.3.4.1 while the IOR and COR frames are explained as follow:

#### 1) Information-of-Registration (IOR) frame:

This frame is similar to the IOR frame in DSMCRN in terms of its unicast transmission to the server in encrypted format with the use of the server's public-key and decryption procedure by the server which applies its private key. However, the main difference is in the content of the encrypted and transmitted information which only includes the user Shared Key, ID and MAC-Key. The format of the IOR frame of the SSMCRN protocol is shown in Figure 3-34 below.

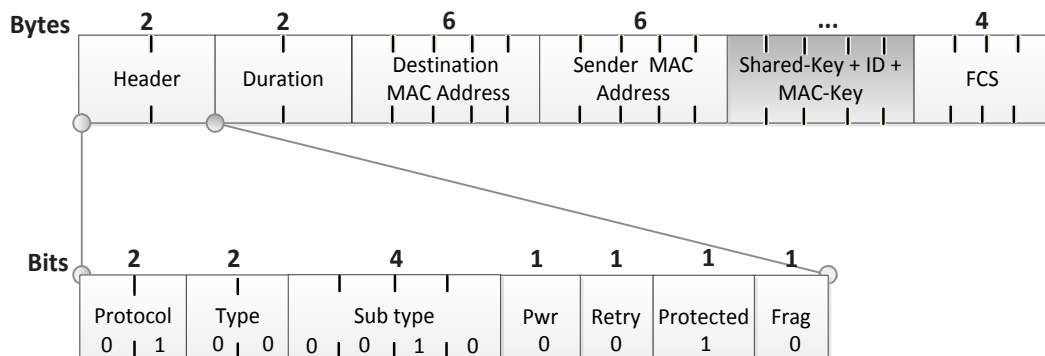


Figure 3-34: IOR frame format in SSMCRN

#### 2) Confirmation-Of-Registration (COR) frame:

This frame is similar to the COR frame in terms of its unicast transmission to the CU and both the encryption and decryption procedures in DSMCRN. However, it is different in the content of the encrypted information, which includes the network's shared key and an ID generated for the registered CUs as well as the MAC Key for the integrity of this information. The format of the COR frame is shown in Figure 3-35.

## Design of the proposed MAC protocols with and without security

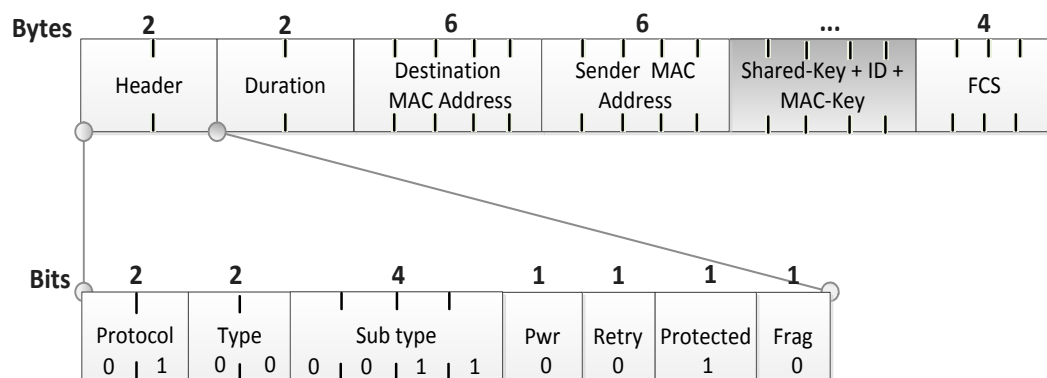


Figure 3-35: COR frame format in SSMCRN

The flowchart of the entire registration process of the SSMCRN protocol is shown in Figure 3-36.

## Design of the proposed MAC protocols with and without security

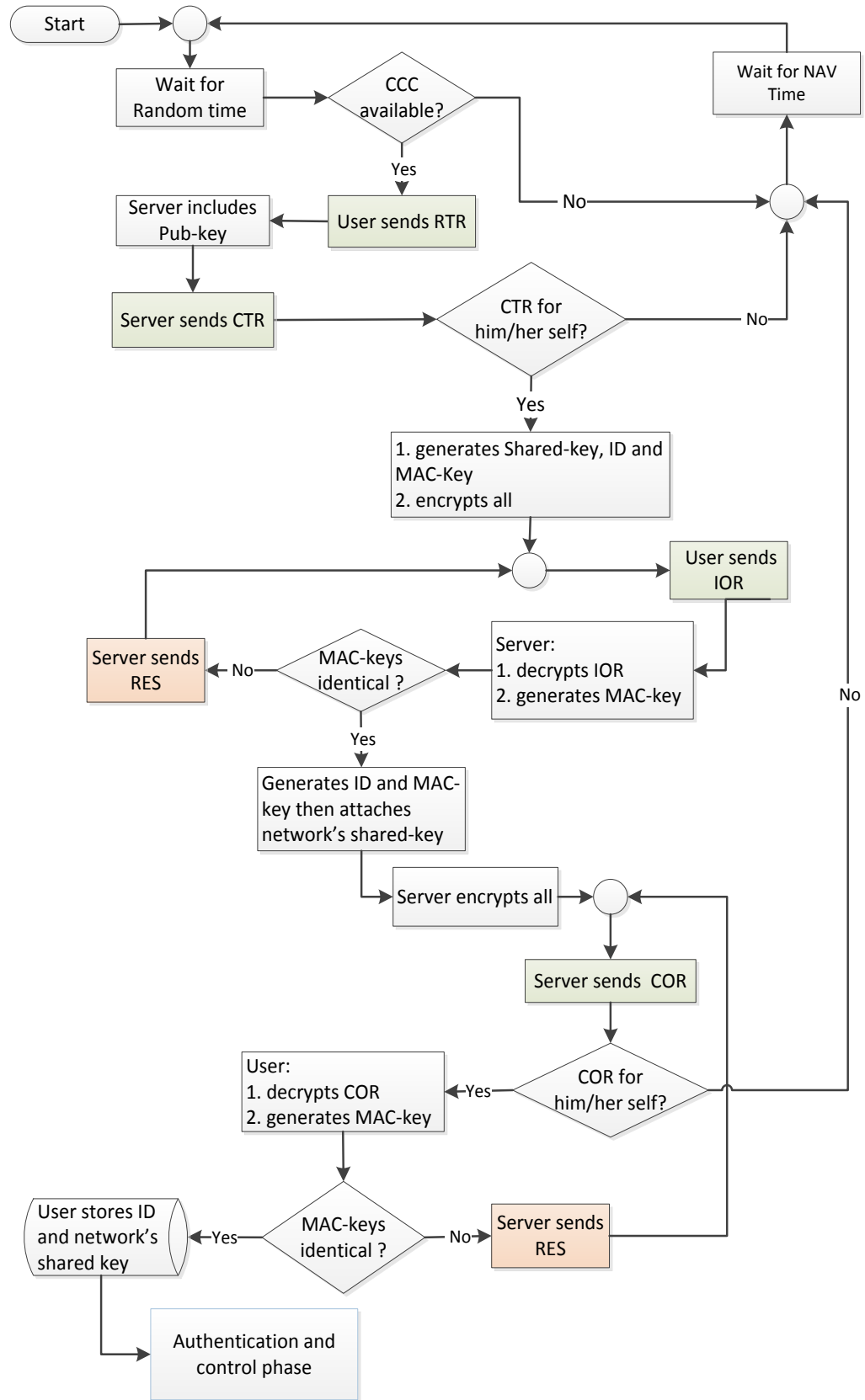


Figure 3-36: Flow chart of the registration process in SSMCRN

### 3.3.5.2. Authentication and control phase of SSMCRN

This phase focuses on achieving the same security and control information objectives of the authentication and control phase in DSMCRN. However, the main difference is the authentication process, which is based upon two different sequence steps; pre-authentication on the CU level and primary-authentication on the server in SSMCRN instead of authenticating CUs through verifying digital signatures in the server in DSMCRN. The frames sequence for the authentication and control phase remain same in both protocols and was shown in Figure 3-18 in section 3.3.4.2.

#### 1) Information-To-Authenticate (ITA) frame

Before a sender tries to communicate with the destination CU, it firstly generates MAC-key through running its ID on the MAC algorithm. The sender encrypts both the ID and MAC-Key using the Network shared key (group 1) that received in COR frame. This encrypted information is transmitted to the intended destination within an ITA unicast frame over the CCC. The recipient needs to pre-authenticate the sender through decrypts the received information. If the receiver CU is able to decrypt it, then this indicates that the sender is a valid user from the receiver point of view. By doing this the recipient involves in protecting the server from any invalid transmitted frame that indirectly would increase the chance of launching a DoS attack by the attacker. The frame format of the ITA in SSMCRN is shown in Figure 3-37.

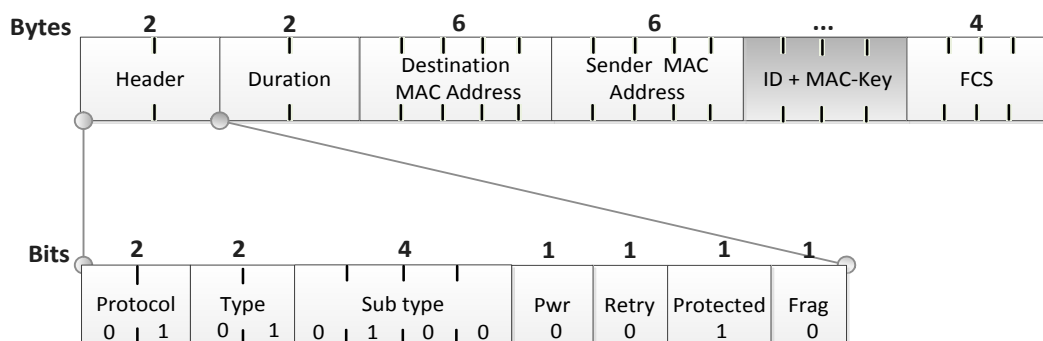


Figure 3-37: ITA frame format in SSMCRN

## 2) Request-To-Authenticate (RTA) frame

When the ITA frame received and decrypted successfully, the receiver does the same process of generating MAC-Key through running its ID on the MAC algorithm. Then the receiver encrypts its ID, the generated MAC-Key and the sender information (sender's ID and MAC-Key). This encrypted information is transmitted to the server within an RTA unicast frame as shown in Figure 3-38. Therefore, the authentication procedure is mainly based on having the network shared-key (group 1) and the user ID for ensuring the information belongs to a certain registered user.

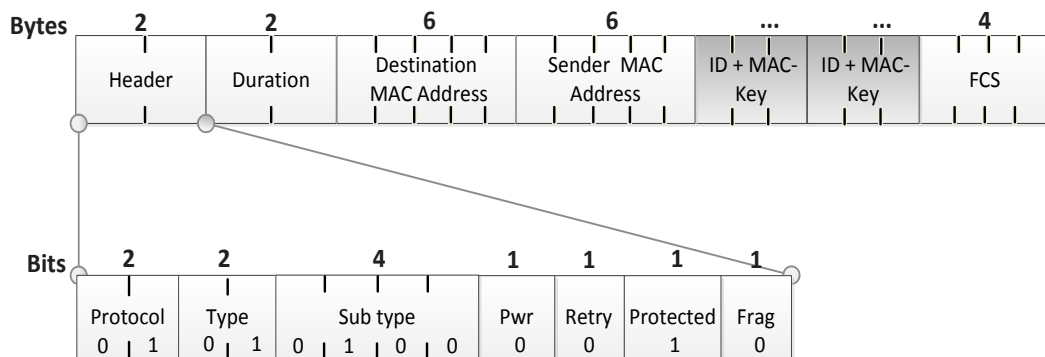


Figure 3-38: RTA frame format in SSMCRN

## 3) Confirmation of User's authentication 1&2 (CUA1&2)

These frames are explained in details in CUA1 and CUA2 frames of the Authentication and Control information phase of the DSMCRN in section 3.3.4.2.

## 4) Request to send (RTS)

RTS frame is explained in details in the Authentication and Control information phase of DSMCRN in section 3.3.4.2.

## 5) Clear to send (CTS)

CTS frame is explained in details in the Authentication and Control information phase of DSMCRN in section 3.3.4.2.

The authentication phase of the SSMCRN flow chart is shown in Figure 3-39.

### 3.3.5.3. Data transmission phase of SSMCRN

This phase includes both Data and ACK frames, which are explained in details in Data transmission phase in section 3.3.4.3.

## Design of the proposed MAC protocols with and without security

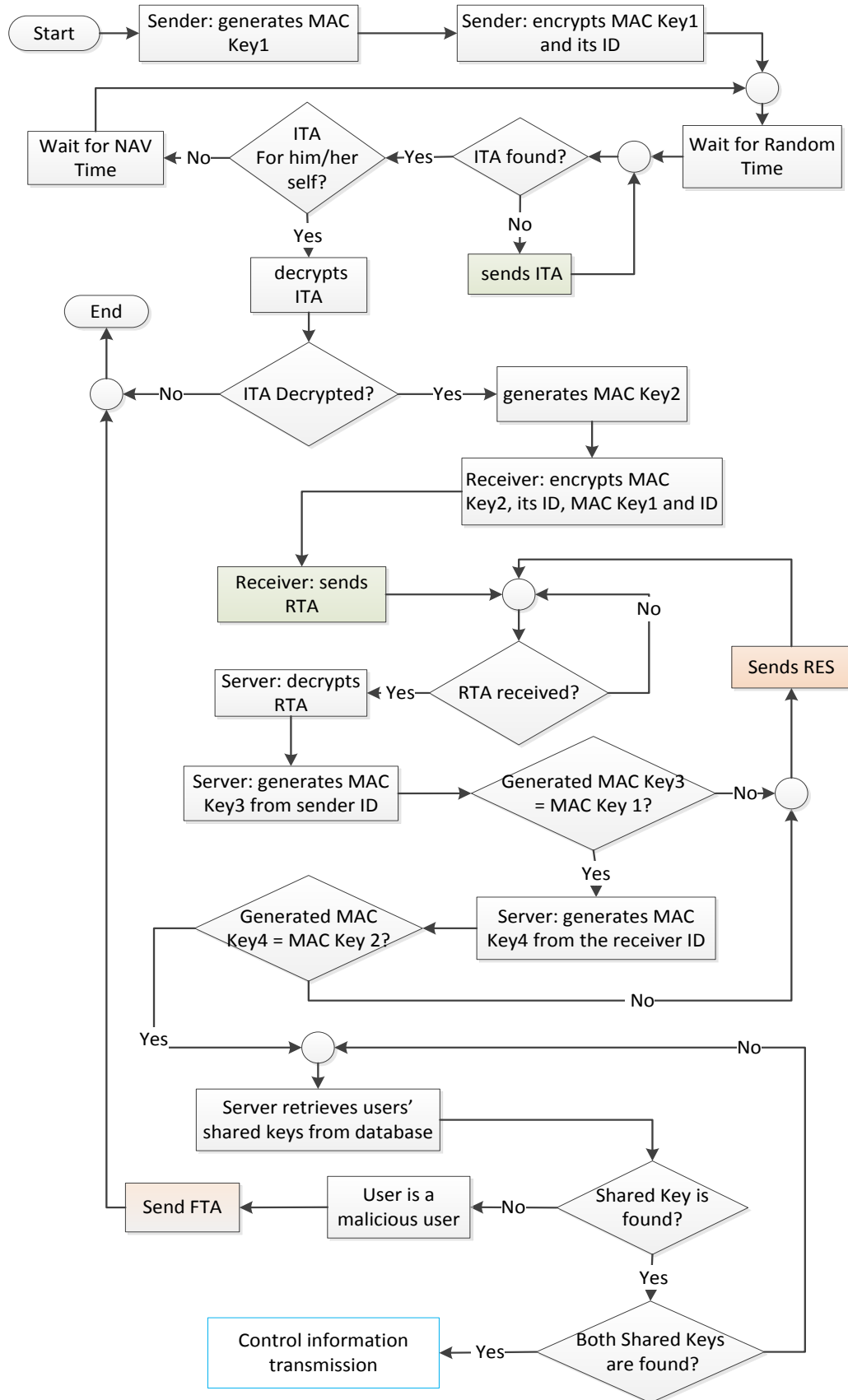


Figure 3-39: Authentication process flowchart in SSMCRN

### 3.3.6. Analysis of the DSMCRN and SSMCRN protocols using BAN logic

This section focuses on analysing and describing the proposed DSMCRN and SSMCRN protocols using a formal logic method called BAN logic. Therefore, the details of how messages sequence of the three phases of the proposed protocols accomplishes with BAN logic and given in the next sections.

#### 3.3.6.1. What is the BAN logic?

In order to analysis any protocol for communication usually there are two different approaches which are simulation technique using tools such as NS2, OPNET Modular, testbed or any programming language like Java or C++ while the second approach using a formal logic method such as BAN (Burrows, et al., 1990), GNY and Belief (David, 1999). Therefore, the BAN logic method is used for analysis and validating the proposed DSMCRN and SSMCRN protocols. The significant motivation of using this method among the others is because it is less complexity comparing to GNY and Belief logics in terms of the understanding. Moreover, it is used as an initial stage to validate the protocol in terms of meeting the communication and the security requirements before the simulation task takes place. Figure 3-40 shows different approaches of protocol analysis.

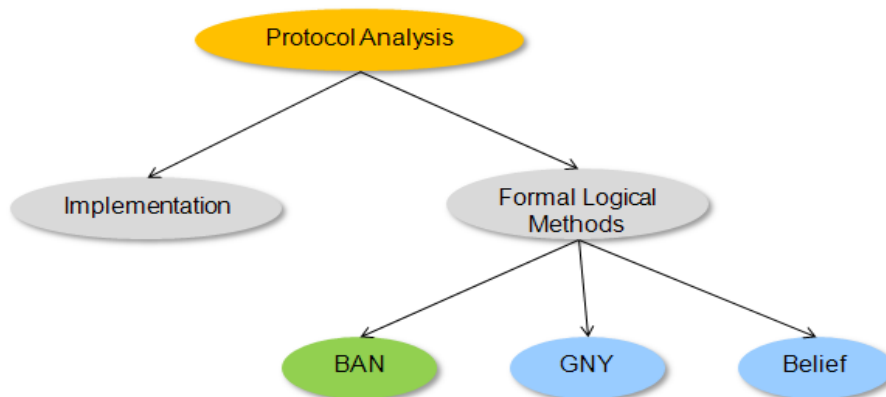


Figure 3-40: Protocol analysis methods

Burrows-Abadi-Needham (BAN) logic (Burrows, et al., 1990) provides a variety of symbols that are used for cryptographic schemes for both symmetric and asymmetric key exchange. Thus, the use of this logic is applicable to analyses the

proposed DSMCRN and SSMCRN protocols since they are designed and involve symmetric and asymmetric techniques. Therefore, Table 3-5 below gives the BAN logic symbols that are used in the current protocols.

Table 3-5: The BAN logic symbols

Symbol	Usage
$X \mid\Rightarrow Y$	X Controls Y
$X \mid\equiv Y$	X Believes Y
$X \mid\sim Y$	X Sends Y
$\overset{K}{\mid\rightarrow} X$	Public Key of X
$K^{-1}$	Private Key (Secret)
$X \overset{K}{\longleftrightarrow} Y$	X and Y shared a secret key
$X \triangleleft M$	X Believes (Sees) M

### 3.3.6.2. BAN logic messages meaning rules

The BAN logic rules are represented in formulas based on the given symbols in Table 3-5 and each has been described in details.

$$1) \text{ Rule 1 } \frac{P \mid\equiv Q \overset{K}{\longleftrightarrow} P, P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

When node P sees the message that is encrypted with the secret key of both P and Q, then node P believes the node Q has transmitted the message since the shared-key is only recognized for those users who can produce this message. Thus, the proposed protocols meet the current rule since the server authenticate and grant a shared key for both the sender and receivers.

$$2) \text{ Rule 2 } \frac{P \mid\equiv \overset{K}{\mid\rightarrow} Q, P \triangleleft \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X}$$

This rule is similar to the previous rule, but as soon as the asymmetric key has two main parts which are the public and private keys, with node P sees the message that is encrypted with the private Key of node Q. Then node P believes Q has sent the message which can only be produced by Q. This rule is met in the DSMCRN protocol analysis since the implication of digital signature is applied.

$$3) \text{ Rule 3 } \frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

If P believes Q controls X then P believes Q believes X. This resulted in P believes X. This rule achieved in all the messages of the DSMCRN and SSMCRN protocols since the MAC-Key is provided with the transmitted messages for achieving the integrity.

### 3.3.6.3. Established initial assumptions for the proposed DSMCRN and SSMCRN

According to the assumptions that were highlighted in section 3.1, five of these assumptions related to the security are described in Table 3-6 to initiate and build sequence processes for analysing the proposed protocols whereas Table 3-7 lists the variables that are used.

Table 3-6: The assumptions that are used in DSMCRN and SSMCRN

Assumptions	Explanation
$S \models N \xrightarrow{K} N, P_{ID}, Q_{ID}$	Server controls the network access information which is shared-key and CUs' IDs for registered CUs
$P \models S \models \xrightarrow{K} Q$	Node P Believes the server controls the public-key of Q once it is registered
$Q \models S \models \xrightarrow{K} P$	Node Q believes the server controls the public-key of P once it is registered
$P \models S \models, \sim P \xrightarrow{K} Q$	Node P believes the server controls the communication and provides a shared-key for control and data frames exchange after the successful authentication
$Q \models S \models, \sim P \xrightarrow{K} Q$	Node Q believes the server controls the communication and provides a shared-key for data exchange after the successful authentication

Table 3-7: The variables that are used in DSMCRN and SSMCRN

Variables	Description
$X_P, X_Q$	Node's P or Q Message
$MX_{MAC}$	Message X MAC Key, which is generated the attached information of message X

### 3.3.6.4. DSMCRN and SSMCRN protocols phases' analysis

Based on the previous assumptions in Table 3-6 the protocols phases are analysed as follows:

### 1) Registration phase analysis

The analysis and descriptions below are for the sequence messages' transmission between a sender (P) that requests the server (S) to register and obtain the required information to join the network in DSMCRN and SSMCRN.

In DSMCRN:

Message (1)  $P \rightarrow \text{Server}$        $P \sim \{X\}$       (Step 1.1)

Message (2)  $\text{Server} \rightarrow P$        $S \sim \{|\xrightarrow{K} S\}$       (Step 1.2)

Message (3)  $P \rightarrow \text{Server}$        $P \sim \{|\xrightarrow{K} P, P \xleftarrow{K} S, P_{ID}, M3_{MAC}\}_{|\xrightarrow{K} S}$   
(Step 1.3.1)

However, in SSMCRN (Step 1.1) and (Step 1.2) remain same while (Step 1.3.1) and (Step 1.4.1) are different and provided in (Step 1.3.2) and (Step 1.4.2) respectively.

Message (3)  $P \rightarrow \text{Server}$        $P \sim \{P \xleftarrow{K} S, P_{ID}, M3_{MAC}\}_{|\xrightarrow{K} S}$  (Step 1.3.2)

The required information about the registration is provided in (Step 1.3.1) and (Step 1.3.2) which they transmitted to the server in encrypted format using the  $|\xrightarrow{K} \text{Server}$ . Here only the server can decrypt and see the content of receiving message 3 after applying its private key SK as shown in the following (Step 1.4.1) and (Step 1.4.2). Since these keys are two parts as a pair which is generated from asymmetric key algorithms and the private key, which is used to decrypt the message 3, is only known to the server.

$$\{ \{ |\xrightarrow{K} P, P \xleftarrow{K} S, P_{ID}, M3_{MAC} \}_{|\xrightarrow{K} S} \}^{SK} \quad (\text{Step 1.4.1})$$

$$\{ \{ P \xleftarrow{K} S, P_{ID}, M3_{MAC} \}_{|\xrightarrow{K} S} \}^{SK} \quad (\text{Step 1.4.2})$$

The message 4 in DSMCRN is analysed as follows:

Message (4)  $S \rightarrow P$        $S \sim \{P_{ID}, M3_{MAC}\}_{P \xleftarrow{K} S}$  (Step 1.5.1)

$P \triangleleft \{P_{ID}, M3_{MAC}\}_{P \xleftarrow{K} S}$  (Step 1.6.1)

$\{ \{ P_{ID}, M3_{MAC} \}_{P \xleftarrow{K} S} \}^{P \xleftarrow{K} S}$  (Step 1.7.1)

However, the message 4 in SSMCRN is shown as follows:

$$S \sim \{N \xrightarrow{K} N, P_{ID}, M3_{MAC}\}_{P \xrightarrow{K} S} \quad (Step\ 1.5.2)$$

$$P \triangleleft \{N \xrightarrow{K} N, P_{ID}, M3_{MAC}\}_{P \xrightarrow{K} S} \quad (Step\ 1.6.2)$$

$$\{\{N \xrightarrow{K} N, P_{ID}, M3_{MAC}\}_{P \xrightarrow{K} S}\}^{P \xrightarrow{K} S} \quad (Step\ 1.7.2)$$

Now node P has been successfully registered its information on the server and granted an ID which is the authorised access to join the network in DSMCRN and network shared-key and  $N_{ID}$  in SSMCRN. These are encrypted and transmitted securely with the  $P \xrightarrow{K} S$  as it is only shared between P and S.

## 2) Authentication/Control information phase analysis

This part introduces three nodes are involved within the communication and identified as P, Q and S for the authentication and the secure transmission of the control information. Both P and Q are assumed completed the registration phase.

$$\text{Message (5) } P \rightarrow Q \quad \{P_{ID}\}^{PK} = P_{sig} \quad (Step\ 5.1.1)$$

The P applies its private key PK to encrypt the  $P_{ID}$  and this resulting in generating a hash value recognised as  $P_{sig}$ .

$$P \sim \{P_{sig}, P_{ID}\}_{| \xrightarrow{K} S} \quad (Step\ 5.2.1)$$

Both  $P_{sig}$  and  $P_{ID}$  are appended and then encrypted with  $| \rightarrow S$  to ensure the confidentiality of the transmitted message.

$$Q \triangleleft \{P_{sig}, P_{ID}\}_{| \xrightarrow{K} S} \quad (Step\ 5.3.1)$$

Here Q has nothing to do with message 5 since it can only be decrypted with the server's private key. However, this message is used to establish the link of the communication with Q. Thus, Q has been notified to be involved within the communication, therefore it necessitate to send message 6.

However, in SSMCRN, P sends  $P_{ID}$  as shown in (Step 5.1.2) which is encrypted with the network shared key that was obtained in (Step 1.7.2 in message 4). Only the registered and authorised recipient users can decrypt the current message.

$$P \mid \sim \{P_{ID}, M5_{MAC}\}_{N \xleftarrow{K} N} \quad (\text{Step 5.1.2})$$

$$Q \triangleleft \{\{P_{ID}, M5_{MAC}\}_{N \xleftarrow{K} N}\}^{N \xleftarrow{K} N} \quad (\text{Step 5.2.2})$$

Message (6)  $Q \rightarrow S$ : In DSMCRN, node Q (destination) generates a digital signature as shown in the following step:

$$\{Q_{ID}\}^{QK} = Q_{sig} \quad (\text{Step 6.1.1})$$

Both  $Q_{sig}$  and  $Q_{ID}$  are appended and then encrypted with  $\mid \rightarrow S$  for achieving the confidentiality of the transmitted message.

$$Q \mid \sim \left\{ \left\{ P_{sig}, P_{ID} \right\}_{\mid \xrightarrow{K} S} \left\{ Q_{sig}, Q_{ID} \right\}_{\mid \xrightarrow{K} S} \right\} \quad (\text{Step 6.2.1})$$

$$S \triangleleft Q \mid \sim \left\{ \left\{ P_{sig}, P_{ID} \right\}_{\mid \xrightarrow{K} S} \left\{ Q_{sig}, Q_{ID} \right\}_{\mid \xrightarrow{K} S} \right\} \quad (\text{Step 6.3.1})$$

$$\left\{ \left\{ P_{sig}, P_{ID} \right\}_{\mid \xrightarrow{K} S} \right\}^{SK} \text{ and } \left\{ \left\{ Q_{sig}, Q_{ID} \right\}_{\mid \xrightarrow{K} S} \right\}^{SK} \quad (\text{Step 6.4.1})$$

The two parts of message 6 have been decrypted by the server  $SK^{-1}$  as shown in (Step 6.4), then based on the attached IDs for P and Q the server retrieves both  $\mid \rightarrow P$  and  $\mid \rightarrow Q$  from the database.

$$\left\{ P_{sig} \right\}_{\mid \xrightarrow{K} S} \text{ and } \left\{ Q_{sig} \right\}_{\mid \xrightarrow{K} S} \quad (\text{Step 6.5.1})$$

Thus, based on rule 2 the authentication process of both users are completed after applying the (Step 6.5.1) since the each pair of asymmetric key is applied correctly to validate each signature.

However, the message 6 of SSMCRN is different and analysed as follows:

$$Q \mid \sim \{P_{ID}, Q_{ID}, M5_{MAC}\}_{N \xleftarrow{K} N} \quad (\text{Step 6.1.2})$$

$$S \triangleleft \{P_{ID}, Q_{ID}, M5_{MAC}\}_{N \xleftarrow{K} N} \quad (\text{Step 6.2.2})$$

$$\left\{ \{P_{ID}, Q_{ID}, M5_{MAC}\}_{N \xleftarrow{K} N} \right\}^{N \xleftarrow{K} N} \quad (\text{Step 6.3.2})$$

The authentication of the P and Q in SSMCRN is based on the decryption of the message 6 also based on the attached IDs within the message to retrieve the

## Design of the proposed MAC protocols with and without security

$P \xleftarrow{K} S$  for user P and  $Q \xleftarrow{K} S$  for user Q and these shared keys will be used for securing messages 7 and 8 in the next steps.

Message (7)  $S \rightarrow P$ :  $S \sim \{P \xleftarrow{K} Q, PQ_{ID}, M7_{MAC}\}_{P \xleftarrow{K} S}$  (Step 7.1)

$P \triangleleft \{P \xleftarrow{K} Q, PQ_{ID}, M7_{MAC}\}_{P \xleftarrow{K} S}$  (Step 7.2)

$\left\{ \left\{ P \xleftarrow{K} Q, PQ_{ID}, M7_{MAC} \right\}_{P \xleftarrow{K} S} \right\}_{P \xleftarrow{K} S}$  (Step 7.3)

Message (8)  $S \rightarrow Q$ :  $S \sim \{P \xleftarrow{K} Q, PQ_{ID}, M8_{MAC}\}_{Q \xleftarrow{K} S}$  (Step 8.1)

$Q \triangleleft S \sim \{P \xleftarrow{K} Q, PQ_{ID}, M8_{MAC}\}_{Q \xleftarrow{K} S}$  (Step 8.2)

$\left\{ \left\{ P \xleftarrow{K} Q, PQ_{ID}, M8_{MAC} \right\}_{Q \xleftarrow{K} S} \right\}_{Q \xleftarrow{K} S}$  (Step 8.3)

After a successful authentication of both P and Q the server sends two different frames include Q and S shared-key and  $PQ_{ID}$  as shown in (Step 7.1) and (Step 8.1). This information is encrypted with different shared-keys that are shared between users and server while the decryptions are represented in (Step 7.3) and (Step 8.1).

Message (9)  $P \rightarrow Q$ :  $P \sim \{FCL, M9_{MAC}\}_{P \xleftarrow{K} Q}$  (Step 9.1)

$Q \triangleleft P \sim \{FCL, M9_{MAC}\}_{P \xleftarrow{K} Q}$  (Step 9.2)

$\left\{ \left\{ FCL, M9_{MAC} \right\}_{P \xleftarrow{K} Q} \right\}_{P \xleftarrow{K} Q}$  (Step 9.3)

Message (10)  $Q \rightarrow P$ :  $Q \sim \{SLDCH, M10_{MAC}\}_{P \xleftarrow{K} Q}$  (Step 10.1)

$P \triangleleft Q \sim \{SLDCH, M10_{MAC}\}_{P \xleftarrow{K} Q}$  (Step 10.2)

$\left\{ \left\{ SLDCH, M10_{MAC} \right\}_{P \xleftarrow{K} Q} \right\}_{P \xleftarrow{K} Q}$  (Step 10.3)

Based on the successful secure exchange of FCL and SLDCH in (Step 9.1) and (Step 10.1), both P and Q agreed about the SLDCH to transmit X over. Thus the next step analysis the secure X between those users.

### 3) Secure data transmission analysis

This stage demonstrates the secure data transmission between the nodes P and Q. Based on (Step 7.1) and (Step 8.1) both users received  $P \xleftrightarrow{K} Q$  that is significantly used in (Step 11.1) to secure the data (X) during its transmission between only P and Q. Since  $P \xleftrightarrow{K} Q$  is only known to this pair of users, the transmitted X can not be decrypted by other users as the required key is not recognised.

$$\text{Message (11) } P \rightarrow Q: P \sim \{X, M11_{MAC}\}_{P \xleftrightarrow{K} Q} \quad (\text{Step 11.1})$$

$$Q \triangleleft P \sim \{X, M11_{MAC}\}_{P \xleftrightarrow{K} Q} \quad (\text{Step 11.2})$$

$$\left\{ \{X, M11_{MAC}\}_{P \xleftrightarrow{K} Q} \right\}_{P \xleftrightarrow{K} Q} \quad (\text{Step 11.3})$$

$$\text{Message (12) } Q \rightarrow P: Q \sim \{ACK\}_{P \xleftrightarrow{K} Q} \quad (\text{Step 12.1})$$

$$P \triangleleft Q \sim \{ACK\}_{P \xleftrightarrow{K} Q} \quad (\text{Step 12.2})$$

$$\left\{ \{ACK\}_{P \xleftrightarrow{K} Q} \right\}_{P \xleftrightarrow{K} Q} \quad (\text{Step 12.3})$$

### 3.3.6.5. Security Analysis

As long as the BAN logic method is employed to determine whether or not the security protocols achieve the authentication requirement (Burrows, et al., 1990), it is used to determine both the DSMCRN and SSMCRN protocols' function of authentication and verifying the secure transmission between the sender and receiver. The evaluation capability of these protocols can therefore be obtained from an examination of the following areas:

#### 1) Mutual Authentication

The authentication task is significantly considered in both protocols through achieving the authorised access information belong to each CU. Thus, it is based on the digital signature technique in the DSMCRN and both CUs' shared-keys and network key to verify the sender and receiver on the server side before the control information transmission between those CUs is initiated. The server

therefore does the authentication process and then informs both the sender and receiver about the status of the authentication through grant them with a unique shared-key allocated for this pair of CUs. The obtained key indicates the success of the authentication process and leads both CUs continue with their communication.

### **2) Secure Communication**

Both symmetric and asymmetric cryptography techniques are considered and involved for secure message transmissions in both protocols. Thus, all the transmitted messages of the three phases are encrypted with the use of whether symmetric or asymmetric keys based on their demands. However, only the RTR and CTR frames which do not require encryption since it initiates the process of communication for mainly requesting the server to send its public-key. For more detail, see sections 3.3.4.1 and 3.3.5.1 in DSMCRN and SSMCRN respectively.

### **3.3.6.6. Vulnerability Analysis**

The current protocols have been investigated from different sides of the security perspective in order to ensure that they are able to operate against a range of different potential attacks that can be launched against CRNs. The following attacks will therefore be explained in terms of their security relationship with the current protocols.

#### **1) Replay and Masquerading Attacks**

In the messages 4, 5, 6, 7, and 8 of the DSMCRN and SSMCRN protocols, an attacker cannot escalate and impersonate the legitimate CUs information and privileges for gaining authorised access since the encryption mechanisms were involved and performed against the replay and masquerading attacks. For example in message 5 and 6 of DSMCRN, the senders and receivers necessitate producing and attaching their digital signatures within the transmitted encrypted messages. Any node requires signing their ID for producing a unique hash value based on both the private-key and the associated ID for authentication purposes. This results in generating digital signatures being attached to the transmitted encrypted messages as shown in (*Step 5.1.1*) and (*Step 6.1.1*). Thus, the attacker's goals of

obtaining the CUs identities cannot be achieved since the asymmetric key encryption algorithm is applied to secure the sender's information transmission. Moreover, the digital signature implication in these two steps also provides non-repudiation security factor in which they can be used as a proof against the CUs themselves if they attempt to misbehave by denying the message transmission.

However, in the same messages of SSMCRN, since the sender necessitates encrypting their IDs and MAC-key using the network's shared-key that is only shared between the legitimate CUs and the server as shown in (*Step 5.1.2*) and (*Step 6.1.2*), this significantly protect the CUs information from being used by malicious users, who need to escalate the CUs privileges to gain authorised access.

In the remaining messages of both protocols, the possibility of masquerading and reply attacks is extremely low and difficult to occur since the shared-keys that are used are not recognised by malicious users and are only known by the senders and receivers. It is difficult for adversary users to gain the required information and use the network's resources.

### **2) DoS Attacks**

A DoS attack can be launched in CRNs since all CUs are involved in the channel sensing and provide the details of the DCHs' availabilities in collaborative mode. Based on the channel sensing results that take place at the CUs level, both the sender and receiver determine and select the appropriate licensed data channel for data exchange. This introduces a DoS attack for the selected channels since the malicious users can make these channels unavailable and causes DoS attack. By doing this, both the sender and receiver lose the time of the data exchange over the selected DCH and then leads to restarting the entire process of the control and authentication phase, causing saturation over the CCC.

In order to overcome this issue, both FCL and SLDCH are protected from being busy and used by an attacker, who intends to launch a DoS attack, by encrypting them between the sender and receiver during their exchanging over the control channel. Also this serves to prevent the saturation of the SLDCH, thereby avoiding the generation of a large number of forged packets that would effectively

block the channel and enable DoS attacks. Therefore, this encryption effectively reduces the possibility of the chosen channel being selected for communication to be recognised by other users and therefore increases the chance of the successful data transmission over the SLDCH.

### **3) Forgery Attack**

Since the transmitted messages are protected by the encryption scheme from the man in the middle attacks in which an attacker resides between the sender and receiver for intercepting and modifying the transmitted message. This causes modified messages will be delivered to the intended recipient. Therefore, the proposed protocol incorporates the MAC algorithm in all the required the transmitted messages to detect any modifications have been occurring during the transmissions. However, in the messages 5 and 6 of the DSMCRN do not apply the MAC algorithm, as they have already been incorporated with the digital signature, which also function to detect the forgery attack since the hash value is recalculated and compared in the server side for the integrity assurance.

## **3.4. Summary**

This chapter introduced the design of the proposed MCRN protocol for distributed CRNs. It has clearly identified the method of exchange the sensing results which include a list of available channels that are not occupied by the licensed users and the determined best channel for data exchange among CUs. Moreover, it provided the details of the main features of the MCRN protocol such as the number of the transceivers that are associated with each CU to observe the ongoing activities over both the CCC and data channel which is selected and agreed upon on the basis of the channel selection technique. The hidden node terminal is considered and solved with multiple transceivers since it has a direct influence on the network performance.

The chapter also introduced the designing part of two different versions of a secure MAC protocol known as DSMCRN and SSMCRN and details the proposed protocols' messages sequence between senders, receivers and server to exchange the associated security information for providing authorised access. Moreover, a reliable communication between end users as well as between end

terminal devices and the server is provided to ensure the security against any attacks that might occur. Therefore, both DSMCRN and SSMCRN proposed protocols consist of two parts apart of the registration process to obtain the authorised access information from the dedicated server. The first is for both authenticating senders and receivers and exchanging the control information respectively. The validity of any user is proved by the server through verifying the digital signatures of both users in DSMCRN and the applied network's shared key for encryption and decryption and the associated IDs of both users in SSMCRN. Thus, any frame that is sent or received has the sender's information for the authentication procedure, is needed to be checked by the server to ensure the user's legitimacy. However, the second part relies on the result of the authentication. Once the user has been verified successfully, then the second part takes place in securing the data transmission, otherwise the communication will be rejected.

In addition, the chapter presented the proposed protocols' analysis using the BAN formal logic which is used as an initial stage that leads to the contribution of implementing, evaluating and validating both DSMCRN and SSMCRN protocols in terms of meeting the communication and the security requirements.

The chapter provided a list of contributions of this research and they can be summarised as follows:

1. Design a framework for accomplishing successful communication among CUs in decentralised CRNs.
2. Design a framework for the achieving the secure communication and addressing the security requirements in CRNs.
3. Limiting the communication to only CUs, so that any user that has not registered and obtained access information will be banned from the communication with a CU due to the failure of the authentication. Therefore, the network resource will be protected and make it available to only registered CUs.
4. Limiting and hiding both control information (FCL and SLDCH) and data exchange to only a pair of CUs after they have been verified and given a shared key. This works against making the SLDCH unavailable by

adversarial users, who can be internal or external and can manipulate or preoccupy the SLDCH, or generate jamming attacks, in which an attacker forces the CU to hop to a different channel to utilise by transmitting high signalling power to disturb the CUs. This resulting in launching a DoS attack that leads to deteriorating the network performance and throughput. Therefore, encrypting the control information and make it unrecognised for malicious users will reduce the chance of targeting the SLDCH by adversary users, who can make this channel unavailable or creating interference to the CUs (jamming attack).

5. Each pair of CUs obtain a shared key after they have been authenticated which then can be used for limiting the data communication to only a pair of CUs and not among a group (more than two CUs) of the registered CUs. This will ensure the confidentiality of the transmitted data.

The next chapter will focus only on the execution time of the associated security algorithms in both DSMCRN and SSMCRN and demonstrates the impact of the encryption algorithms in the sizes of the transmitted frames.

## Chapter 4 APPLYING SECURITY MECHANISMS

With the application of the BAN formal logic method in the analysis and validation of the DSMCRN and SSMCRN protocols for achieving the authentication and secure communication requirements in the previous chapter, this chapter focuses on the simulation and the execution times of the considered security features of the proposed protocols using Java. Since the security execution time is required and will be added in the communication time of the proposed protocols in Chapter 6. This will investigate of the possible effect on the protocols' performance due to different attacks that can be launched such as modification on the transmitted messages, and the unauthorised access to the network resources. These security algorithms include the encryption and decryption procedures of the transmitted messages along with the keys' generations using two standard algorithms known as RSA and AES. Also the Message Authentication Code (MAC) algorithm is involved for checking the integrity and the authenticity of the transmitted messages along with the digital signature algorithm for generating and verifying the signed information for the authentication process.

### 4.1. Applying digital signature

A Digital Signature has two different main parts; *message signature* and *message verification*. This process requires a pair of public and private keys cryptographic method which also called Asymmetric-Key scheme for the operation (Harn & Ren, 2011) (G, et al., 2012). This pair of key usually associated together and is owned by a particular user or server for encryption and decryption procedures. Generally the public key is used to encrypt a message while the private key is kept secret and utilised for decrypting that message. However, in a digital signature procedure, the private key is used to sign (encrypt) messages while the public key is the key element to verify (decrypt) these encrypted messages (G, et al., 2012). Therefore, the digital signature technique is applied only in DSMCRN protocol and its implication provides the authentication security demand of CUs within the protocol. Therefore, both sender and receiver CUs are required to generate their

digital signatures and send them to the server for authentication within RTA frame (See the ITA and RTA frames discussed in section 3.3.4.2). However, this process requires a successful registration and gain authorised ID which is associated with the right public-key in the verification process. Thus the sender signs its ID using its private key and this process goes through a set of steps as follow:

- 1- Each CU produces a hash value that represents the ID from the Message-Digest 5 (MD5) algorithm.
- 2- Encrypting the generated hash value using the sender's private key (Signing Key)
- 3- Append the ID to the encrypted hash value and this represents a signed ID (digital signature).

The pseudo code of the first two steps that belong to generating the Hash value and then encrypts it with the sender private key is shown as follows:

### Digital signature generation pseudo code in DSMCRN

---

---

```
===== Sender Side =====  
// ID= User's ID an input that is going to be transmitted to another entity  
  
//Generating Hash value from User's ID  
1. Uses ID as input for Message-Digest 5 (MD5) algorithm  
2. Make          plaintext = generated hash value  
  
//Generating signature  
3. uses user's Private-Key to encrypt plaintext  
4. Make          Signature = encrypted plaintext  
5. Make          Digital-Signature = ID + Signature  
6. Uses server's public-key to encrypt Digital-Signature  
7. Make          User's-Digital-Signature = Encrypted Digital Signature
```

---

---

As soon as these steps have been completed, the sender uses the server's public key to encrypt the digital signatures within the ITA frame which is then transmitted to the receiver CU. This encryption is significantly important because of hiding the ID from any users, including CUs who intended to manipulate with this information and leads to launch a DoS attack. Therefore, the chance of intercepting this encrypted information and decrypting it by unauthorised user is may be impossible since the RSA algorithm with the keys size equals to 1024 bits

is deliberately considered and preferable rather than the keys size equals to 512 bits of the same algorithm in the proposed protocol for generating the pair of the public and private keys. This increases the efficiency of the protocol since the encryption discourages attackers to attack this particular information.

Therefore, the receiver necessitates generating their digital signature through applying the same steps and then encrypts it using the server's public key. After that, both encrypted digital signatures are sent to the server within RTA frames.

After receiving and decrypting the RTA frame, the server verifies both signatures individually through the use of the attached ID for retrieving the public key of each CU. Then the verifications of each signature is applied through the use of public key to decrypt the encrypted hash value that will then be compared to the computed hash for each CU ID as shown in pseudo code follow while the entire process sequence of the digital signature verification is shown in Figure 4-1.

### Digital signature verification pseudo code in DSMCRN

---

#### //Decryption

1. Server uses its *private-Key* to decrypt (Cipher text)

#### //Verifying Digital Signature

2. Uses ID to retrieve the relevant *public-key*  
*IF*            *the public-key is found*  
              *Then*        *Go To 3*  
              *Else*        *Go To 4*  
              *Endif*
  3. Uses user's public-key to verify the *Signature*  
              *IF*            *Signature verification = True*  
                              *Then* *Go To 5*  
                              *Else*        *Go To 4*  
                              *Endif*
  4. Send FTA frame
  5. The user is valid
-

## Applying security mechanisms

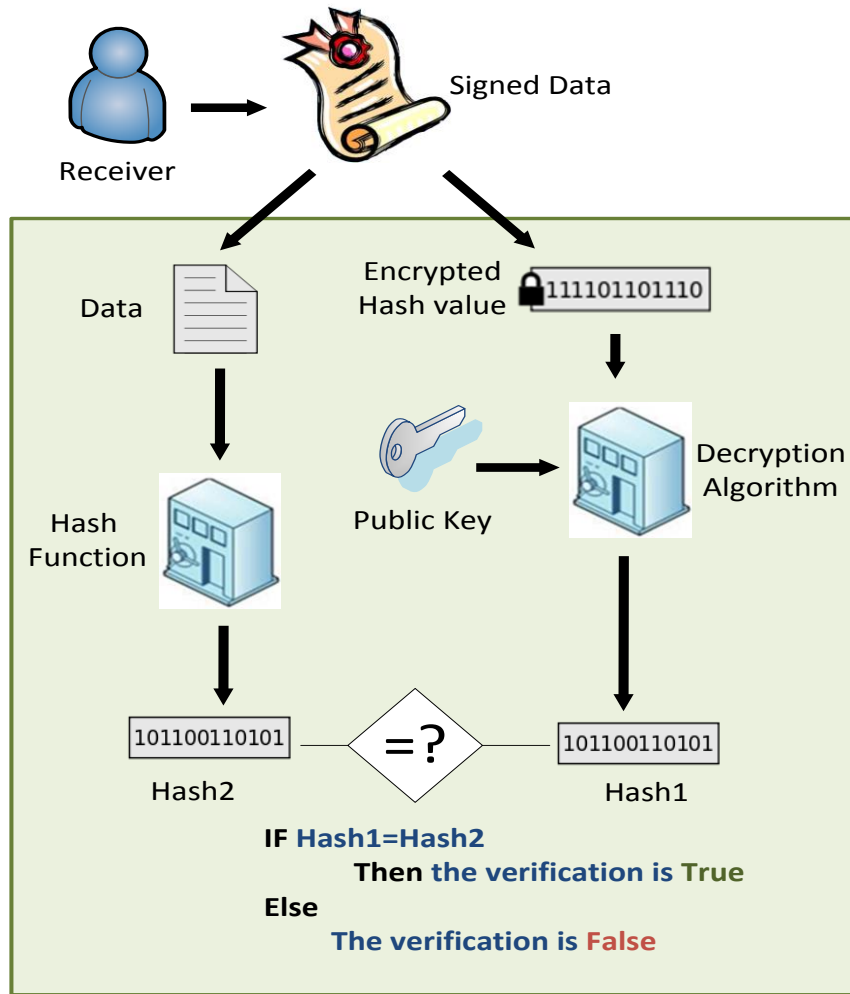


Figure 4-1: Verification process of the digital signature

Table 4-1 gives the required execution times to sign two different IDs by the sender and receiver separately in ITA and RTA frames. Also, it shows the required time to verify these signatures by the server. Therefore, the execution time of signing each ID is 861.5μsec in ITA and RTA while the verification time of each signature is 55261.04μsec.

Table 4-1: Generating and verifying digital signatures in DSMCRN

Frames	Original Message	Message Signature		Message Verification	
		Users' Private Key	Time To Sign	Users' Public Key	Time To Verify
ITA	ID-X	Private key-X	861.5	Public key-X	55261.04
RTA	ID-Y	Private key-Y	861.5	Public key-Y	55261.04

## 4.2. Applying Message Authentication Code (MAC)

The MAC scheme is a symmetric key cryptography based in which a shared key is involved to the MAC algorithm operation. The main principle and goal of this algorithm is to ensure both the integrity and authenticity of the transmitted data which they are concerned in the communication field. In other words, it detects any manipulation or modification has been occurred by a malicious user during the transmission process. Thus, the MAC algorithm confirms that the message is originated by the known sender who shares the same shared key with the receiver. If any modification has been occurred during the transmission, it results in failing the verification on the receiver side due to producing incorrect MAC key that indicates the received message is not authentic and should be discarded. Therefore, the MAC algorithm plays a significant role to ensure the integrity and authenticity of the transmitted message between two entities in both DSMCRN and SSMCRN protocols. The process of this algorithm implication is shown in Figure 4-2 which has two main steps called MAC Key generation and MAC Key and Message verification.

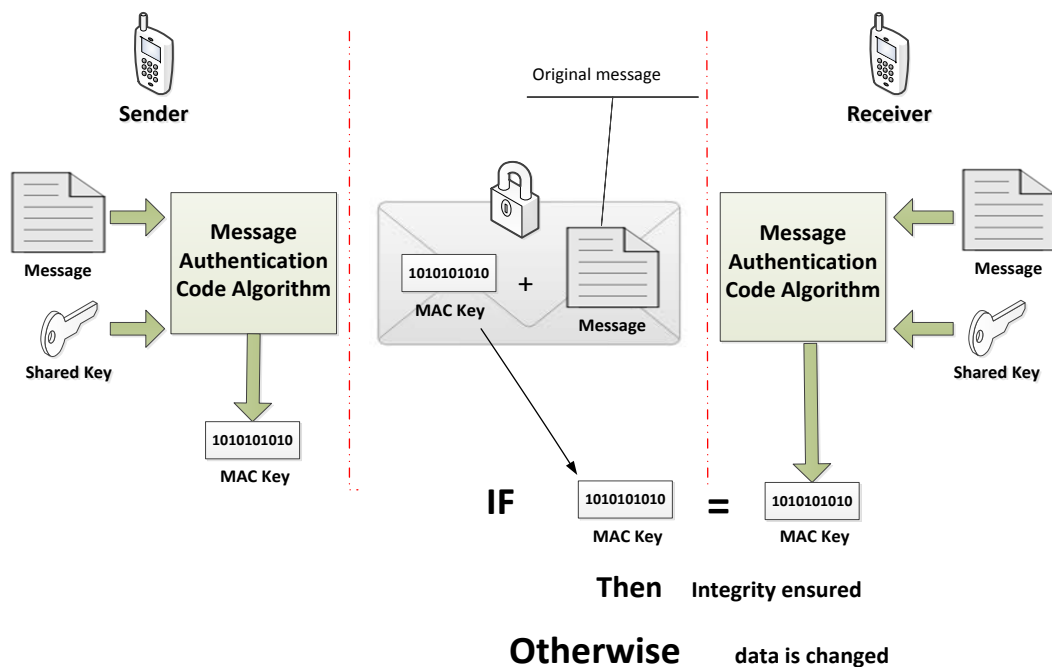


Figure 4-2: MAC Key generation and verification

## Applying security mechanisms

As soon as shared keys are exchanged securely among entities as explained in section 3.3.2, it plays a significant aspect of the MAC algorithm to generate and verify MAC keys in the sender and receiver sides in both DSMCRN and SSMCRN protocols. A certain message, which is going to be sent, and a shared key are the two main inputs to the MAC algorithm and resulting in generating a unique MAC-key for that particular message and that shared key. Thus, the generated MAC-key, then attaches to the original message for encryption before the transmission to the intended destination.

Generally the transmitted messages can be verified after its decryption in the receiver side. The receiver uses the same procedure of generating a new MAC-key from the received message and then compares it with the received MAC-key. If these MAC-keys are matching, then this indicates the message is originated from the right sender and has not been modified during its transmitting. Otherwise the message is discarded as it is not authentic or a significant change to it has occurred. Thus, the following steps of the verification are applied to each message has been received on each frame that includes MAC-key in both DSMCRN and SSMCRN:

- 1- Decrypt the received messages
- 2- Recalculating new MAC-key from the received message which is taken as a first input and the shared key as a second input.
- 3- Compare the received MAC-key with the new generated MAC key.

The pseudo code of generating MAC-keys in the senders' sides and verifying the MAC-key in the receivers' sides of both DSMCRN and SSMCRN as follow:

### MAC algorithm pseudo code in DSMCRN and SSMCRN

---

---

```
===== Sender Side =====
// info= an input that is going to be transmitted to another entity

//Generating MAC-Key
1. Mac_Key = senderGenMAC from (Sharedkey, "Info")
2. Make          plaintext = mac_key+"Info"

//Encryption
3. Uses a Key to encrypt (plaintext) = Cipher text
4. Sends Cipher text

===== Destination Side =====
//Decryption
5. Receiver uses a Key to decrypt (Cipher text)

//Verifying MAC-Key
6. NewMac_key= receiverGenMAC(Sharedkey, "Info");
7. comparemacKey (NewMac_key, Mac_Key)
   IF NewMac_key = Mac_Key
   Then      accept "info"
   Else      Go To 8
   Endif
8. Send RES frame
```

---

---

#### 4.2.1. MAC-Key Generation and verification in the Registration Phase of DSMCRN and SSMCRN

There are only two frames out of four in the registration process of both DSMCRN and SSMCRN protocols where the MAC algorithm is applied. Table 4-2 and Table 4-3 show the original messages of these frames; IOR and COR along with the utilised shared keys to participate in generating MAC-keys in DSMCRN and SSMCRN. Each frame of the both protocols has a different message while the shared keys that are used by both the CU and the server is *X-S-Shared-Key* which was generated by the CU before transmitting IOR frame. The original message that is intended to be transmitted in the IOR frame of the DSMCRN is the CU's Public-key, Shared-key and ID and requires 29.88µsec and 54.33µsec for generating and verifying MAC-keys respectively. However, it is different in the same frame of the SSMCRN in which it includes the sender's

## Applying security mechanisms

Shared-key and ID necessitates 27.88 $\mu$ sec and 46.33 $\mu$ sec for MAC-keys generation and verification respectively.

However, the original message of the COR frame in the DSMCRN is only the CU's ID which is generated by the server after the successful registration process while it is different in the same frame of SSMCRN since it is network's shared-key and CU's ID. Therefore, it requires time equals to 21.36 $\mu$ sec and 44.37 $\mu$ sec for generating and verifying MAC-keys respectively in COR of the DSMCRN while it necessitates different time in the same frame of the SSMCRN which equals to 26.86 $\mu$ sec and 52.83 $\mu$ sec for MAC-keys generation and verification respectively.

Table 4-2: Time to generate and verify MAC-keys in the registration phase of DSMCRN

Frames	Original Message	Shared Key	Time to generate MAC-key	Time to verify MAC-key
RTR	N/A	N/A	N/A	N/A
CTR	N/A	N/A	N/A	N/A
IOR	User' X ID, public key and shared key	X shared key	29.88	54.33
COR	User' X ID	X shared key	21.36	44.37

Table 4-3: Time to generate and verify MAC-keys in the registration phase of SSMCRN

Frames	Original Message	Shared Key	Time to generate MAC-key	Time to verify MAC-key
RTR	N/A	N/A	N/A	N/A
CTR	N/A	N/A	N/A	N/A
IOR	User' X ID and shared key	X shared key	27.88	46.33
COR	X ID and network's shared key	X shared key	26.86	52.83

### 4.2.2. MAC-key Generation and verification in Control Phase of DSMCRN and SSMCRN

Generating and verifying MAC-keys process in the control phase of both DSMCRN and SSMCRN remain same. However, the main difference here is that which shared keys are used in each frame for generating and verifying the MAC-keys?

## Applying security mechanisms

To answer this question, Table 4-4 and Table 4-5 give the original messages as the first input and the applied shared key in each frame as a second input for the MAC algorithm in SSMCRN and DSMCRN respectively.

The attached MAC-keys in ITA and RTA frames of SSMCRN only were generated with the use of the network's shared-key (Group 1) and users' IDs as the original messages. Thus, the sender's MAC-key, which is sent in ITA, requires processing time equal to 27.17 $\mu$ sec for generation at sender side and 40.15 $\mu$ sec for verification at the receiver side. This verification is necessary before requesting the server to authenticate the sender since the integrity of the sender's ID is significantly important for the server to authenticate the user. Therefore, the receiver CU also requires 34.71 $\mu$ sec to generate their MAC-key based on the received ID and MAC-key along with his/her ID using the network shared key. In the server side, the verifications takes place and requires time to validate the integrity of the transmitted message equals to 44.98 $\mu$ sec.

However, in DSMCRN and SSMCRN protocols, one different MAC-keys are generated for both CUA1 and CUA2 frames instead of generating two different MAC-keys for both the sender and the receiver since it provides the same functionality and both users have been authenticated. This will save extra time for the server to process and generate another MAC-key if each frame has a different MAC-key. Therefore, the generated MAC-key which is attached to both frames is obtained by running the X-Y-Shared Key and new ID on the MAC algorithm and requires 21.43 $\mu$ sec for generating by the server. In contrast, each CU necessitates verifying the integrity of the received information in CUA1 and CUA2 independently since these frames were transmitted to different CUs. Therefore, the required times for verifying these keys are 26.56 $\mu$ sec and 25.66 $\mu$ sec of the CUA1 and CUA2 respectively.

In RTS and CTS frames of both protocols, the MAC-keys are generated with the use of *X-Y-Shared Key* as the first input while the second input is FCL in RTS and SLDCH in CTS frames to the MAC algorithm. Thus, the required time for generating these MAC-keys are 21.35 $\mu$ sec and 20.41 $\mu$ sec in RTS and CTS respectively, while they require times equal to 32 $\mu$ sec and 30.31 $\mu$ sec to verify these keys in both frames.

## Applying security mechanisms

Table 4-4: Time to generate and verify MAC-key in the control phase of SSMCRN

Frames	Original Messages	Shared Keys	Time to Generate MAC Key	Time to Verify MAC Key
ITA	MAC-Key+ID-A	Network's shared key (Group1)	27.17	40.15
RTA	MAC-Key+ID-B	Network's shared key (Group1)	34.71	44.98
CUA1	G-ID+Shared Key	X-S-Shared Key (Group2)	21.43	26.56
CUA2	G-ID+Shared Key	Y-S-Shared Key (Group2)		25.66
RTS	FCL	X-Y-Shared Key (Group3)	21.35	32
CTS	SLDCH	X-Y-Shared Key (Group3)	20.41	30.31

Table 4-5: Time to generate and verify MAC-key in the control phase of DSMCRN

Frames	Original Messages	Shared Keys	Time to Generate MAC Key	Time to Verify MAC Key
ITA	N/A	N/A	N/A	N/A
RTA	N/A	N/A	N/A	N/A
CUA1	Gid+Shared Key	X-S-Shared Key (Group2)	21.43	25.66
CUA2	Gid+Shared Key	Y-S-Shared Key (Group2)		25.03
RTS	FCL	X-Y-Shared Key (Group3)	21.35	32
CTS	SLDCH	X-Y-Shared Key (Group3)	20.41	30.31

### 4.2.3. MAC Key Generation and verification in the Data Transmission Phase of DSMCRN and SSMCRN

For generating a MAC-key for an intended data for transmission in both DSMCRN and SSMCRN, only Group 3 shared key (*X-Y-Shared Key*) is applied for the data integrity assurance and the secure transmission. Therefore, Table 4-6 demonstrates the size of the payload; 1500 bytes as a first input belongs to the original message and the X-Y-Shared Key belongs to Group 3, which is generated by the server after the successful authentication of both the sender and receiver, as the second input for the MAC algorithm. Therefore, the required time for generating a MAC-key is 43.47μsec and 59.16μsec is consumed at the receiver side to verify the integrity of the transmitted message in both DSMCRN and SSMCRN protocols.

Table 4-6: Time to apply and verify MAC-keys in Data phase of DSMCRN and SSMCRN

Frame	Original Messages	Shared Key	Time to Generate MAC-key	Time to Verify MAC-key
Data	1500 bytes of text	X-Y-Shared Key (Group3)	43.47	59.16

### 4.3. Encryption and Decryption cryptography schemes

Due to the desire cases of the security conditions, AES and RSA are two different cryptographic systems that are considered in the DSMCRN and SSMCRN protocols for the purpose of encrypting and decrypting the required transmitted information. AES is used in all the phases of both protocols while the RSA is applied in the registration process of both protocols and only in the authentication/control phase of the DSMCRN. Table 4-7 highlights the use of both AES and RSA in the phases of each protocol.

Table 4-7: AES and RSA implications in DSMCRN and SSMCRN

Phases	Frames from	SSMCRN		DSMCRN	
		AES	RSA	AES	RSA
Registration	Server to Node	✓		✓	
	Node to Server		✓		✓
Control	Node to Node	✓			
	Node to Server	✓		✓	✓
	Server to Node	✓			✓
Data	Node to Node	✓			✓

#### 4.3.1. Advanced Encryption Standard – AES implication

As explained in section 1.4.2.3, the AES cryptography algorithm is based on a shared key cryptography, the determined key size is 128 bits for both encryption and decryption mechanisms in both DSMCRN and SSMCRN protocols. Therefore, the use of this algorithm and its execution time in each phase of the proposed protocols are detailed as follows:

##### 4.3.1.1. AES algorithm in the registration Phase of DSMCRN and SSMCRN

In the registration phase of both protocols, only COR frames are encrypted and decrypted using AES algorithm. However, the sizes of the included encrypted information are different in each protocol. This refers to the associated plaintext size, which has significant influence on the time is consumed for both encryption and decryption. Therefore, in the DSMCRN, the size of the plaintext (ID and

MAC-Key) of the COR frame is 27 bytes and it requires 84.82 $\mu$ sec for encryption. Meanwhile the size of the MAC-key and ID after applying the encryption process is expanded to 44 bytes. This increase has occurred since the encryption procedure has a direct influence on the size of the encrypted payload due to the total repetition iteration of the transformation rounds which converts plaintexts to cipher texts (Pavithra & Ramadevi, 2012). In terms of the decryption procedure, the time required to decrypt the COR frames in the same protocol is 87.84 $\mu$ sec.

In contrast, in the SSMCRN, the total size of the plain text (Network's shared-key, ID and MAC-Key) of the COR is 43 bytes and requires 148.21 $\mu$ sec for encryption. This size is not remained continuously after the encryption since it is expanded to 64 bytes as a cipher text and necessitates 149.11 $\mu$ sec for decrypting the cipher text of the same frame in SSMCRN protocol. Table 4-8 illustrates the execution times of the encryptions and decryptions of the COR frames in both protocols.

Table 4-8: AES implication in Registration phase of the DSMCRN and SSMCRN

Protocol	Frame	Size after Encryption	Time to Encrypt	Time to Decrypt
DSMCRN	COR	66	84.82	87.84
SSMCRN	COR	86	148.21	149.11

#### **4.3.1.2. AES algorithm in the control phase of DSMCRN and SSMCRN**

In the control phase of both protocols, the number of the transmitted frames that incorporate the AES encryption is different. In the SSMCRN protocol, six frames are encrypted and decrypted with the use of the AES algorithm while in DSMCRN only 4 frames out of six are encrypted and decrypted using the same algorithm and the remaining 2 frames have different encryption mechanism.

Table 4-9 gives the characteristics of ITA and RTA frames in terms of their attached information before and after the encryption procedure with the AES in SSMCRN only. Thus, the plain text size of the ITA is 27 bytes which is combined of both the MAC-key and ID. This size is increased to 44 bytes after the

## Applying security mechanisms

encryption and requires 84.82 $\mu$ sec and 87.84 $\mu$ sec for encryption and decryption respectively. On the other hand, the plain text size of the RTA is 54 bytes which include two IDs and two MAC-keys of both the sender and receiver CUs. Once the encryption is applied the cipher text size increases to 90 bytes and necessitates time for encryption and decryption equal to 131.14 $\mu$ sec and 133.65 $\mu$ sec respectively.

Table 4-9: AES implication in control phase of the SSMCRN

Frames	Plain Text	Plain Text size	Cipher Text size	Time to Encrypt	Time to decrypt
ITA	MAC_key + A-ID	27	44	84.82	87.84
RTA	MAC_key+UidA+ MAC_key+UidA	54	90	131.14	133.65

Table 4-10 provides the details of the common frames of the control phase in the SSMCRN and DSMCRN protocols in terms of the plaintexts and cipher texts that are associated to those frames and their sizes in bytes. Also, it gives the required times in microseconds for encrypting and decrypting these various sizes of plain texts. Thus, CUA1 and CUA2 have the same plaintexts (MAC-key, Shared Key and ID) and the same sizes which equal to 43 bytes of each frame. However, as soon as the encryption is applied the sizes of these frames are expanded to 64 bytes as a cipher text of each frame. Moreover, each frame requires 149.11 $\mu$ sec for encryption using the recipient's shared-key and 148.21 $\mu$ sec for decryption procedures using the same key.

On the other hand, each of RTS and CTS has the same size of plain text which is equal to 25 bytes. This size includes FCL and the MAC-Key in RTS frame and SLDCH and MAC-key in the CTS frame of both protocols. However, the plain text size of each frame is affected after the encryption is applied and increased to 44 as a cipher text. Therefore, the required time to encrypt each plain text on each frame is 136.16 $\mu$ sec and decrypt the cipher text is 130.40 $\mu$ sec of each frame.

Note: 2 bytes are assigned for the SLDCH while only 4 bits are used to represent the SLDCH and the remaining bits are set to 0 for the future work to address the backup channels procedure.

## Applying security mechanisms

Table 4-10: AES implication in the common frames of control phase SSMCRN and DSMCRN

Frames	Plain Text	Plain Text size	Cipher Text size	Time to Encrypt	Time to decrypt
CUA1	userBid+sharkeybytes+mackey	43	64	149.11	148.21
CUA2	userBid+sharkeybytes+mackey	43	64	149.11	148.21
RTS	FCL+mackey	25	44	136.16	130.40
CTS	SLDCH+mackey	25	44	136.16	130.40

### 4.3.1.3. AES algorithm in the data transmission phase of DSMCRN and SSMCRN

In the data transmission phase, both the DSMCRN and SSMCRN protocols have the same time for encryption and decryption over the data channel as they both utilise the AES algorithm and the same data size of the transmitted data. Although, 1500 bytes of plain text is considered and selected as sample of data in order to determine the required time of encrypting and decrypting, both protocols are applicable to any size of data for transmission as long as there is no fixed standard for packet size in the IEEE 802.22. Therefore, the encryption time of 1500 bytes of data and the generated MAC-key before its transmission over a data channel is 858.18 $\mu$ sec and the size of the cipher text is 2100 bytes which requires 510.43 $\mu$ sec to be decrypted. Table 4-11 shows the details of the data frame in both protocols in terms of applying the AES algorithm for encryption and decryption procedures.

Table 4-11: AES implication in the data phase of DSMCRN and SSMCRN

Frames	Plain Text	Plain Text size	Cipher Text size	Time to Encrypt	Time to decrypt
Data	Data + MAC_key	1500	2100	858.18	510.43

### 4.3.2. RSA implication in DSMCRN and SSMCRN

As discussed in section 1.4.2.2, RSA cryptography scheme is based on public and private keys, the determined key length is 1024 for both encryption and decryption mechanisms in both proposed protocols. Therefore, the RSA is used in the registration phase of both protocols to encrypt and decrypt the IOR frame while it is used only in the control phase of the DSMCRN protocol to encrypt and decrypt both the ITA and the RTA frames. The details of applying this algorithm in both protocols are provided as follows:

#### 4.3.2.1. RSA algorithm in the registration phase of DSMCRN and SSMCRN

In the registration phase of both DSMCRN and SSMCRN protocols, only IOR frames are encrypted and decrypted using the RSA cryptographic scheme. However, their attached information sizes are different for each protocol and this effect on the time of the encryption and decryption. Thus, the plain text size of the IOR frame in SSMCRN is 43 bytes and requires 186.55 $\mu$ sec and 12136.18 $\mu$ sec for encryption and decryption respectively. On the other hand, the plain text of the IOR frame in DSMCRN protocol is 252 bytes and necessitates time equal to 204.66 $\mu$ sec and 12817.39 $\mu$ sec for encryption and decryption respectively. Therefore, Table 4-12 shows the details of the applied RSA algorithm in the registration phase of both DSMCRN and SSMCRN protocols while the pseudo code of the encryption and decryption of the IOR frame is shown as follow:

##### Encrypting and decrypting IOR frame pseudo code in SSMCRN and DSMCRN

---

---

```
// Plaintext= (MAC-Key +Shared-Key + Public –Key + ID) OR (MAC-Key+Shared-Key+ID)
```

##### //Encryption

1. Uses *server's Public-Key* to encrypt plaintext
2. Make **Cipher text** = encrypted plaintext
3. Attaches **Cipher text** within IOR frame
4. Sends IOR frame

##### //Decryption

5. Server uses its *Private-Key* to decrypt the **Cipher text**
  6. Make **Plaintext** = decrypted Cipher text
- 
- 

Table 4-12: RSA implication in the registration phase of the DSMCRN and SSMCRN

Protocol	Frames	Plain Text	Plain Text size	Cipher Text size	Time to Encrypt	Time to decrypt
DSMCRN	IOR	mac_key+ Public-key+ Sharedkey+X-id	252	307	204.66	12817.39
SSMCRN	IOR	mac_key+ Sharedkey+X-id	43	64	186.55	12136.18

#### 4.3.2.2. RSA algorithm in the control phase of DSMCRN

However, in the control phase of the DSMCRN, there are only two frames out of six are encrypted and decrypted using the RSA algorithm. These frames are ITA and RTA in which they include digital signatures and users' IDs of the CUs who transmitted these frames. Each CU uses the server's public-key to encrypt their generated digital signature and ID while the server, which is the final destination, decrypts the received encrypted information of the RTA frame using its private key. Thus the time is taken to encrypt and decrypt the attached information in ITA frame is 545.15 $\mu$ sec and 1015.45 $\mu$ sec respectively, while it necessitates time equals to 546.36 $\mu$ sec and 1020.88 $\mu$ sec for the encryption and decryption respectively of the RTA frame of the same protocol. Table 4-13 shows the plain text information and its size before and after the encryption (cipher text) and both the time to encrypt and decrypt the information included within the ITA and RTA frames.

Table 4-13: RSA implication in the control phase of the DSMCRN

Frames	Plain Text	Plain Text size	Cipher Text size	Time to Encrypt	Time to decrypt
ITA	signature + A-ID	52	64	545.15	1015.45
RTA	MAC_key+UidA+ MAC_key+UidA	52	64	546.36	1020.88

### 4.4. Summary

Different security algorithms such as digital signatures, Message Authentication Code and discrepant types of encryptions based on RSA and AES have been implemented in the current chapter. The execution time of each security algorithm has been determined in each proposed protocol and considered as the first part of implementing the secure MAC protocols to meet the intended task. Therefore, the following chapter will consider and apply the obtained execution times of the mentioned security algorithms to the MCRN protocol, which is discussed in chapter 3. This will provide secure MAC protocols for establishing secure communication process among CUs.

## **Chapter 5 MEDIUM ACCESS CONTROL (MAC) FOR DSMCRN AND SSMCRN**

Extending the work of the previous chapter, which mainly focused on the simulation of security features that are associated with the proposed protocols, DSMCRN and SSMCRN, this chapter discusses their simulation in terms of secure communication between CUs and a dedicated server. This requires modifications to the processing of MAC channel access frames, comparing to the frames in MCRN protocol, in reference to incorporating additional security frames and the bits associated with each frame, especially when a server node is involved in the communication process. This can affect the communication time required for CCC, and the data channel availability. Therefore, this chapter discusses the details of the secure communication of DSMCRN and SSMCRN in terms of MAC channel access.

### **5.1. The common features of DSMCRN and SSMCRN**

Although, the proposed protocols are designed to achieve successful communication in CRNs, they have certain features common to their network operations. These features are associated with the number of transceivers equipped by each CU, as explained in section 3.2.2.1; in addition, the channel sensing approach and licensed data channel selection criteria were discussed in section 3.2.2.2. Moreover, all the proposed protocols are based on the same assumption; that of utilising a dedicated CCC, as explained in section 3.2.1.

### **5.2. MAC access model and timing in DSMCRN and SSMCRN**

The MAC access for DSMCRN and SSMCRN is similar to that discussed in section 3.2.6 for the MAC of the MCRN. However, the main difference is the additional number of involved SIFS over time, due to the increase in the number of transmitted frames belonging to the security factor. A part of this, it is the same

mechanism as the DCF, which is based on CSMA/CA for channel access, and is considered in both DSMCRN and SSMCRN protocols. Therefore, the application of MAC access modes and timing for both DSMCRN and SSMCRN is briefly discussed, as follows:

### 5.2.1. MAC for the registration phase in DSMCRN and SSMCRN

To support the registration process of both protocols, 4 frames are obligatory for transmitting data between a user and a dedicated server, over the CCC. According to the IEEE 802.11 standard, both DIFS and SIFS waiting times are necessary for channel access decisions and high-priority transmissions respectively. DSMCRN and SSMCRN apply these times, and NAV, in order to provide the same functionalities as the employed CSMA/CA in IEEE 802.11. Thus, Figure 5-1 shows the associated interframe spacing (DIFS and SIFS) for coordinating CCC access for the registration process with the NAV factor in both protocols.

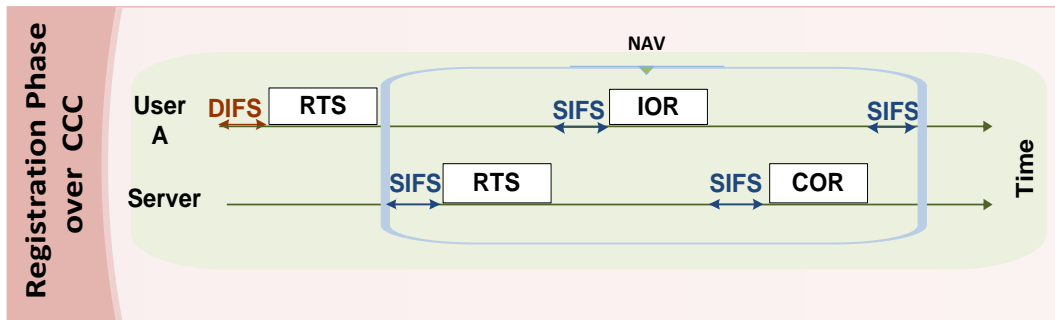


Figure 5-1: The time required for each user to register and join the network

The following equation is used to calculate the overall time required for each CU to register the requisite information on the server and obtain authorised access to information to join the network in both DSMCRN and SSMCRN,

$$\begin{aligned}
 &T_{RTR+CTR+IOR+COR} + DIFS + 3(SIFS) + T_{gen\_MACKey} + T_{verify\_MACKey} \\
 &+ T_{enc(RSA)} + T_{dec(RSA)} + T_{enc(AES)} + T_{dec(AES)} \\
 &+ T_{gen\_SharedKey}
 \end{aligned}$$

Equation 1: The total time for each CU to register and gain the access information

### 5.2.2. MAC for control phase and data transmission

The current phase exists in the MCRN protocol and involves only two frames, recognised as RTS and CTS, before switching to the selected data channel. It is considered in both DSMCRN and SSMCRN, with an additional 4 security frames launched over the same CCC, before both RTS and CTS transmissions. Three entities, which are; *senders*, *receivers* and the *dedicated server*, participate in the transmission process for these 6 frames. Thus, Figure 5-2 shows the sequence of these security and control frames over the CCC, with their NAVs settings, and both DIFS and SIFS in both DSMCRN and SSMCRN. The mechanism of access for CCC, and the waiting time after receiving each frame is known as SIFS (see section 3.2.6 for details of CCC access, which remain the same).

The following Equation 2 is used to calculate the required time to exchange control frames between the sender and the receiver in both DSMCRN and SSMCRN.

$$T_{ITA+RTA+CUA1+CUA2+RTS+CTS} + DIFS + 6(SIFS) + T_{gen\_MACKey} + T_{verify\_MACKey} + T_{enc(RSA)} + T_{dec(RSA)} + T_{enc(AES)} + T_{dec(AES)} + T_{gen\_SharedKey} + T_{Data+ACK} + SIFS + T_{gen\_MACKey} + T_{verify\_MACKey} + T_{enc(AES)} + T_{dec(AES)}$$

Equation 2: The total time to exchange the authentication and control frames over the CCC

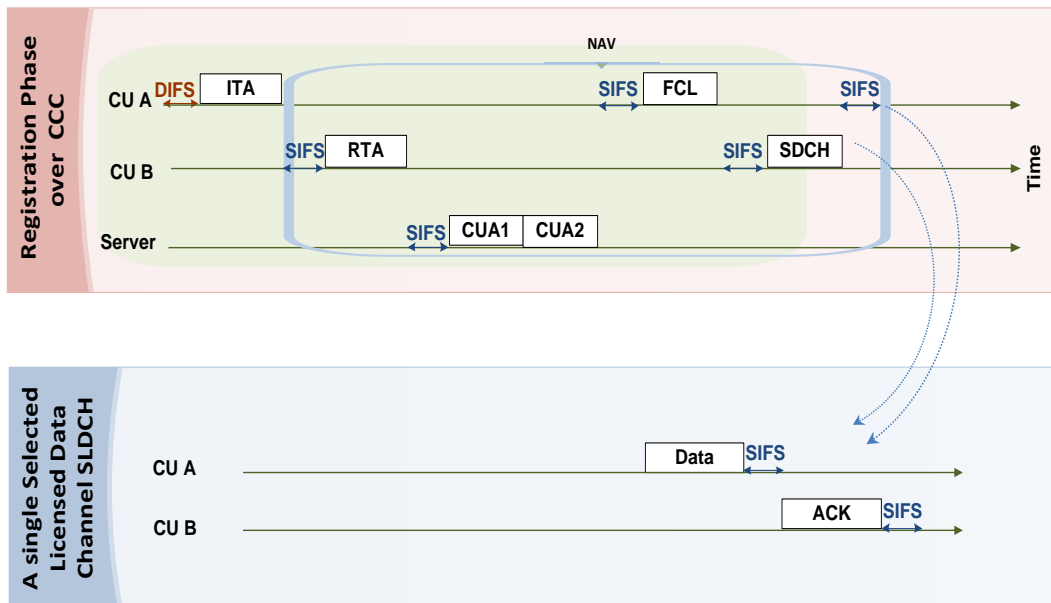


Figure 5-2: The time required for CUs to exchange their control frames

### 5.3. Simulation and Performance evaluation of SSMCRN and DSMCRN

Simulating the DSMCRN and SSMCRN are essential to identify the protocols' performance and assist to visualise the evaluated network performance. MATLAB simulator is extensively used for wireless technology research is used as it is capable of simulating communication systems, analysing data, supports a high-level language, and features an interactive environment (Uk.mathworks.com, 2009) (Ahmad, et al., 2011). Therefore, despite CR technology research has recently emerged, the proposed protocols with and without security and the benchmark protocols are simulated and evaluated in MATLAB for comparison, evaluation and validation purposes and including aspects related to the network performance. As discussed in (Maziar, 2010), a large portions of the TV white space becomes available for CUs to utilise. Therefore, the TV portion; from 471.25MHz to 607.25MHz, which are available most of the time, are considered for the CCC and 10 data channels to exchange both the control information and data respectively of the proposed and benchmark protocols.

Thus, in order to simulate the proposed protocols, a set of wireless parameters are significantly identified to be configured for the simulation tasks. These parameters include the size of the frames, the number of CUs and LUs, the number of control and data channels, and the data channels availability that are associated with measuring the network performance. Therefore, in the simulation task, the parameters of the IEEE 802.11b has been considered for simulating both the proposed and the benchmark protocols since these parameters are used by most of the published MAC protocols for CRNs (Joe & Son, 2008) (Zhang & Su, 2011) (Jie, et al., 2013). In addition, the Distributed Coordination Function (DCF) based on the CSMA/CA is considered for providing the CCC access mechanism by CUs. Thus, the proposed protocols are simulated with two different scenarios; five runs with different number of CUs, consisting of 4, 8, 12, 16 and 20 users to exchange their control information and data while the second involves five runs with different number of CUs, consisting of 4, 8, 12, 16 and 20 users with LU become ON to utilise the licensed data channel. These scenarios are considered to

measure the influence on the successful messages delivery rate and the time performance for each protocol.

### **5.3.1. The network parameters**

Several parameters are considered in the DSMCRN and SSMCRN design and simulation to fulfil the entire communication process among 20 CUs. These involve a single control and 10 data channels used by CUs, considering the best data channel selection criteria which is based on the most available time as discussed in section 3.2.2.2 for enabling the success of data transmission. These channels have the same data rate of 11Mbps and the DSSS PHY layer characteristics are applied. 10  $\mu$ sec is allocated for switching time after selecting and exchanging the most appropriate data channel between senders and receivers. Moreover, 1500 bytes of data as a payload size is considered in the proposed scenario to analyse its influence on the entire communication over the data channels. Table 5-1 highlights the parameters used with their values in the MCRN protocol.

Thus, the frames and their sizes incorporated within DSMCRN and SSMCRN are given in Table 5-2, while their format details were discussed in the design stage in sections 3.3.4 and 3.3.5.

## Medium Access Control (MAC) for DSMCRN and SSMCRN

Table 5-1: The network parameters

Name of the parameter	Value	Description
DIFS	50 $\mu$ sec	Distributed Interframe Space
SIFS	10 $\mu$ sec	Short Interframe space
CCC-TR	11 Mbps	CCC Transmission rate
DCH-TR	11 Mbps	DCH Transmission rate
T <sub>DCH Scan</sub>	5s	Time of Data Channels Scan
N <sub>TS</sub>	2	Number of Transceiver
PHY layer Characteristics	DSSS	Direct-sequence spread spectrum
T <sub>switch</sub>	10 $\mu$ sec	Time to switch from CCC to selected data channel
CNT <sub>Window</sub>	32	Contention Windows
RTS	20 bytes	Request-To-Send frame
CTS	20 bytes	Clear-To-Send frame
Data	1520 bytes	Data frame
ACK	20 bytes	Acknowledgement frame
N <sub>CCC</sub>	1	Number of Common Control Channel
N <sub>SLDCH</sub>	10	Number of Data Channels
N <sub>CUs</sub>	20	Number of CUs where 4, 8, 12, 16, 20 CUs for 5 runs
N <sub>S</sub>	1	Number of Sensor

Table 5-2: DSMCRN and SSMCRN frames

Name of the frames	Frames' sizes in DSMCRN	Frames' sizes in SSMCRN	Description
<b>Registration phase</b>			
RTR	22	22	Request-To-Register
CTR	49	49	Clear to register
IOR	329	86	Information for registration
COR	66	86	Confirmation-OF-Registration
<b>Control phase</b>			
ITA	86	66	Information-To-Authenticate
RTA	150	110	Request-To-Authenticate
CUA1	86	86	Confirmation of User's Authentication 1
CUA2	86	86	Confirmation of User's Authentication 2
RTS	66	66	Request-To-Send
CTS	66	66	Clear-To-Send
<b>Data phase</b>			
DT	2122	2122	Data transmission
ACK	46	46	Acknowledgement
<b>Security Frames</b>			
RES	22	22	Resend
FTA	46	46	Failed-To-Authenticate

### 5.3.2. Communication time of DSMCRN and SSMCRN

Although, both DSMCRN and SSMCRN protocols share many features, such as the number the transmitted frames and the control and data channels, they have different security features proceeding from the implications of having asymmetric and symmetric keys for authentication. This considerably affects the duration and performance of the protocols, since the applied security features require different lengths of time for execution (see section 4.3). Therefore, in order to calculate the total required time (T) taken to successfully exchange the control and data phases of the DSMCRN and SSMCRN protocols between senders and receivers, the following Equation 3 is applied.

$$T = \{T_{DIFS} + T_{ITA} + T_{RTA} + T_{CUA1} + T_{CUA2} + T_{RTS} + T_{CTS} + T_{Data} + T_{ACK} + 7 * T_{SIFS}\}$$

Equation 3: Total time to exchange authentication, control information and data frames

Thus, Figure 5-3 below shows the entire successful communication process and the time taken for a single pair of CUs to exchange data successfully. As shown, the time required to complete the communication process in DSMCRN is significantly higher than the time required in SSMCRN, by approximately 11 times. This is because of the point introduced above, regarding security features, since the DSMCRN accommodates and applies the digital signature, which operates based on asymmetric key cryptography and relevant frame sizes.

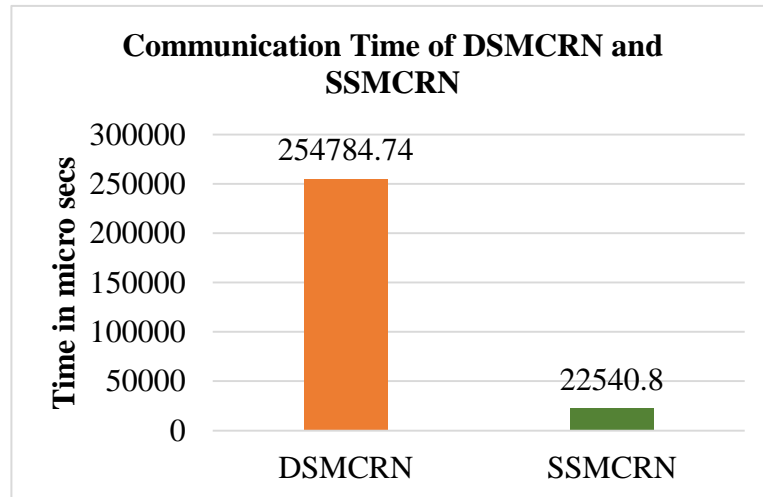


Figure 5-3: The communication time for a single pair of CUs in DSMCRN and SSMCRN

However, Figure 5-4 demonstrates the communication time for 10 pairs of CUs, over both control and data channels in DSMCRN and SSMCRN. The data transmission initiates, only after the selected data channel has determined the CTS frame between both the sender and receiver. Thus, the first pair of CUs, who won in the channel contention process, accesses the control channel immediately, since it is dedicated and available, this requires time equal to 254784.74 $\mu$ sec in DSMCRN and 22540.8 $\mu$ sec in SSMCRN to successfully exchange the control and data frames in an encrypted format. However, the second pair of CUs necessitates total time equal to 506378.39 $\mu$ sec in DSMCRN and 41881 $\mu$ sec in SSMCRN, to exchange the same frames effectively. The time frame is different because of the waiting time, which is recognised as a NAV period, and is equal to 251593.65 $\mu$ sec in DSMCRN and 19349.71 $\mu$ sec in SSMCRN for the control channel to be vacant, since it is occupied by the first group seeking to exchange control frames. As soon as the first group successfully exchanged the CTS frame and switched to the determined data channel, the control channel became available and ready for the second group to access based on the channel's contention. Therefore, the second group necessitates a time equal to 254784.74 $\mu$ sec to exchange the control and data frames successfully.

However, in terms of the third group, the sender needs a waiting time equal to 503187.3 $\mu$ sec in DSMCRN and 38689.9 $\mu$ sec in SSMCRN to be able to access the control channel, and entails 254784.74 $\mu$ sec and 22540.8 $\mu$ sec in DSMCRN and SSMCRN respectively to exchange the control and data frames successfully. Thus, this process remains continuous for the remaining 7 groups of CUs, while considering the waiting time for the control channel to be vacated and made available to the next pair of CUs, to avoid any collisions.

# **Medium Access Control (MAC) for DSMCRN and SSMCRN**

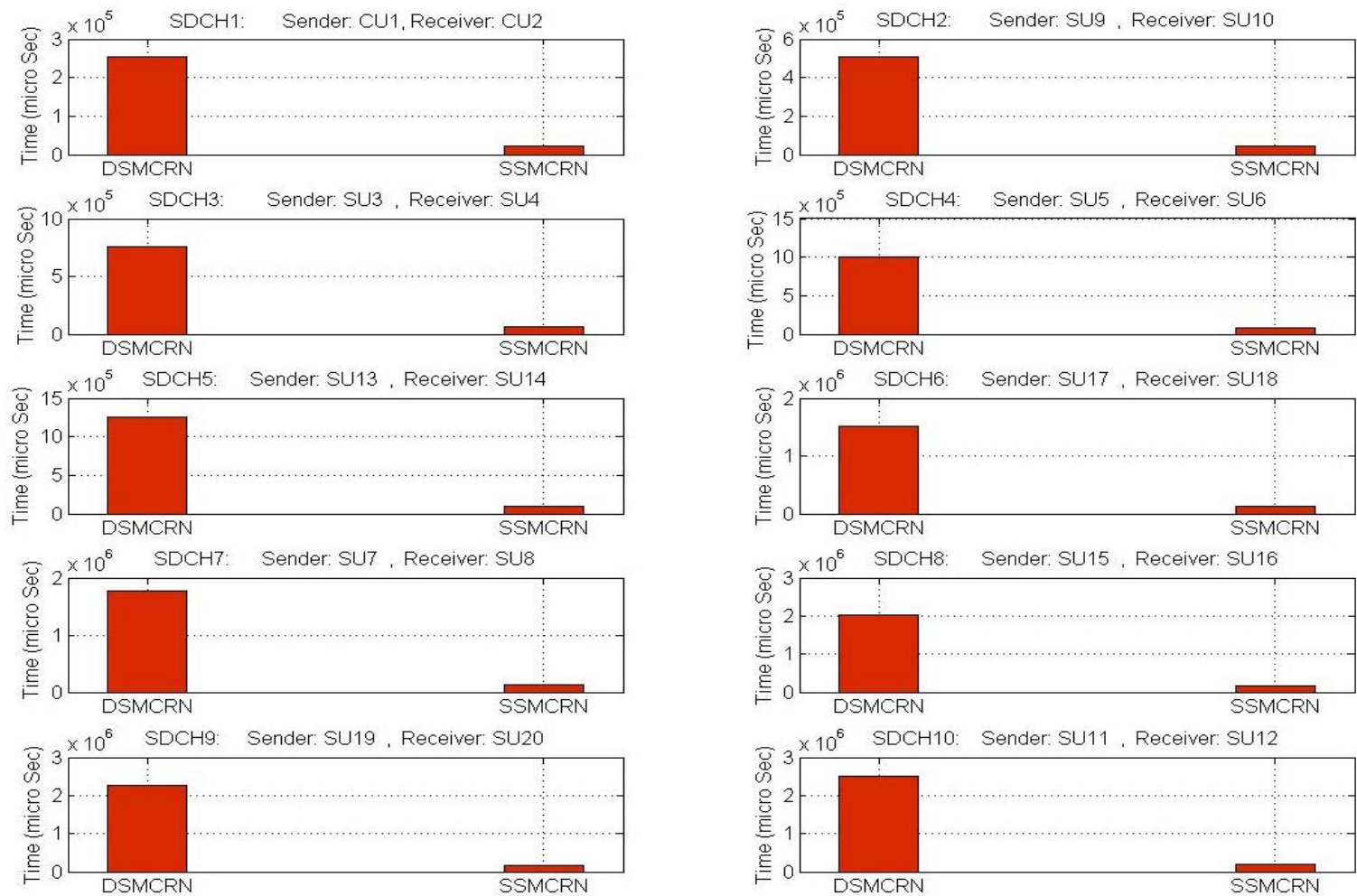


Figure 5-4: The communication time for 10 pairs of CUs in DSMCRN and SSMCRN

Therefore, in order to evaluate the total time for the performance of 20 CUs in conjunction with the LUs activities (which affects the protocols' run time), Figure 5-5 demonstrates the communication time in microseconds for five runs (on 4, 8, 12, 16 and 20 CUs, with and without LUs activities), when using both DSMCRN and SSMCRN protocols. It is apparent that there is a significant difference in the communication time of each protocol, since they have different security features, authentication mechanisms, and encryption procedures. Generally, the time for both protocols increases when the number of incorporated CUs involved in the communication process increases, as only one CCC is used by the incorporated CUs to exchange and control information. The total communication time for the 20 CUs increases significantly and is higher in DSMCRN compared to the SSMCRN protocol. This is because there are two different main factors responsible for generating and verifying digital signatures, as well as an RSA algorithm that is used to encrypt and decrypt some of the control frames (see section 4.3) for 20 CUs. This leads to the SSMCRN protocol performing much faster (about 11 times faster) in each run, compared to the DSMCRN.

However, if a LU becomes ON, to utilise a data channel, the time pattern is not affected. Since the CUs' data's transceiver is still ON for observing the LUs' activities over the data channel and time is passing. Therefore, CUs are not allowed to transmit data during the period the data channel is occupied by the LU's activities. However, there is another case, in which the time taken for the CU to communicate can be affected due to the data channel's occupancy by LUs' activities, in which a backup data channel is involved in the communication. This leads to the CUs being switched to the selected backup data channel for retransmitting data, and requires additional time for both successful switching to the backup data channel and data transmission. However, due to the limitations affecting the current research, in which the backup channel is considered as part of future work, the process of data channel retransmission over a backup data channel is not considered.

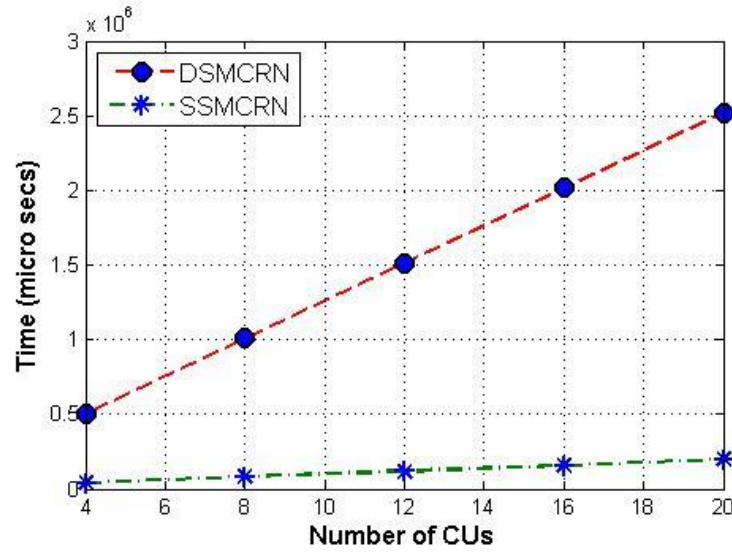


Figure 5-5: Time performance of DSMCRN and SSMCRN with and without LUs' activities

To summarise the communication time performance of both DSMCRN and SSMCRN, the execution of the security algorithms require additional time over the CCC and have led to slow switching to the SLDCHs. Consequently, the overall communication time significantly increases between a pair of CUs. However, the difference in the communication time of both protocols is based on different associated security algorithms, asymmetric and symmetric keys cryptography, which have different effects on the reservation time of the CCC for a pair of CUs. Thus, SSMCRN performed fast switching to the SLDCHs to initiate and complete 1500 bytes due to two discrepant factors; the first is the less time required to authenticate CUs using the shared key (symmetric key) compared to the CUs' validations approach that is based on the digital signatures, which rely on asymmetric key, in DSMCRN. The second relates to the number of the security frames that are encrypted using asymmetric keys in DSMCRN is higher than those in SSMCRN. Consequently, these two aspects led to an increase in the communication time in the DSMCRN compared to that in SSMCRN.

### 5.3.3. DSMCRN and SSMCRN throughput analysis

Throughput is a contributing factor used to analyse the performance of the MCRN protocol. Various parameters during the information transmission among entities within the control and data phases have a direct influence on the throughput.

These parameters are associated with and related to each other in terms of increasing and decreasing the network throughput value as explained in Table 5-3.

Table 5-3: Throughput parameters

Parameters	Notations	Relations to the throughput
Number of Transceivers	Tx and Rx	Two different transceivers (Tx and Rx) are assigned for CCC to observe the activities and selected Data Channels. This resulted in an increase in the network throughput.
Number of Licensed Data Channel(s) (LDCH)	LDCH	It significantly influences the time of successful data transmission. The required time to transmit data decreases when the multiple LDCH increase. This resulted in an increase in the network throughput.
Payload of Data (PD)	PD	It indicates the actual data transferred over the SLDCH and This resulted in an increase in the network throughput.
Data Rate (DR)	DR	Data rate (DR) for both the CCC and LDCH channels is set to 11Mbps. When higher DR is determined the larger size of data is transmitted and this resulted in an increase in the network throughput. More data can be transmitted when higher data rate is determined and this resulted in an increase in the network throughput.
Probability of Successful Access of Common Control Channel ( $P_{SCCC}$ )	$P_{SCCC}$	Higher probability of successful CCC access ( $P_{SCCC}$ ) for the authentication and control frames exchange over the CCC will reduce the communication time through the fast switching to the SLDCH. This resulted in an increase in the network throughput.
Time of Communication (T)	T	Higher Time of the Communication (T) over both the CCC and Selected Licensed Data Channels decreases the network throughput and vice versa.

Therefore, the throughput value is influenced by different parameters in which it is directly proportional to  $P_{SCCC} * PD * DR * T_X R_X * SDCHs$  and inversely proportional to  $T$ . Thus, it can be calculated from Equation 4:

$$\eta \propto \frac{P_{SCCC} * PD * DR * T_X R_X * SDCHs}{T}$$

Equation 4: Throughput value

Thus, two different scenarios, with and without LUs activities as part of network operations, are considered to evaluate the throughput performance and activities of the LUs' effect in each protocol.

### 5.3.3.1. Throughput analysis without LUs' activities

Figure 5-6 illustrates the throughput factor for both the DSMCRN and SSMCRN protocols for 20 CUs, based on five runs involving 4, 8, 12, 16 and 20 CUs. It is obvious that in both protocols, the number of the CUs, who participated in the communication process, has a direct influence on the throughput rate, leading to an increase in the rate of the message delivery, which affects the situation as the number of CUs increases. However, the throughput rate of the SSMCRN protocol increases significantly, and is higher compared to throughput in DSMCRN. The difference is then related to the smaller security execution time over the control channel, which leads to a fast switch to the selected data channel to initiate data transmission. In other words, the longer communication affects the control channel, and other aspects, which affect and delay the message transmissions, and result in lower throughput. This occurred in DSMCRN, which saw a slight increase in the throughput in each run, compared to SSMCRN.

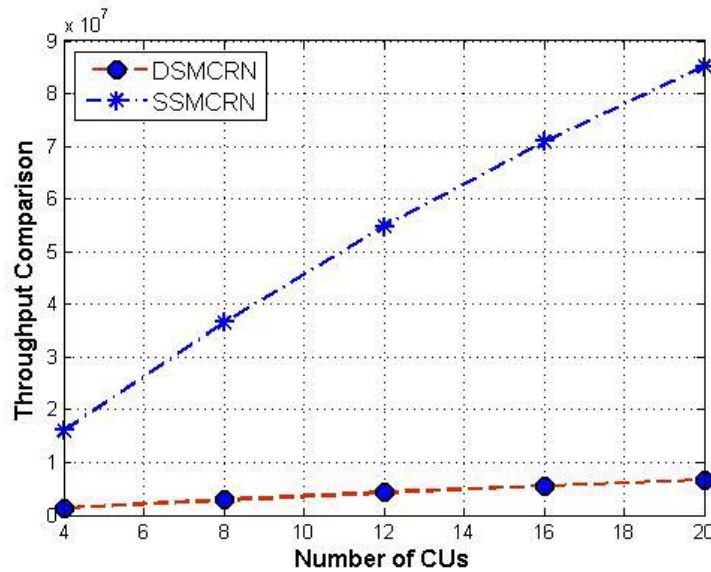


Figure 5-6: Throughput in DSMCRN and SSMCRN without involving LUs

### 5.3.3.2. Throughput analysis with LUs' activities

Figure 5-7 illustrates the throughput factor for both the DSMCRN and SSMCRN protocols, based on five runs, involving 4, 8, 12, 16 and 20 CUs, and LU activities in the communication process. As discussed previously, in Figure 5-6, the throughput rate is associated with the time taken to exchange and determine the

SLDCH in the control channel, in which it increases in cases where the time over the control channel decreases and vice versa. Additionally, it increases if the number of incorporated CUs intended to exchange messages over SLDCHs increases. However, the network throughput rate is also affected by the LUs, which have the priority for utilising the SLDCH, resulting in the vacancy of the SLDCH by the CUs, requiring an end to the transmitted message. This causes a low throughput rate, due to the unsuccessful message transmission over the SLDCH. This case occurred in the second run of both protocols, as shown in Figure 5-7, where 8 CUs are involved in the communication and a single SLDCH is utilised by the LUs. Although, the throughput values of both protocols increase in the second run, they are still lower than the throughput rate for the same run in the same protocols without LUs activities, as shown above in Figure 5-6.

Therefore, successful messages delivery increases significantly in SSMCRN, and reaches the same value in the scenario showing no LUs' activities involvement in the third run, where 12 CUs are involved. This is because the SLDCHs' availability for data transmissions belongs to 6 pairs of CUs. However, along the same run of 12 CUs, there is a slight increase in the throughput rate of the DSMCRN compared to the SSMCRN, which reaches the same value for the same run in the scenario, without the involvement of LUs activities. The difference in the increased results of the third run of both protocols relates to the time required for each protocol to access the control channel, which influences the throughput rate, as discussed in Figure 5-6.

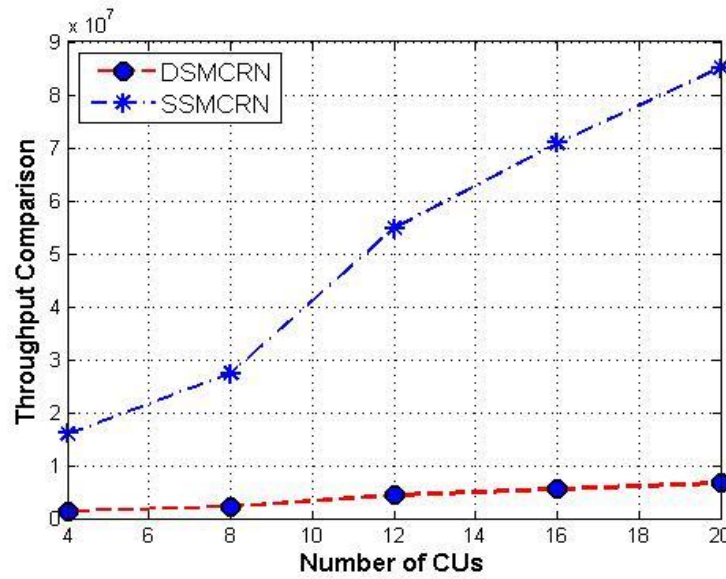


Figure 5-7: Throughput in DSMCRN and SSMCRN with LUs activities

To summarise the throughput in DSMCRN and SSMCRN protocols, in SSMCRN the throughput was significantly higher than that what was achieved by DSMCRN due to the less time required over the CCC. This time subsequently led to fast switching to the SLDCHs by CUs to initiate the data communication. Thus the relation between the time and throughput are associated together, and the more time required over the CCC will leads to low throughput rate and vice versa. Moreover, the appearance of LUs to utilise the SLDCH also affected the network's throughput since they have the priority to utilise the licensed channel. As a result, CUs were prevented from transmitting data over the SLDCH and led to decrease the network' throughput.

## 5.4. Impact of malicious users on DSMCRN and SSMCRN

The communication process for the entire network can be affected by associated malicious behaviours, since malicious activities affect the time required by both the control and data channels, resulting in a lower performance of the network. Modification and unauthorised access are the two types of attacks considered in this thesis, and these are analysed to investigate the extent of the impact on time and the throughput of both DSMCRN and SSMCRN.

### 5.4.2. Impact of modification attacks on the time taken to perform DSMCRN and SSMCRN

When applying the MAC algorithm in DSMCRN and SSMCRN, CUs can authenticate received messages by checking the integrity assurance of messages transmitted. Thus, the detection of any invalid message leads to retransmission of the frame, causing more time to elapse when delivering the transmitted frame, whether over the control or data channels. This is considered as a delay of successful message delivery between the intended CUs. Therefore, the scenario when applying modification attacks on COR, CTS and Data frames are applied in each proposed DSMCRN and SSMCRN.

#### 5.4.2.1. Modification attack in DSMCRN

Figure 5-8 demonstrates the differences in the communication time for a single pair of CUs in DSMCRN and DSMCRN with modification attacks applied. Evidently there is a significant delay, since the intended receiver detects the invalid received messages belonging to the COR, CTS and data frames. This increase the time by 2604.5 $\mu$ secs over both the control and data channels, as the validation process for these retransmitted frames is repeated, to insure the integrity of received messages.

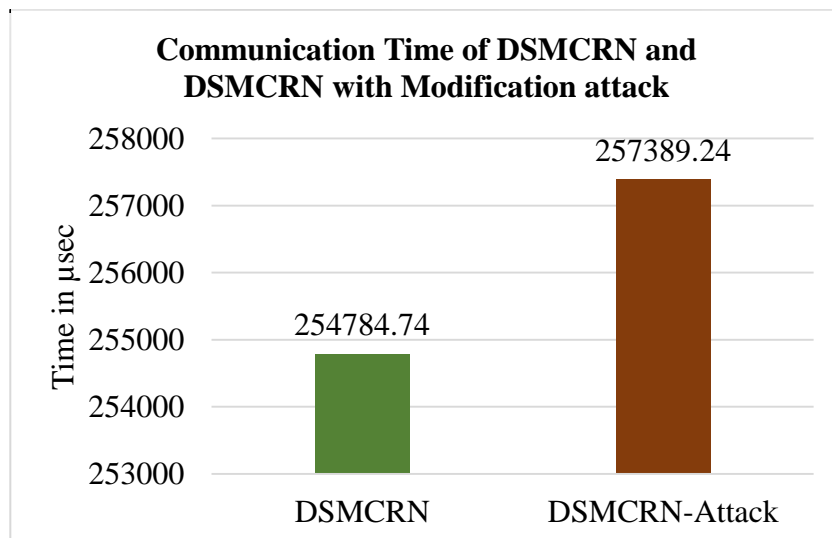


Figure 5-8: Communication time of a single pair of CUs in DSMCRN and DSMCRN with modification attack

However, Figure 5-9 shows the communication time in microseconds for five runs, involving 4, 8, 12, 16 and 20 CUs, without LUs activities in both DSMCRN and DSMCRN with modification attacks applied. Aside from what was discussed in Figure 5-3 for the time increase due to the applied security features, there is a slight difference in the communication times for both protocols, with modification attacks compared to the same protocols without attacks. As discussed in the Figure 5-8, this increase results from the retransmission of CUR, CTS and data frames, which requires more time in DSMCRN with a modification attack protocol. However, a slight difference is difficult to perceive clearly from the graph, since the delay time is still very small, compared to the actual security time.

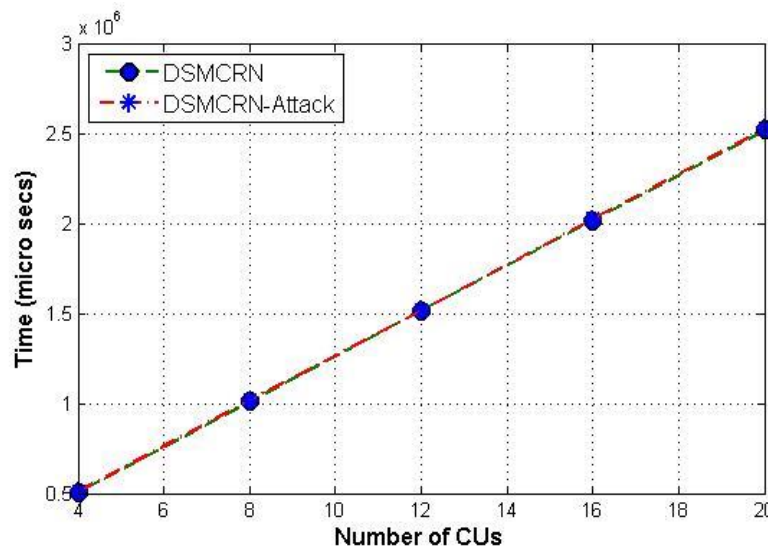


Figure 5-9: Communication time of 20 CUs in DSMCRN and DSMCRN with modification attack

#### 5.4.2.2. Modification attack in SSMCRN

Figure 5-10 illustrates the variation in the communication time for a single pair of CUs in SSMCRN and SSMCRN with modification attacks applied. The time required for successful message delivery in SSMCRN, with a modification attack is higher than the time taken for the message transmission in SSMCRN. This difference relates to the retransmitting of the COR, CTS and Data frames in SSMCRN, with modifications to attacks, for the validation of the integrity process applied to the messages received. Thus, the total delay time is equal to

2661.42 $\mu$ secs, over both the control and data channels in SSMCRN with the attack.

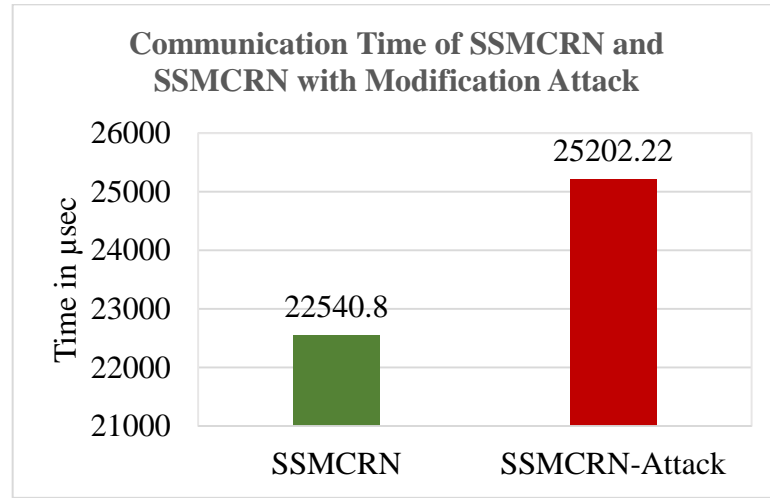


Figure 5-10: Communication time of a single pair of CUs in SSMCRN and SSMCRN with modification attack

However, Figure 5-11 describes the communication time in microseconds for five runs, involving 4, 8, 12, 16 and 20 CUs in both SSMCRN and SSMCRN, with modification attacks. As discussed previously in section 5.3.2, the time is associated with the number of CUs incorporated in the communication process, and it increases with each run, due to the increase in the participating CUs, in both SSMCRN and SSMCRN with a modification attack. However, it is notable that the SSMCRN with modification attacks time is higher than the time for SSMCRN in each run. This increase is considered to represent a delay, which has occurred over both control and data channels, because of the mandatory retransmitting of three modified frames recognised as CUR, CTS and Data frames. Moreover, the difference in the time for the 5<sup>th</sup> run is 10 times that of the 1<sup>st</sup> run, due to the increase in the number of modified frames belonging to 10 pairs of senders and receivers. Thus, the increase in communication time depends on relationship between the time and number of modified and retransmitted frames.

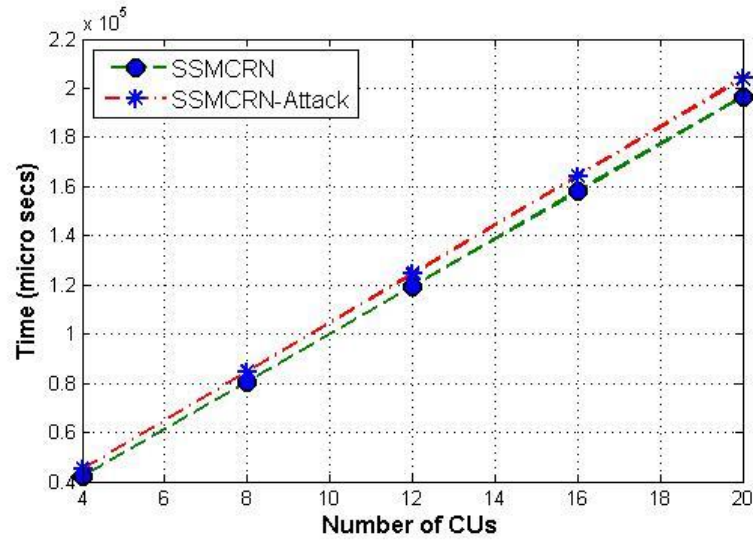


Figure 5-11: Communication time of a 20 pair of CUs in SSMCRN and SSMCRN with modification attack

### 5.4.3. Impact of modification attacks on the throughput of DSMCRN and SSMCRN

Since the time for the proposed protocols performance is affected by the modification attack, the throughput aspect might also be influenced as it is related to performing the fast switch to the SLDCHs. Therefore, the message delivery rate in both the DSMCRN with modification attack and the SSMCRN with modification attack were analysed as follows:

#### 5.4.3.1. Throughput in DSMCRN with modification attacks

Figure 5-12 illustrates the successful messages delivery rate in both DSMCRN and DSMCRN with the attack for five runs, including 4, 8, 12, 16 and 20 CUs. It was discussed previously in Figure 5-6 that throughput rate increases if the number of message transmissions increases over the multiple available SLDCHs. Thus, it is evident that both trends increase significantly in each run, due to the number of data packets exchanged over the SLDCHs. The increase pattern remains the same in each run, due to the availability of the selected channels and the LUs activities, which are OFF during each run. However, as soon as the throughput rate is effected by the time over the control and data channel, the modification attack for the transmitted messages in COR, CTS and Data frames

increases the time resulting from the frames' retransmissions and the associated security algorithms for both the decryption and the messages for integrity assurance. Therefore, the throughput rate for DSMCRN with modification attack is slightly lower than the throughput for the same protocol without the attack. This slight difference is difficult to perceive clearly from the graph, since the time is still very small, compared to the actual security time.

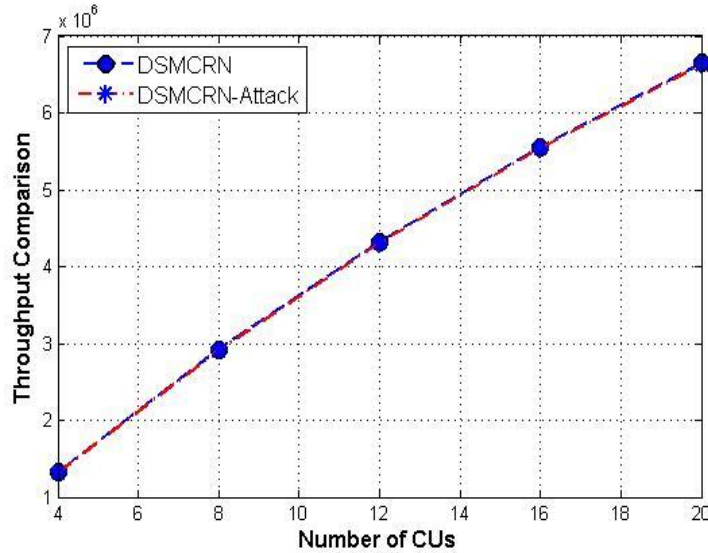


Figure 5-12: Throughput for 20 pair of CUs in DSMCRN and DSMCRN with modification attack

#### 5.4.3.2. Throughput in SSMCRN with modification attack

However, Figure 5-13 shows the same throughput factor as SSMCRN and SSMCRN with the attack for five runs, including 4, 8, 12, 16 and 20 CUs. The same discussion for Figure 5-12 above is applied here in terms of the relationship between the throughput rate and the number of contributing CUs, who admit to transmitting and receiving messages. Therefore, it can be observed that in both trends, the message delivery rate increases as soon as the number of participating CUs transmitting and receiving messages is increased. However, the main difference is that the successful messages delivery rate, in SSMCRN with modification attack, is lower than the throughput in SSMCRN, due to the modified messages in COR, CTS and Data frames, leading to extra time being required for retransmitting the messages over the control and data channels. Based on this, the difference in the throughput varies in each run for both trends, this is due to the increase in the modified messages in SSMCRN with modification of

the attack in each run; there are 6 modified messages in the 1<sup>st</sup> run, 12 modified messages in the 2<sup>nd</sup> run, 18 modified message in the 3<sup>rd</sup> run, 24 modified messages in the 4<sup>th</sup> run and 30 modified messages in the final run.

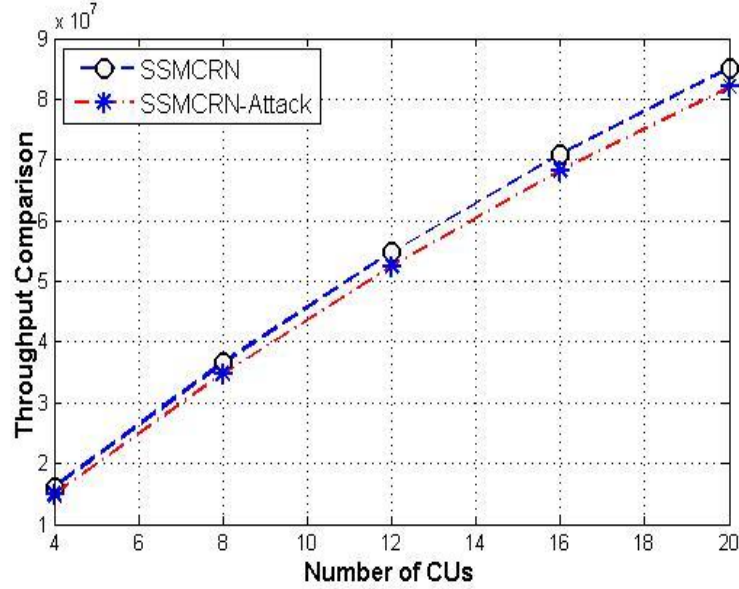


Figure 5-13: Throughput for 20 pair of CUs in SSMCRN and SSMCRN with modification attack

To conclude the impact of modification attacks on the throughput of DSMCRN and SSMCRN, the message delivery rate is associated with the time taken over both control and data channels. Thus, the correlation can be explained as the throughput is inversely proportional with the required communication time and the decrease in throughput depends on relationship between the time and number of modified and retransmitted frames in both protocols.

#### 5.4.4. Impact of unauthorised access on the time performance of DSMCRN

Unauthorised access by malicious users, who have not registered and obtained authorised access information, can affect the network performance, resulting in a delay in the overall communication process for the other CUs. This delay resulted from the failure of successful authentication by the dedicated server, which makes the CCC busy for others waiting for the contention process to launch ITA frames. Therefore, both throughput rate and total successful communication time include authentication, and exchanging both control information and data, that is affected

by malicious users, since they contribute to the communication process with other valid CUs. In the unauthorised access scenario, it has been assumed that malicious user usually communicates with a valid CU, and we do not consider the situation of 2 malicious users communicating with one another. Two different cases, which have different numbers of invalid users involved in the communication over the CCC by transmitting ITA frames for initiating communication with other CUs, are considered to investigate their influence on the network's performance. Therefore, the first case includes only 1 invalid user in the communication process, while 6 malicious users are considered in the second case.

#### **5.4.4.1. Communication time in DSMCRN with unauthorised access**

Figure 5-14 shows the successful communication time for 20 users over both control and data channels in five different runs, consisting of 4, 8, 12, 16 and 20 users, in which the case of 1 malicious user on the 4<sup>th</sup> run is considered. Generally, the increase in each run occurs due to the increase in participating CUs in the communication process, which arises when exchanging both the control and data frames phases. However, it is evident that the increase in the communication time affected the 4<sup>th</sup> run, in which 7 out of 8 pairs of CUs successfully completed their communication processes over both the CCC and data channel, the difference is obvious compared to the same run in case showing no malicious users involvement in the communication of the DSMCRN, as shown previously in Figure 5-5. This is because of the detection mechanism of unauthorised access by a malicious user who transmits the ITA and fails to be authenticated by the server after receiving the RTA. Therefore, the receiver is updated by the status of the sender to halt the process of communication with that particular user. This process requires time over the control channel, and affects other legitimate users from using the CCC channel and transmitting their ITA frames.

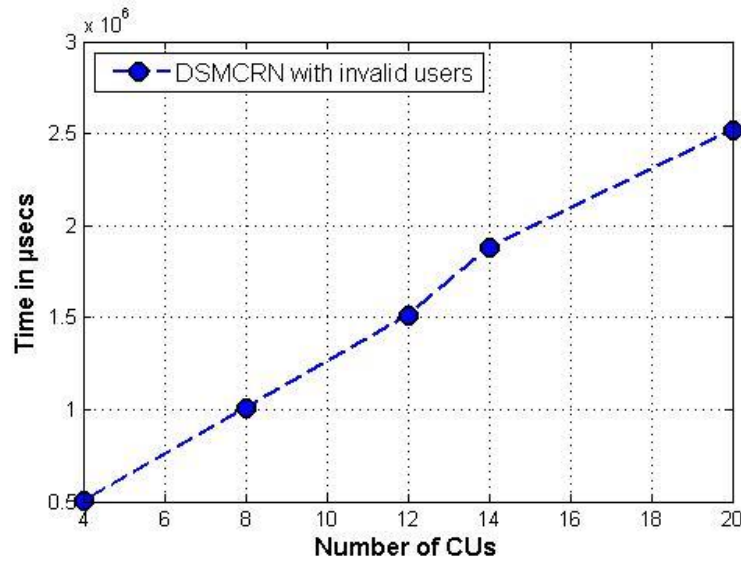


Figure 5-14: Communication time for 20 pairs of users, including 1 malicious user in DSMCRN

Figure 5-15 shows the communication time for 20 users over both the control and data channels in five different runs, consisting of 4, 8, 12, 16 and 20 users; in which the cases of 1, 2 and 3 malicious users in the 3<sup>rd</sup>, 4<sup>th</sup> and 5<sup>th</sup> runs are considered respectively. Although, the communication time increases in each run, due to the increase in the number of CUs participating in the communication process, it experienced a different increase pattern in the 3<sup>rd</sup>, 4<sup>th</sup> and 5<sup>th</sup> runs, where the malicious users participated in the communication process. This creates a delay resulting from unsuccessful authentication processes, leading to termination of the communication before the control information can be exchanged with the malicious users. For example, the first run indicate 4 CUs successfully communicating with each other and requiring time equal to  $0.5 \times 10^6$   $\mu\text{secs}$ , while the second run involves 8 CUs that are successfully authenticated and exchange their data in  $1 \times 10^6$   $\mu\text{secs}$ .

In contrast, in the third run, only 10 valid users out of 12 successfully completed their communication over both the control and data channels, since 1 malicious attempt to make unauthorised access was detected by the server, resulting in stopping the communication process. Thus, the total time for the run requires  $1.4 \times 10^6$   $\mu\text{secs}$ , including the detection process. Therefore, 139003.61  $\mu\text{secs}$  refers to the detection time over the control channel for the 6<sup>th</sup> pair of users, which includes 1 malicious and 1 valid CU user.

However, the 4<sup>th</sup> run, which involves 16 users in the communication, only 12 valid CUs communicated and exchanged their data successfully, since 2 malicious users were detected and banned from continuous communication with other valid users. Therefore, the total communication time, including the detection process, was  $1.75 \times 10^6 \mu\text{secs}$ . Regarding the last run, in which 20 users were communicating, only 14 CUs successfully exchanged data and three invalid users (senders) were banned from the communication process as soon as the recipients CUs were updated because of failed authentication. Thus,  $2.15 \times 10^6 \mu\text{secs}$  is the time required to successfully complete the communication time for the last run.

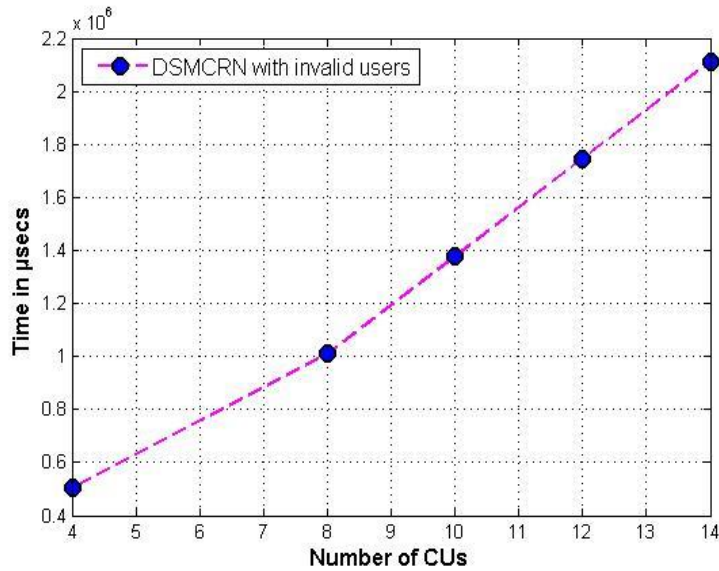


Figure 5-15: Communication time for 20 pair of users include 4 malicious users in DSMCRN

#### 5.4.4.2. Throughput in DSMCRN with unauthorised access

Figure 5-16 shows the throughput rate for 20 users in five different runs, consisting of 4, 8, 12, 16 and 20 users, in which the case of 1 malicious users being present in the 4<sup>th</sup> run is considered. Despite the successful messages delivery rate increasing significantly for the 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> and 5<sup>th</sup> runs, due to the number of successful data exchanges among the intended destinations, there was a slight increase noted in the throughput rate of the 4<sup>th</sup> run, because only 14 out of 16 users successfully exchanged their data over the selected data channels. This decreased the message delivery rate, especially when the detection time over the control channel involved and has direct influence on the throughput compared to

the same run in case showing no malicious users involvement in the communication of DSMCRN in Figure 5-12.

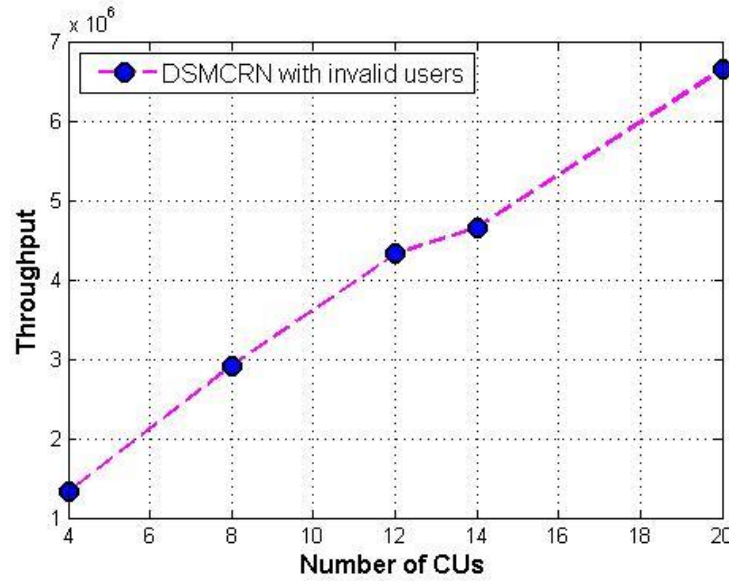


Figure 5-16: Throughput for 20 pair of users include 1 malicious user in DSMCRN

However, Figure 5-17 shows the throughput rate for 20 users in five different runs, consisting of 4, 8, 12, 16 and 20 users, in which the cases of 1, 2 and 3 malicious users in the 3<sup>rd</sup>, 4<sup>th</sup> and 5<sup>th</sup> runs respectively are considered. The figure shows a significant increase in the throughput rate for both the 1<sup>st</sup> and 2<sup>nd</sup> runs, due to the quantity of successful data exchanged over the SLDCHs in each run. However, the increasing pattern did not remain same in the others runs, which all have less successful message delivery rate compared to the same runs in the situation showing no malicious user's involvement in the DSMCRN. This is because of the malicious users' detection, which results in terminating the communication process before the control and data exchanged. Subsequently the throughput rate decreased since there was no data exchange with unauthorised users. Thus, only 5 pairs out of 6 in the 3<sup>rd</sup> run, 6 pairs out of 8 in the 4<sup>th</sup> run and 7 pairs out of 10 in the final run which the CUs complete the data exchange successfully.

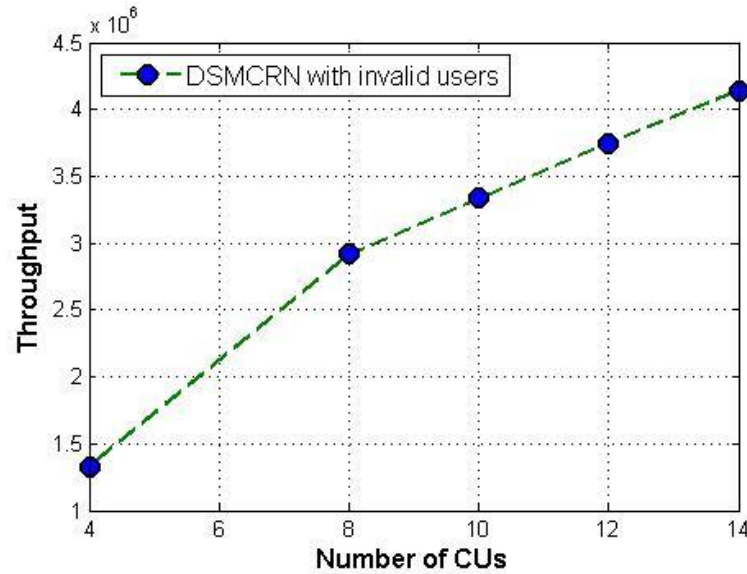


Figure 5-17: Throughput for 20 pair of users include 4 malicious users in DSMCRN

To summarise the impact of unauthorised access by malicious users, both communication time and throughput can be affected by unauthorised access. Although, the detection process requires a time to proceed, which affects the entire network by increasing communication time, there is no data exchanged with the detected malicious users and resulting in a decrease of the message delivery rate.

## 5.5. Discussion of DSMCRN and SSMCRN

The network performance for the proposed DSMCRN and SSMCRN was affected by two main factors, which have a strong relationship to the throughput rate and the communication time. The first factor is related to the applied security features, which differ to some extent in each protocol, while the second belongs to the frames' sizes for each protocol. These security features involved encryption and authentication procedures, operating according to different approaches in the proposed protocols. For instance, some of the encryption processes in DSMCRN were based on applying the RSA algorithm, which operates based on a large key size equal to 1024, required for encrypting and decrypting a message. This necessitates a significant time for performing the task, and results in increasing the communication time for the proposed protocols. Thus, there were three implementations of RSA in DSMCRN, in IOR, ITA and RTA, but only the IOR

frame in SSMCRN. Moreover, the authentication process in DSMCRN is based on the digital signature implementation, which requires a multi process generation and verification of each signature belonging to each CU, while it is based on only the decryption of the received RTA frame in SSMCRN. Thus, the time required to perform the authentication in DSMCRN was significantly higher than the authentication time in SSMCRN, since it requires an average time equals to 870.045 $\mu$ secs and 55260.54 $\mu$ secs, for generating and verifying each digital signature respectively in DSMCRN, and 219.98 $\mu$ secs for authenticating both the sender and receiver in SSMCRN.

The need to apply the RSA and AES for the authentication process in DSMCRN and SSMCRN also affected the transmitted frames size. For instance, the sizes of the ITA and RTA frames in DSMCRN were 86 and 150 bytes respectively, while they were less in SSMCRN, and equal to 66 and 110 in the same ITA and RTA frames respectively. Therefore, both the security and frames sizes applied considerably affected the messages transmission time over the control channel, and resulted in faster communication in SSMCRN compared to the DSMCRN.

On the other hand, the network throughput rate was affected by the associated security and communication time taking over the control and data channels. Since, more time is taken over the control channel, this leads to a lower throughput rate, especially once a large number of CUs are involved in the communication process. This is because the control channel becomes busy when exchanging both the security frames that belong to the authentication process, and the other two frames belonging to the FCL and SLDCH for each pair of CUs. Although, the security time and data frames sizes in the data phase are the same in both DSMCRN and SSMCRN, SSMCRN achieves a better throughput rate compared to DSMCRN, since the overall communication time over CCC is less. Thus, Table 5-4 shows the time over both the control and data channels, and the differences in throughput rate in both DSMCRN and SSMCRN for each run, which include 4, 8, 12, 16 and 20 CUs.

## Medium Access Control (MAC) for DSMCRN and SSMCRN

Table 5-4: The differences in the time and throughput of DSMCRN and SSMCRN

Number of CUs in each run	DSMCRN		SSMCRN	
	Time (ms)	Throughput	Time (ms)	Throughput
4 CUs	506.38	$1.3262 \times 10^6$	41.89	$1.6035 \times 10^7$
8 CUs	1009.55	$2.9182 \times 10^6$	80.59	$3.6566 \times 10^7$
12 CUs	1512.75	$4.3212 \times 10^6$	119.29	$5.4812 \times 10^7$
16 CUs	2015.94	$5.557 \times 10^6$	157.99	$7.0926 \times 10^7$
20 CUs	2519.13	$6.6456 \times 10^6$	196.69	$8.5137 \times 10^7$

Since both protocols have different mechanisms to authenticate CUs, they contribute in addressing the security threats in CRNs. Therefore, Table 5-5 below describes and compares the methods of addressing the security threats and providing defence against most of the related MAC layer's attacks in DSMCRN and SSMCRN.

## Medium Access Control (MAC) for DSMCRN and SSMCRN

Table 5-5: Contributions regarding the security threats and countermeasures in DSMCRN and SSMCRN

Security requirements and threats	DSMCRN	SSMCRN
Authentication	Authenticate CUs through the applied digital signature	Authenticate CUs through the applied network's shared key, which is obtained in the registration process
Secure communication	Different symmetric keys are generated for securing the registration, authentication and control information exchange and data transmission processes. Asymmetric key also is applied to secure the messages' transmissions to the dedicated server.	
Data Integrity	Message Authentication Code algorithm is applied in the protocol phases to ensure the authenticity and data integrity of the transmitted messages	
DoS Attack	Encrypting and making the FCL and SLDCH unreadable to a malicious user, who attempts to make the SLDCH busy, increases the chance of data transmission over the SLDCH.	<ul style="list-style-type: none"> <li>• Encrypting and making the FCL and SLDCH unreadable to a malicious user, who attempts to make the SLDCH busy, increases the chance of data transmission over the SLDCH.</li> <li>• Reducing the Request-To-Authenticate frame which intended to be transmitted to the server through applying a Prior authentication of the sender in the receiver side.</li> </ul>
Non-repudiation	Authenticating both senders and receivers through verifying their digital signatures will ensure non-repudiation.	After authenticating both the sender and receiver and generating a shared key for only this pair of CUs in order to applying and generating a MAC-key based on both the user's ID and the message, which they will be encrypted, non-repudiation would not be violated.
Compromised-Key Attack	The control information and data transmission are encrypted with different shared keys to increase the level of the security and each pair of CUs uses a shared key once for exchanging both control information and data	
Spectrum sensing data manipulation/falsification Attack	Encrypting both the FCL and the associated MAC-key ensure the authenticity of the transmitted message and detecting any manipulation has been occurred on the received message.	
Forgery Attack	Authenticating both the sender and receiver through the applied digital signature provides defence against forged messages.	Authenticating both the sender and receiver through the applied network shared key provides defence against forged messages.

Table 5-6: Contributions regarding the security threats and countermeasures in DSMCRN and SSMCRN (cont.)

Modification Attack	Generating and encrypting a MAC-key for each transmitted message leads to validate the received data at the receiver side by checking the authenticity and integrity of the received message.
MAC address Spoofing Attack	Both protocols provide the authentication mechanisms of both senders and receivers in which the user's identity along with the MAC-key is associated with the transmitted messages in encrypted format for the message validity and integrity.
Unauthorised Access Attack	Authenticating both senders and receivers through verifying their digital signatures limits the networks access to only authorised users.
Jamming Attacks	Reducing the possible interference that can be created by malicious users and leads to DoS through encrypting and hiding both the FCL and SLDCH.
Eavesdropping Attack	The applied authentication mechanisms and encryption of the transmitted messages strongly assist and work against intercepting the communication process by an attacker for gaining access to data. The encryption mechanism makes these encrypted messages useless for the attacker.
Data Tamper Attack	Apart of the authentication, avoiding the wrong decision made by the spectrum management through encrypting and ensuring the integrity of the transmitted FCL and SLDCH.

## 5.6. Summary

This chapter has described evaluation of the DSMCRN and SSMCRN proposed protocols in reference to two main factors associated with the network performance. These factors were the communication time over both the control and data channels and the successful message delivery rate. In addition, two alternative scenarios, with and without LUs activities over the data channel were considered for the proposed protocols, to analyse the LUs impact on the communication time and throughput. The comparison of both protocols with and without the potential modification attack occurrence and its impact on the network performance were analysed. The current chapter also examined unauthorised access in DSMCRN, in which has a significant influence is placed on the communication time and decreasing the throughput rate. The chapter was concluded by highlighting the main differences between DSMCRN and SSMCRN operations in terms of the security execution time, when obtaining throughput for multiple runs including different participatory CUs.

In this chapter, several contributions of this research were achieved when the proposed security protocols provided defence against different types of threats related to the MAC layer that aimed to launch DoS attacks to deteriorate the network performance. These can be summarised as follows:

- 1- Both DSMCRN and SSMCRN performed successful secure communication among only valid CUs through the associated security features, and selected the best data channel according to the criteria of the highest channel availability that led to increasing the network throughput.
- 2- DSMCRN performed defence against unauthorised access by malicious users and successfully detected the invalid users who were prohibited from continuing the communication with valid CUs. This led to protecting the network resources.
- 3- Both protocols protected the sensing results from any modification that can be occurred during their transmission. Since the detection mechanism on the modification of the FCL prevented incorrect decision making of the licensed data channel based on the defined selection criteria, while the detection on SLDCH protected the network from DoS attacks. This protection was achieved by ensuring the integrity and authenticity of the transmitted control messages among CUs.
- 4- Protecting and hiding the channel sensing results, which is considered one of the network components and resources, from adversary users (internal and external) by limiting the recognition of the FCL and SLDCH to only the sender and receiver CUs, so that protect the availability of the SLDCH to this pair of CUs and reduces the chance of making the SLDCH unavailable or launching interference (jamming attacks) to the CUs. This led to increasing the network throughput.
- 5- Reducing the communication time of malicious users over the control channel in SSMCRN. This was done by applying fast detection (pre-authentication) at the receiver side to protect the server from receiving fake control frames from the CUs, since these frames can lead to increase the overload of the network and server. Thus, detection is performed in the earliest stage once the malicious user transmit ITA frame for requesting

and setting the communication with a CU. It significantly ensured the credibility of the robust security features that are integrated with the protocol. However, there was no need to launch an attack based on unauthorised access while the receiver has the accountability to pre-authenticate the sender by using *the network's shared key* to decrypt the received content of the ITA frame. If the decryption has proceeded successfully then the RTA frame is sent to the dedicated server for the final authentication and obtaining the security key assigned for those pair of CUs. Therefore, the early stage of detecting malicious users, who attempt to obtain the advantages of the network components and its resources will:

- Reduce the communication over the CCC and make it available for others instead of transmitting RTA to the server for validating the sender.
- Protect the server from receiving unauthentic frames, which leads to increase the server's overload.

The next chapter will deliver a comparative analysis of the proposed and two benchmarks protocols, with and without incorporating the security features. Thus, the MCRN, which was discussed in chapter 3, will be compared with two benchmark protocols. In addition, two versions of the security features have been added to both the proposed MCRN and resulting in introducing two versions of security protocols recognise as Digital-signature based Secure MAC protocol for CRNs (DSMCRN) and Shared-key based secure MAC protocol for CRNs (SSMCRN) that were discussed in the current chapter will be compared with the two benchmarks after adding the security algorithms.

## Chapter 6 COMPARATIVE ANALYSIS OF THE PROPOSED AND BENCHMARK PROTOCOLS

Since the proposed MCRN was designed and detailed in section 3.2, its simulation part and performance analysis are introduced in this chapter. The chapter also presents two different comparative approaches, to highlight the differences between the proposed and the benchmark protocols, with and without security features included. The details of the benchmark protocols operations before and after incorporating two versions of the security features will be provided. In addition, the chapter includes an evaluation of the throughput analysis and time performance, which are both considered significant factors in research aiming to evaluate proposed protocols for comparison with benchmark protocols. The comparisons consider two different scenarios; over the selected data channels: with and without LUs activities.

### 6.1. Simulation and performance evaluation of the MCRN

The same discussion of both the simulation part and network parameters that were introduced in sections 5.3 and 5.3.1 are applied here for the MCRN and benchmark protocols without security. Thus, Table 6-1 gives the frames and their sizes that are used in the MCRN protocol.

Table 6-1: MCRN frames

Name of the parameter	Value	Description
RTS	20 bytes	Request-To-Send frame
CTS	20 bytes	Clear-To-Send frame
Data	1520 bytes	Data frame
ACK	20 bytes	Acknowledgement frame

The pseudo code of the proposed MCRN protocol is shown as follows:

## MCRN protocol pseudo code

```

=====
1. Wait for Random time
2. IF RTS found
    Then Go To 4
    Else Send RTS
    Endif
3. Check IF CTS received
    Then Go To 7
    Else Go To 1
    Endif
4. IF the RTS for him/her self
    Then Send CTS
    Else wait for NAV time, then Go To 1
    Endif
5. Switch to SLDCH
6. IF LU is ON
    Then wait for expiring time, then Go To 1
    Else Go To 7
    Endif
7. Transmit/Receiving Data
   Go To 1
=====

```

### 6.1.1. Channel sensing results

Figure 6-1 demonstrates the white spaces and the LUs' activities over the licensed data channels. The spectrum sensing results of these channels are determined by CUs, who are contributing in the communication process to observe the LUs' activities over these channels. In each channel, the X-axis represents the duration of the LUs' activities in microseconds while the Y-axis shows the amplitude of the LUs' activities (the signal strength is represented by the American Standard Code for Information Interchange, ASCII, format (Injosoft, 2015) since the LUs activities pattern falls out of the scope of this thesis). Therefore, each CU senses the 10 channels and records the channels' status that is whether the LUs are ON or OFF. The green area indicates the LUs activities over each channel and signals that the channel is ON whereas the white area refers to the availability of the channel with the LUs being OFF. Thus, the channels' holes are easily determined and enable the launch of data transmission based on previous channel prediction. For instance, in channel 1 most of the channel status is not efficiently utilised and an LU appears to be ON at the time of  $1.9 \times 10^4 \mu\text{secs}$ ; however channel 10 has less

### **Comparative analysis of the proposed and benchmark protocols**

availability because the LU is ON during most of the recorded period. In this case CUs consider channel 1 as the highest priority and the most reliable channel for data channel selection criteria due to its higher availability than others and the possibility of successful data transmission between a pair of CUs increase. In contrast, channel 10 is recorded as the lowest priority due to its low availability because the LU is ON for most of the duration. This decreases the chance of successful data transmission between a pair of CUs.

## Comparative analysis of the proposed and benchmark protocols

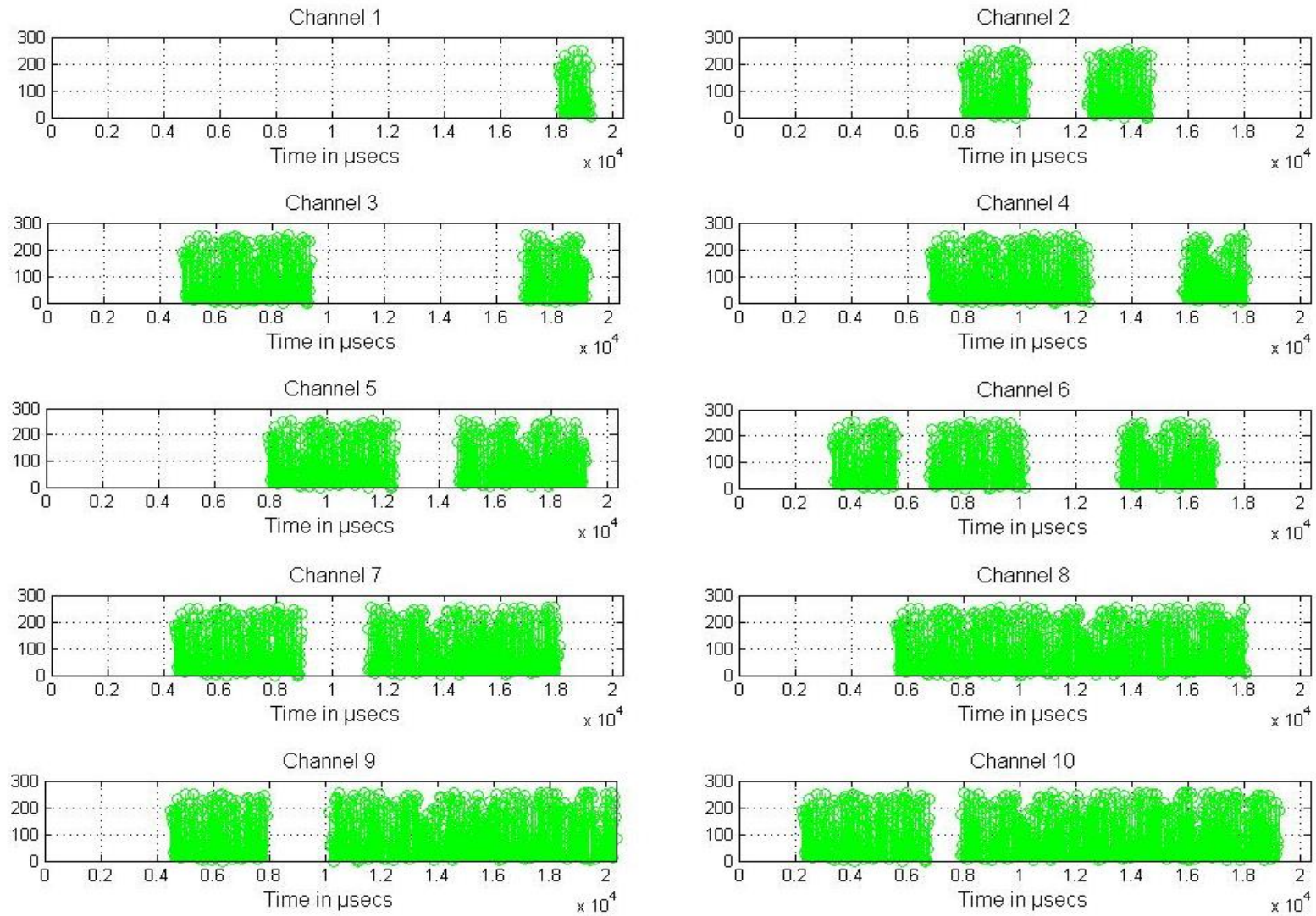


Figure 6-1: Recording LUs activities over licensed data channels

### **6.1.2. Control channel activities**

The effect of the control channel activity is based on the number of CUs attempt to content and reserve the channel to exchange the control information. It is obvious that each pair reserves the control channel for a specific time duration as they are required to send only the RTS and CTS frames. Thus, the channel is simultaneously occupied by different pairs of CUs as soon as it becomes idle. The control channel availability depends on the number of associated CUs who need to initiate communication. Therefore, each pair of CUs requires 109.91µsecs, while 10 pairs require 1099.1µsecs in all to exchange their control frames.

In order to calculate the required time to successfully exchange control information over the CCC ( $T_{CCC}$ ) between the sender and receiver, the following Equation 5 is applied in MCRN protocol.

$$T_{CCC} = \{T_{DIFS} + T_{RTS} + T_{CTS} + 2 * T_{SIFS}\}$$

Equation 5: Time to successfully exchange control frames in MCRN

### **6.1.3. Probability of successful access of common control channel**

The most significant part of the CRNs is the exchange of the control information belonging to FCLs among CUs in order to determine the criteria of selecting the appropriate data channel to initiating the data transmission. This FCL is referred to as control information and is exchanged over a CCC. The CCC access mechanism in the proposed MCRN is based on the IEEE 802.11 wireless standard (Dappuri & Venkatesh, 2014). However, a large number of CUs, which attempt to access the CCC, decrease the Probability of Successful Access due to possible collisions. Therefore, the transmission process is initiated solely when the idle time of the CCC is equivalent to the DIFS time. However, when there is a collision, CUs necessitate the selection of a random back off time from the range  $[0, CNT_{Window} - 1]$  where  $CNT_{Window}$  indicates the size of the Contention Window ( $CNT_{Window}$ ) which is set to 32 in the MCRN. The following Equation 6 is derived from (Vu & Sakurai, 2006) and belongs to the collision probability ( $P_{CCC}$ ) of the contention process to access the CCC by CUs.

$$P_{CCC} = (1 - \frac{1}{CNTWindow})^{N_{CUs}-1}$$

Equation 6: The collision probability of the contention process to access the CCC

In order to avoid collision of CUs for CCC access, the Equation 7, which is derived from (Vu & Sakurai, 2006), is used to contribute to the Probability of Successful Access of Common Control Channel (PSCCC). Where  $N_{CUs}$  signifies the number of CUs trying access CCC.

$$P_{SCCC} = 1 - (1 - \frac{1}{CNTWindow})^{N_{CUs}-1}$$

Equation 7: The probability of successful access of CCC

#### **6.1.4. Communication time over control and data channels**

Figure 6-2 shows the communication time over the control and data channels for each pair of CUs. Each pair exchanges 1500 bytes of payload after the data channel is determined. Therefore, the total time to successfully exchange the control information within the RTS and CTS and 1500 bytes of data for the first pair of CUs (CU1 and CU2), who first won in the channel contention process, is 1242.82μsecs.

However, the second pair of CUs (CU9 and CU10), who the second winner in the control channel contention, requires a waiting time equal to 109.91μsecs to access the CCC as it is reserved for the first pair of CUs and the channel is vacated after this period of time. Then both the sender (CU9) and receiver (CU10) necessitate 1242.82μsecs to successfully complete the data communication.

The waiting time to launch the RTS frame belonging to Group 3 of CUs (CU11 and CU12) is doubled to 2\*109.91μsecs since the control channel is busy exchanging four control frames belonging to Groups 1 and 2. In addition to this time, the third pair of CUs also requires 1242.82μsecs to complete their entire communication over both channels. This process is repeated for the remaining 7 groups of CUs including the waiting time for the control channel to be vacated and available for the next pair of CUs in order to avoid any collisions.

## Comparative analysis of the proposed and benchmark protocols

In order to calculate the total required time to exchange the control and data phases of the MCRN protocol ( $T_{MCRN}$ ) between senders and receivers successfully the following Equation 8 is applied.

$$T_{MCRN} = \{T_{DIFS} + T_{RTS} + T_{CTS} + T_{Data} + T_{ACK} + 3 * T_{SIFS}\}$$

Equation 8: Total time to successfully exchange control and data frames in MCRN

Comparative analysis of the proposed and benchmark protocols

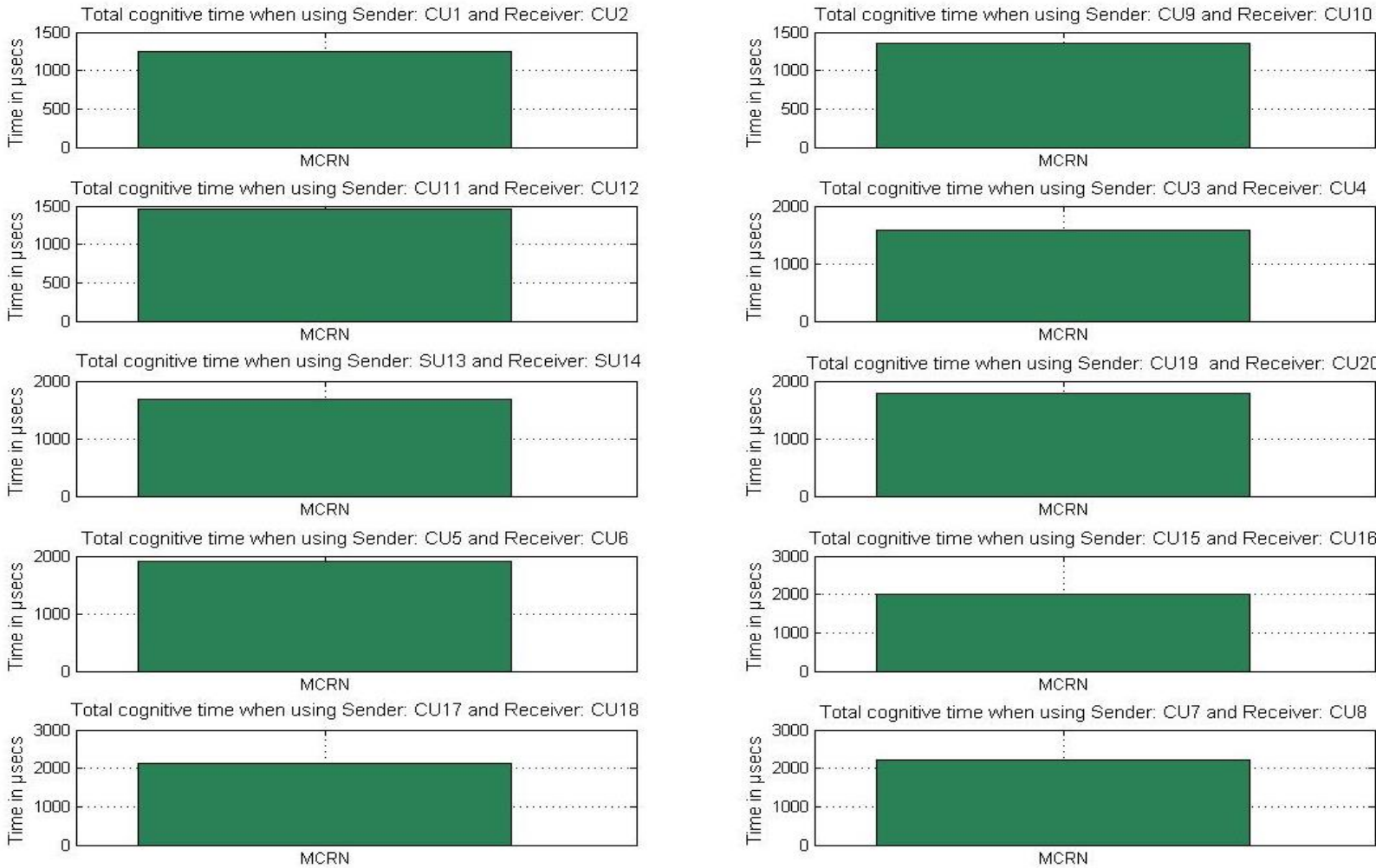


Figure 6-2: Total communication times for 10 pairs of CUs over control and data channels

However, Figure 6-3 demonstrates a scenario in which the communication activities of 10 pairs of CUs, and the prediction activities of LUs take place over 10 data channels. In each data channel, the x-axis explains which LUs are busy and which have free time; the green areas show the busy signals for the LUs and the remainder are available to the CU. Therefore, the red areas represent the CUs activities in the white space in each channel. However, the y-axis shows the amplitude of the LUs' and CUs' activities (the signal strength is represented by the ASCII format).

As discussed in (Hussein, et al., 2013) CUs are allowed to share the spectrum with LUs with some restrictions such as the transmitted power's limitation. Thus 20 CUs are involved in the communication and initially two users, who won in the channel contention process perform the successful exchange of the control information over the CCC and select a data channel based on the highest available time as shown in channel 1 while the rest of CUs wait until the first group moved from the control to the data channels. Then, again contention process starts and only one CU wins the contention, which then leads to exchange the control information between the next pair of CUs and so on. Generally, channel 1, which is occupied by the first group of CUs; CU1 and CU2, has the maximum time of availability since LUs utilise the current channel after a period of time equal to  $1.9 \times 10^4 \mu\text{s}$ . This makes this channel is the most reliable data channel for the first pair of CUs to transmit the data. In contrast, channel 10, which is occupied by the last pair of users, CU11 and CU12, has the lowest time availability in which the LU is predicted to appear in approximately  $0.2 \times 10^4 \mu\text{s}$  and this results in channel 10 having the lowest priority in terms of data channel selection criteria. Although the time of the CU activities over these channels is equal, since they have the same size of data to exchange, their communication process is initiated at different times based on the waiting time of the control channel's availability. For instance, the first pair of CUs utilises the CCC immediately after the successful contention process for the channel utilisation while the last pair of CUs (CU11 and CU12) had to wait  $9 \times 109.91 \mu\text{s}$  to content the CCC and initiate their communication over CCC and SLDCH respectively. The time required over the

### **Comparative analysis of the proposed and benchmark protocols**

control channel would influence the data channel availability since the LUs have priority to utilise the licensed data channel at any time.

## Comparative analysis of the proposed and benchmark protocols

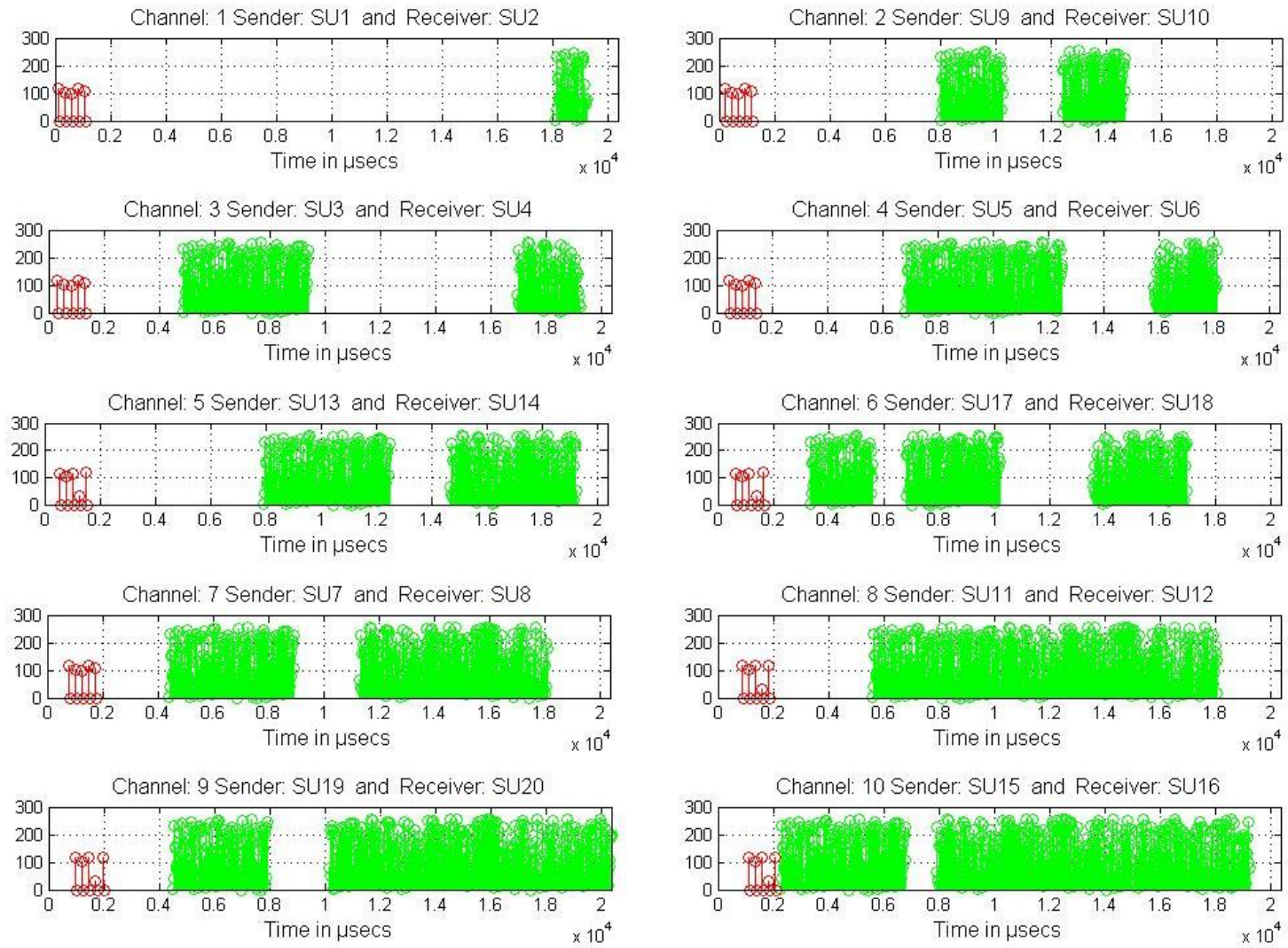


Figure 6-3: 1500 bytes of Data activities over the SLDCHs (Red colour represents CUs activities and green colour represents the LUs activities)

However, Figure 6-4 shows the overall time in microseconds which is required for 20 CUs to successfully complete the communication process in the MCRN protocol. This time refers to both the period over the CCC for control frames exchange and the period over the SLDCHs for data transmission for 10 pairs of CUs. Both the number and the sizes of the control frames significantly affect the time of the frames exchange between two CUs. Moreover, the overall time increases with the number of participating CUs. This is common sense where each sender wins contention for accessing the CCC to launch their RTS and CTS frames for channel selection and this requires 109.91 $\mu$ secs where each pair needs 1132.91 $\mu$ secs to exchange their data and ACK frames over the SLDCH.

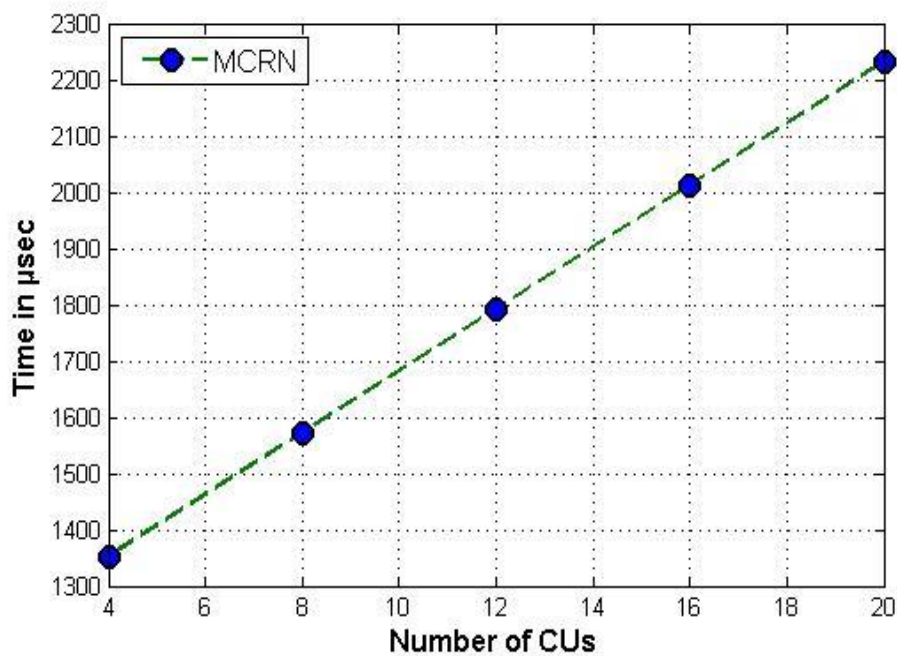


Figure 6-4: Total communication time of 20 pair of CUs in MCRN

### 6.1.5. Throughput analysis of the MCRN

The parameters of the throughput analysis, as discussed in section 5.3.3 for the DSMCRN and SSMCRN protocols, remained the same when analysing the throughput factors in MCRN protocol.

Therefore, Figure 6-5 demonstrates the throughput factor in MCRN for five runs including 4, 8, 12, 16 and 20 CUs without LU activities. It is obvious that the message of a successful delivery increases in each run due to the increase in the number of the CUs who participated in the communication and exchange of 1500

bytes of data. Although each pair of CUs requires a time equal to  $109.91\mu\text{secs}$  over the CCC, the increase of the throughput rate remains significant in each run where the CUs increase. This is due to the availability of the determined data channels that aim to perform the successful switch by the participating CUs and results in each SLDCH being occupied by a single pair of CUs for data transmission. This clearly indicates the main advantages of the CR technology in terms of improving the use of channels since 10 data channels are available and utilised by those CUs.

However, the throughput rate can also be affected by the LUs activities. For example, in the second run where 2 pairs of CUs exchanged their data (see Figure 6-6), the throughput rate decreased to  $1 \times 10^9$  compared with the same run in Figure 6-5. This decrease resulted from the occupation of a single data channel by an LU who has priority in the use of the licensed data channels. Apart of this, the throughput rate remained the same as in other runs where the data channels are available due to the status of the LUs being OFF.

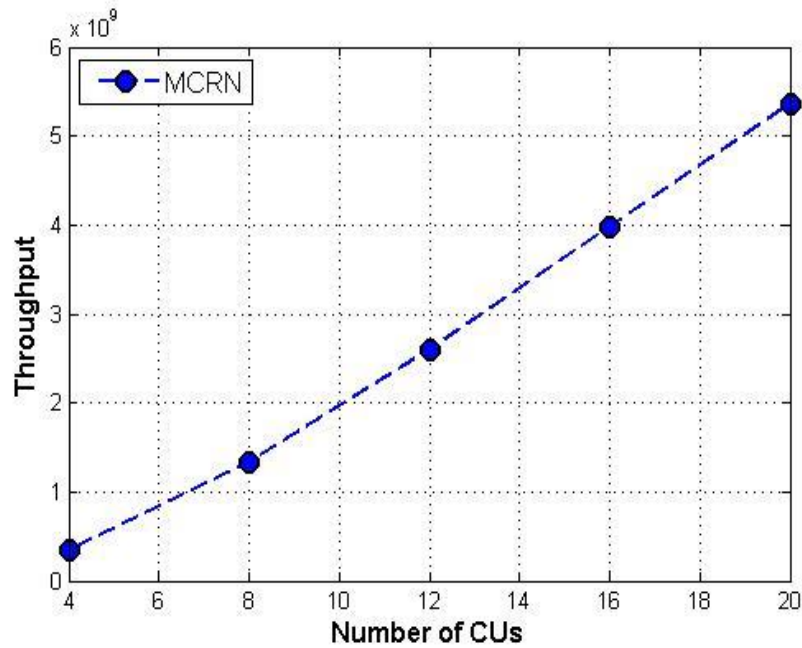


Figure 6-5: Throughput for 20 pair of CUs in MCRN without LUs activities

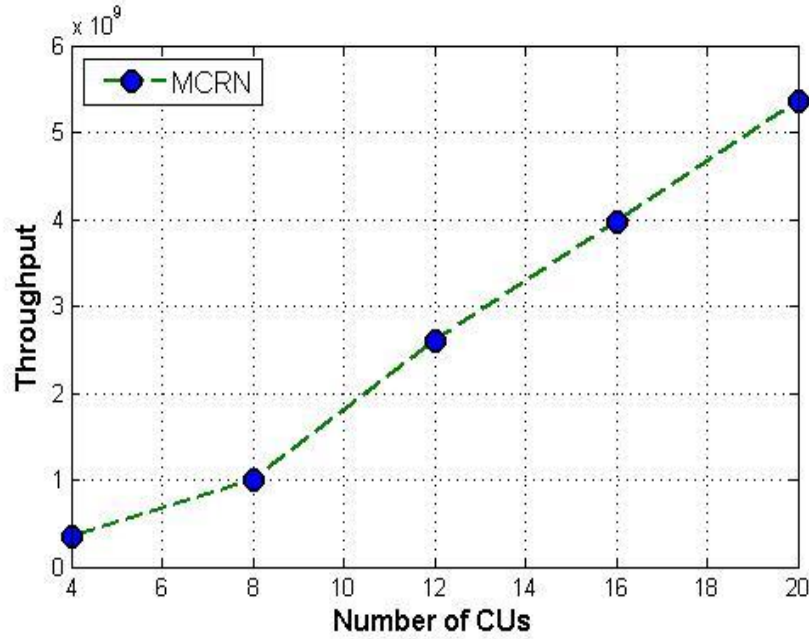


Figure 6-6: Throughput for 20 pair of CUs in MCRN with LUs activities

## 6.2. Benchmarks CREAM and RACRN protocols

Both Cognitive Radio-Enabled Multi-channel MAC (CREAM-MAC) (Zhang & Su, 2011) and Cognitive-radio-based carrier sense medium access with collision avoidance (CR-CSMA/CA) (Qian, et al., 2013) for CRNs are two different benchmarks protocols. These protocols were discussed in Chapter 2, section 2.1.1.2. Thus, they are selected among the available MAC protocols, since they are well known for decentralised CRNs, and are the closest to the proposed MCRN in the two networks features. These features include the use of a dedicated control channel to exchange control information among participating CUs in the communication, and multiple Licensed Data Channels (LDCHs), which are involved for data transmission. However, due to the long names of these protocols, they are renamed and abbreviated only in this thesis, to CREAM and RACRN instead of CREAM-MAC and CR-CSMA/CA respectively. Thus, from this point, these two abbreviations will be used and appear all the time when they are used.

### 6.3. Handshaking frames over the control channel and data channels in MCRN, CREAM and RACRN

Table 6-2 below demonstrates the number of control and data phases' frames, and their sizes in MCRN and the benchmarks protocols. Despite all the protocols considering two different frames, known as data and ACK in the data phase, the number of control frames does not remain the same, since only 2 frames are used in MCRN, while 4 and 3 frames are exchanged in CREAM and RACRN respectively. This is considered as a clear contribution point of this research, since MCRN performs the negotiation with less hand shaking frames, leading to a reduction of the communication time over the control channel and resulting in accomplishing fast switching to the SLDCH. Moreover, both CREAM and MCRN protocols use 20 bytes of common control and data frames; whereas, RACRN uses different sizes and equals 14 bytes in PTS and CTS, while the RTS size remains the same, and equal to 20 bytes.

It is not possible to deny that, the smaller sizes of frame exchange lead to reservations in the channels for a shorter time; however, the extra handshaking frames increase the time over the control channel, since both the size of the transmitted control frames and SIFS are two contributory factors leading to reserving the channel for extra time. This case is applied to both the benchmark protocols, since MCRN reduces the number of the handshaking frames over the CCC.

Table 6-2: Control and data frames in MCRN, CREAM and RACRN

Protocols	Control frames	Control frames' sizes in byte	Data frames	Data and ACK frames' sizes in byte
MCRN	2	RTS= 20 and CTS= 20	2	Data= 1520 and ACK= 20
CREAM	4	RTS= 20, CTS= 20, CST= 20 and CSR= 20	2	Data= 1520 and ACK= 20
RACRN	3	PTS= 14, RTS= 20 and CTS= 14	2	Data= 1514 and ACK= 14

## **6.4. Comparative analysis of the proposed and benchmarks protocols without security**

Both the communication time and successful messages delivery are the two network performance factors aiming for a comparison's analysis of both MCRN against the benchmark protocols, CREAM and RACRN, when not incorporating security.

### **6.4.1. Time performance analysis of MCRN, CREAM and RACRN**

Although, the proposed MCRN protocol has been discussed and analysed in section 3.2, it is also introduced in this section as a constituent of the comparisons against the benchmark protocols. These protocols do not incorporate security features and their analysis is required to compare their performance in terms of communication time and throughput rate. Moreover, the LUs activities are taken into the consideration to analyse their potential impacts on channel availability and network performance in general. Therefore, both the time taken for the communication process, and the message delivery rate with and without LUs activities in the network in the proposed and benchmark protocols are discussed next.

Figure 6-7 illustrates the time spent on the communication process in microseconds for five runs, including 4, 8, 12, 16 and 20 CUs in the proposed and benchmark protocols, without considering the security features. This time refers to both the period consumed over the control channel to exchange the control frames, and the period over the SLDCH to transmit 1500 bytes of data. Both the number and sizes of the handshaking control frames considerably affects the communication time for the frames' exchanges between senders and receivers. Consequently, it is clear that CREAM requires more time to exchange messages successfully than RACRN and the proposed MCRN protocols in each run. This is because there are 4 handshaking frames belonging to each pair of CUs, which are

transmitted over the control channel in CREAM, while 3 and 2 frames for RACRN and MCRN respectively are launched over the same channel.

Moreover, the overall times in the benchmarks and the proposed MCRN protocols increase as soon as the participating number of CUs is increased in each run. This is logical when each sender necessitates contention access the control channel to launch his or her RTS frames for data channel selection. However, a large and notable performance is achieved by MCRN compared to the benchmarks protocol, especially once the number of contributing CUs is increased due to the fewer handshaking frames that have been transmitted over the control channel, which lead to fast switching of the SLDCH for data transmission. Although, the RACRN operates based on 3 handshaking frames over the control channel, it is closer to the proposed MCRN than CREAM protocols in each run, due to the smaller sizes of the control frames transmitted, compared to those in the MCRN.

Thus, in the first run, where 2 pairs of CUs communicate, the total time required to successfully complete the communication process is 1439.27 $\mu$ secs in CREAM, 1361.09 $\mu$ secs in RACRN and 1352.73 $\mu$ secs in MCRN. However, in the second run, where 4 pairs of CUs are communicating, the total time for completing the data transmissions over the different SLDCHs increases by 306.09 $\mu$ secs in CREAM, 239.82 $\mu$ secs in RACRN and 219.82 $\mu$ secs in MCRN. These increases resulted from exchanging the control frames, belonging to the 3<sup>rd</sup> and 4<sup>th</sup> participating pairs of CUs. Therefore, requirements are: 1745.36 $\mu$ secs in CREAM, 1600.91 $\mu$ secs in RACRN and 1572.55 $\mu$ secs in MCRN. This process remains the same for the third, fourth and final runs, where 6, 8 and 10 pairs of CUs contributed to the communication in the same order.

It is notable that, the differences in the time are significantly distinct in cases where a large number of CUs are participating in the network. For instance, in the last run, CREAM necessitates the highest time, equalling 2664.71 $\mu$ secs, to successfully exchange the data among the intended CUs, while the proposed MCRN requires the lowest time and is equal to 2232.01 $\mu$ secs when exchanging the same data. Thus, achieving the lowest time for successfully completed the communication among CUs by MCRN is considered as one of the contribution

point of this research since the communication time is critical for CUs needing to switch to the SLDCH and perform data transmission.

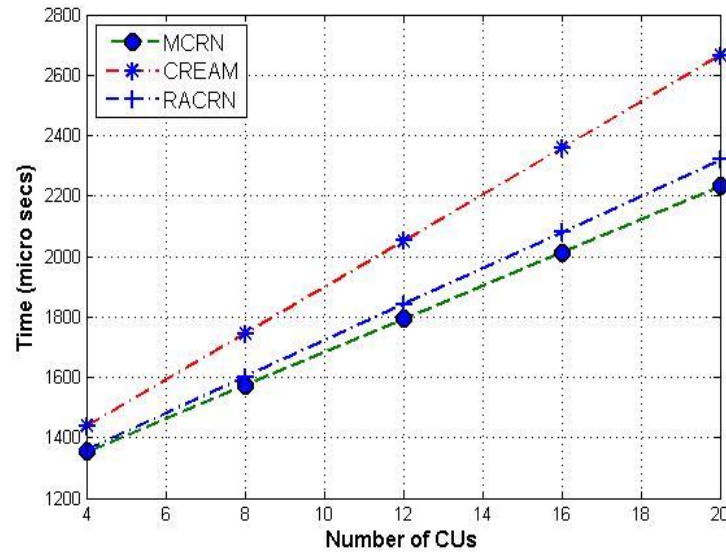


Figure 6-7: Communication time of 20 pair of CUs in MCRN, CREAM and RACRN with and without LUs activities

### 6.4.2. Throughput performance analysis of MCRN, CREAM and RACRN

Figure 6-8 shows the message delivery rate in both the MCRN and benchmark protocols for five runs, including 4, 8, 12, 16 and 20 CUs without LUs activities. The discussion of the throughput increase in the protocols for each run is associated with the number for the contributing CUs; since each sender transmits a message over a different SLDCH. Therefore, it is apparent that the throughput increases dramatically in each run, since the SLDCHs are available to the CUs to initiate the data transmissions. However, although, the throughput rate in the MCRN is higher than the message delivery rate in the benchmarks for each run, the difference is significant between MCRN and CREAM. This is because the higher communication time is required among the contributing CUs to exchange the control frames over the control channel in the CREAM. Moreover, in each run of the MCRN and other benchmarks, the difference in throughput continuously increased, due to the increase in the number of successful data exchange among the participated CUs over the SLDCHs.

## Comparative analysis of the proposed and benchmark protocols

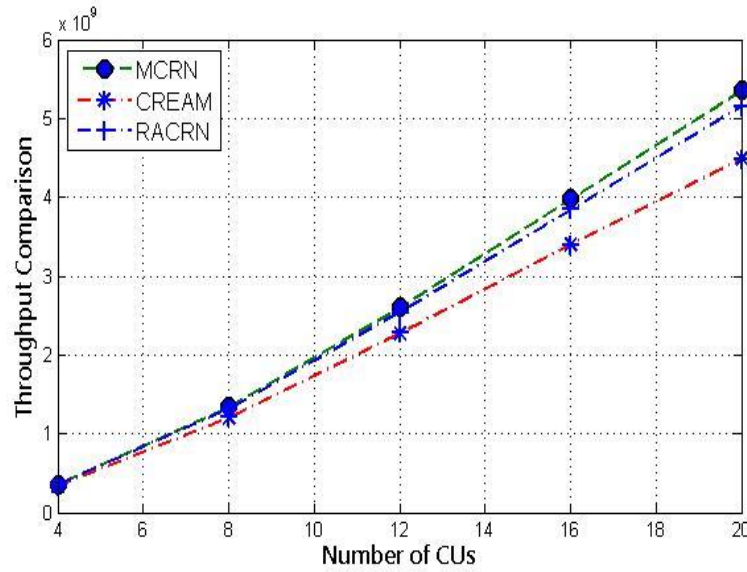


Figure 6-8: Throughput for 20 pair of CUs in MCRN, CREAM and RACRN without LUs activities

However, Figure 6-9 shows the message delivery rate in both the MCRN and benchmark protocols for five runs, including 4, 8, 12, 16 and 20 CUs with LUs activities. The same discussion of the throughput increases, and its comparison in the MCRN and benchmarks protocols for the previous figure is applied here. However, the LUs activities play a major role in utilising the LDCH with higher priority; therefore, it can be observed that the increase in the throughput in the second run is slight compared to that in the others runs, as the LU turned ON in the current run, for utilising a single LDCH, and this led to the channel being vacated by the CUs. As a result, the CUs are unable to transmit data over this busy channel causing a decrease in throughput, compared to the situation in which the channel is available and utilised by the CUs. However, the status of the throughput increases in the remaining runs is dramatic compared to those in the second run, since the LUs remain OFF during the communication process.

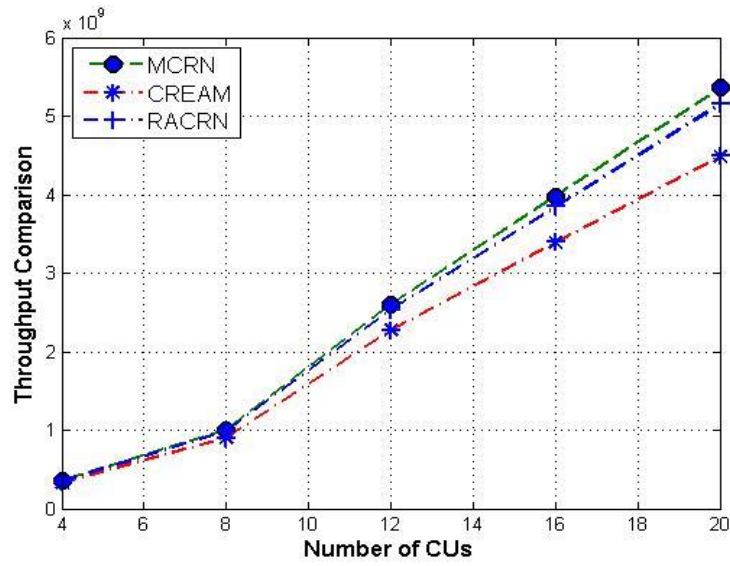


Figure 6-9: Throughput for 20 pair of CUs in MCRN, CREAM and RACRN with LUs activities

A clear contribution point of this research is accomplished in this section by obtaining a higher throughput that is achieved by the MCRN compared to the benchmark protocols. This is due to the less communication time, which is inversely proportional with the throughput, is performed by the MCRN for a pair of CUs over CCC and subsequent switching to the SLDCH and initiate data transmission.

## 6.5. Comparative analysis of the proposed and benchmark protocols with security

This section considers the same analytical approaches to throughput and communication time for the same proposed and benchmark protocols after adding two different security features belonging to the digital signatures and shared key for the authentication procedure. Therefore, these protocols are recognised as DSMCRN and SSMCRN, as discussed before in Chapter 4, and compared against the same benchmark protocols after adding the same security features. Therefore, for the digital signature MAC protocols group, the DSMCRN will be compared with both Digital Signature based Cognitive Radio-Enabled Multi-channel MAC (DSCREAM) and Digital Signature based cognitive Radio medium Access for Cognitive Radio Network (DSRACRN), while for the shared key MAC protocols, the SSMCRN will be compared with both Shared-key based Secure Cognitive

Radio-EnAbleD Multi-channel MAC (SSCREAM) and Shared-key based Secure cognitive Radio medium Access for Cognitive Radio Network (SSRACRN).

### **6.5.1. Time performance analysis of DSMCRN, DSCREAM and DSRACRN**

Figure 6-10 shows the difference in the time taken for a single pair of CUs to communicate with each other in DSMCRN, DSCREAM and DSRACRN protocols. It is evident that the difference is very small due to the security time, which is significantly large, due to both the RSA encryption and decryption, as well as applying the digital signature for authenticating CUs. Thus, there are only 1.27µsecs different between DSMCRN and DSRACRN and 46.12µsecs between DSMCRN and DSCREAM. This is a clear contribution point of this research where the DSMCRN showing less time required for successful secure data exchange among valid CUs compared to the benchmark protocols (DSRACRN and DSCREAM) due to the less handshaking of frames.

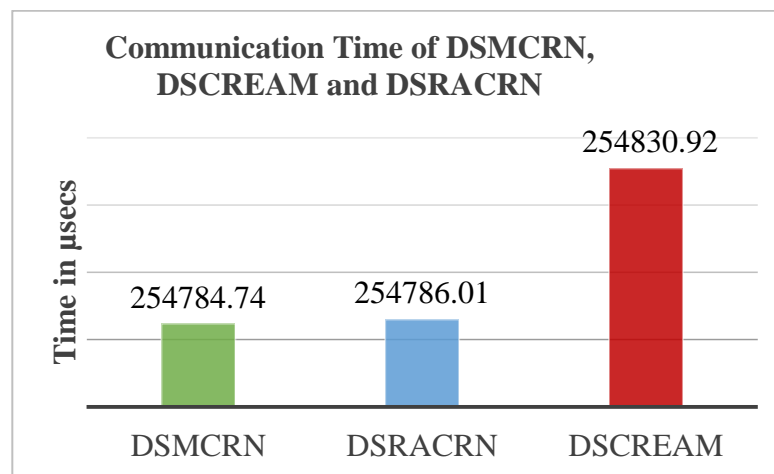


Figure 6-10: Communication time of a single pair of CUs in DSMCRN, DSCREAM and DSRACRN

However, Figure 6-11 demonstrates the communication time required to successfully exchange the control and data frames for five runs, including 4, 8, 12, 16, and 20 CUs in DSMCRN, DSCREAM and DSRACRN. As discussed previously, the time to access and exchange the control frames over the control channel increases, as soon as the number of joined CUs increases, since each

sender necessitates launching of the ITA frame. Thus, the communication time for these control frames doubles in each run, compared to the previous run. However, it is difficult to observe the time differences in the current figure for both the DSMCRN and benchmarks protocols, as they have same lengthy security time, while the communication time is very short, as discussed in the previous figure. This makes these trends very closely aligned, requiring maximisation for each run.

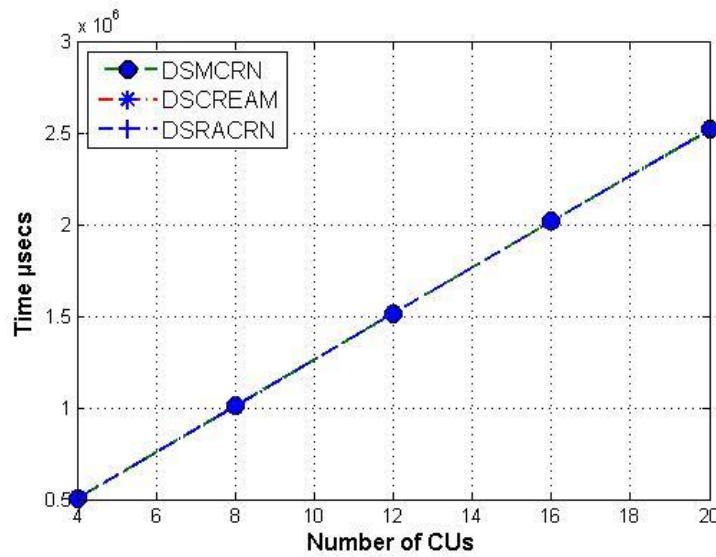


Figure 6-11: Communication time of 20 pair of CUs in DSMCRN, DSCREAM and DSRACRN without LUs activities

### 6.5.2. Throughput performance analysis of DSMCRN, DSCREAM and DSRACRN

Figure 6-12 shows the throughput rate for five runs, including 4, 8, 12, 16, and 20 CUs without LUs activities in DSMCRN, DSCREAM and DSRACRN. Since the SLDCH are available for the CUs' message transmissions, and the LUs are OFF during the communication process, the messages are successfully delivered to the intended destinations. The number of transmitted messages increased in each run, due to the number of participating CUs, and the availability of the LDCHs function; the successful message delivery resulted in an increased throughput rate.

## Comparative analysis of the proposed and benchmark protocols

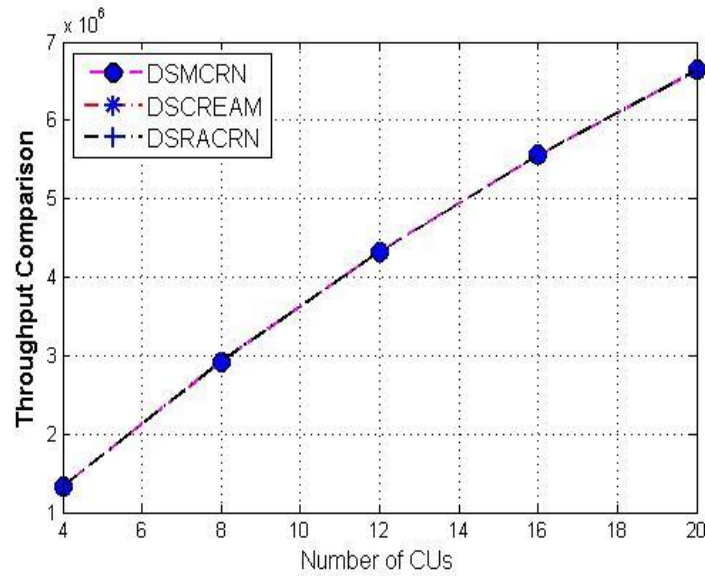


Figure 6-12: Throughput for 20 pair of CUs in DSMCRN, DSCREAM and DSRACRN without LUs activities

However, Figure 6-13 demonstrates the successful message delivery rate for five runs, including 4, 8, 12, 16, and 20 CUs, with LUs activities in DSMCRN, DSCREAM and DSRACRN. A component of what has been discussed in the previous figure without the LUs activities, the throughput rate in the second run of the proposed DSMCRN and the benchmarks is different compared to the scenario without the LUs activities, due to channel occupancy by the LUs. This affects the throughput rate, since the number of the data channels decreases, while the number of contributing CUs remains the same. Thus, there is a slight increase compared to the scenario without LUs in the rate of the message delivery, since the LU, who has the priority to utilise it, occupies a single data channel. However, the throughput rates for other runs remain the same, since the LUs are OFF and this results in making the SLDCHs available to the CUs.

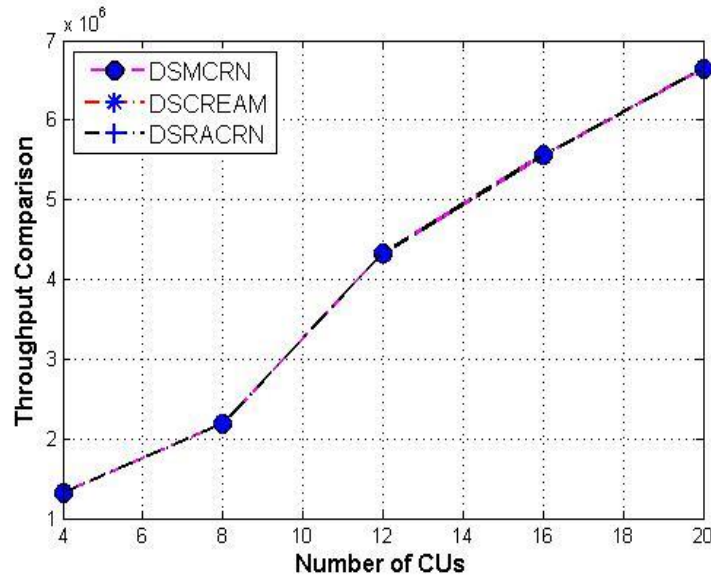


Figure 6-13: Throughput for 20 pair of CUs in DSMCRN, DSCREAM and DSRACRN with LUs activities

### 6.5.3. Time performance analysis of SSMCRN, SSCREAM and SSRACRN

Figure 6-14 demonstrates the communication and security time frame for a single pair of CUs in the SSMCRN, SSCREAM and SSRACRN protocols. It is clear that the proposed SSMCRN protocol perform better and faster than the benchmark protocols, since 1.27 $\mu$ secs and 46.18 $\mu$ secs are the additional times taken in SSRACRN and SSCREAM respectively, compared to the communication time in SSMCRN. Therefore, this is considered as another contribution point of this research since the secure communication time in SSMCRN is less compared to that in the benchmark protocols (SSRACRN and SSCREAM).

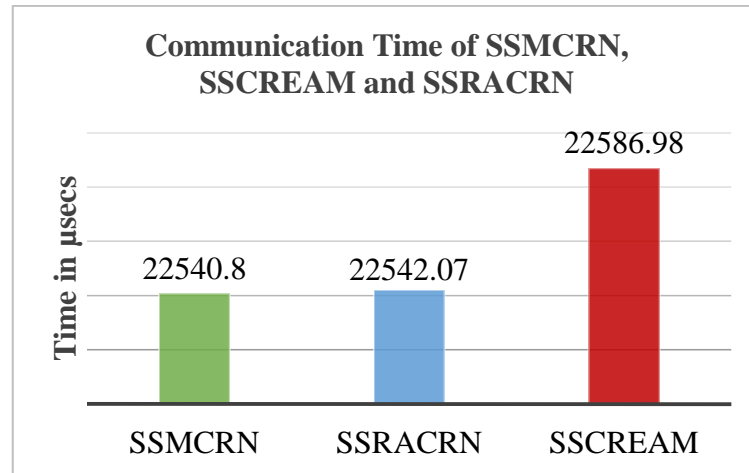


Figure 6-14: Communication time of a single pair of CUs in SSMCRN, SSCREAM and SSRACRN without LUs activities

Figure 6-15 demonstrates the communication time required to successfully exchange the control and data frames for five runs, including 4, 8, 12, 16, and 20 CUs in SSMCRN, SSCREAM and SSRACRN. It can be seen that the throughput rate in SSMCRN and the benchmarks increases dramatically in each run, because of the increase in the number of CUs participating in the communication process. Therefore, the status of the time increase is constant in each run, due to the availability of the SLDCHs for those CUs; and there are no activities belonging to the LUs over these SLDCHs. However, the communication times for these protocols are close, since the same applied security features are considered, and the difference is apparent in the communication time, relative to the associated frames in the benchmark protocols, as shown in the previous figure. This makes these trends very closely aligned, requiring maximisation for each run.

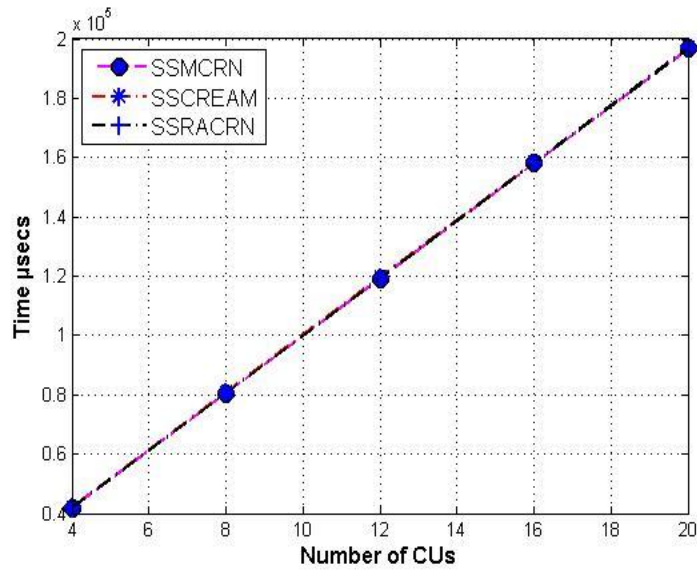


Figure 6-15: Communication time of 20 pairs of CUs in SSMCRN, SSCREAM and SSRACRN without LUs activities

#### 6.5.4. Throughput performance analysis of SSMCRN, SSCREAM and SSRACRN

Figure 6-16 demonstrates the successful message delivery rate for five runs, including 4, 8, 12, 16, and 20 CUs without LUs activities in SSMCRN, SSCREAM and SSRACRN. Generally, the throughput rate increases in each run because of the number of messages transmitted by the participating CUs. However, the security time affects throughput rate, and it can be seen that the difference in the message delivery rate for the proposed protocol and the benchmarks is not significant. This is because the large time relates to the same applied security features in each protocol compared to the time for the same protocols in the scenario not involving security features (see Figure 6-8). The throughput increase for each protocol remains continuous in each run, because the SLDCHs by CUs are available and not utilised by the LUs, which are OFF during message transmissions; this leads to increased throughput of data communications.

## Comparative analysis of the proposed and benchmark protocols

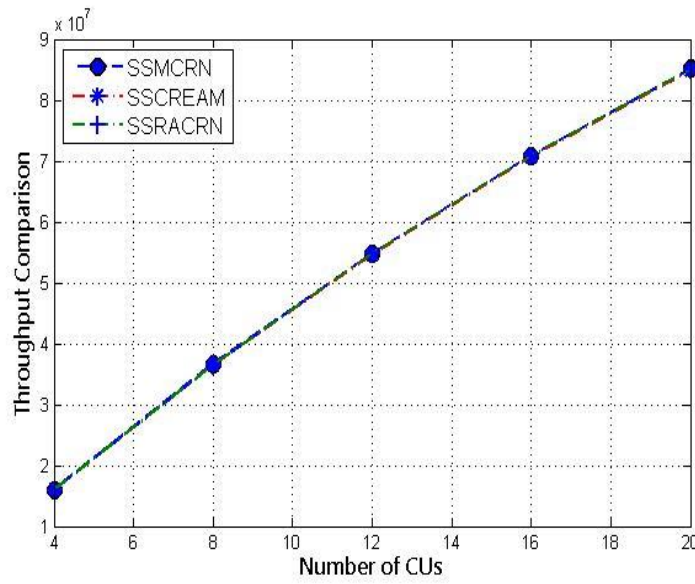


Figure 6-16: Throughput for 20 pair of CUs in SSMCRN, SSCREAM and SSRACRN without LUs activities

Figure 6-17 demonstrates the throughput rate for five runs, including 4, 8, 12, 16, and 20 CUs with LUs activities in SSMCRN, SSCREAM and SSRACRN. Although, the message delivery rate for the proposed and benchmark protocols increased in each run, due to the increase in the senders, the LUs activities had a considerable impact on throughput rates. This influence resulted from LUs occupying a licensed data channel, making it unavailable for CUs willing to transmit data. An obvious example is shown in the second run, where 8 CUs participate in the communication process in the figure. Therefore, the throughput pattern is different compared to the scenario in which the LUs are OFF during the communication (see Figure 6-16). Thus, there is a slight increase in the throughput rate in the second run of the SSMCRN and benchmark protocols; however, the throughput increases dramatically to the point that it should be in the third run due to the increase in both the number of transmitted message and the channels available for the contributing CUs. Therefore, the increase in the status of the throughput remains the same in the 4<sup>th</sup> and final run compared to the scenario where the LUs are OFF.

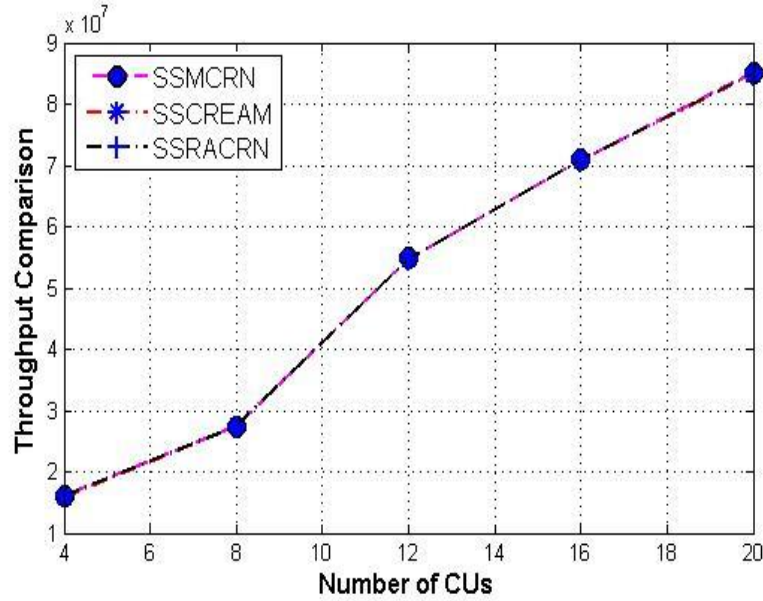


Figure 6-17: Throughput for 20 pair of CUs in SSMCRN, SSCREAM and SSRACRN with LUs activities

Therefore, based on the comparison results of the proposed and benchmarks protocols with and without security and with and without the LUs appearance scenarios, it is clear that the number of the transmitted control frames significantly affects the communication time over the CCC in general. This effect plays a major role on the switching time to the SLDCH for each pair of CUs. Thus, there is no doubt about the fact that throughput results are different from protocol to another since the communication time differs on each protocol with and without incorporating the security features. As the correlation between the throughput and communication time is significantly inversely linked to each other in which the increase in the communication time leads to the decrease of the throughput and vice versa as explained in section 5.3.3.

## 6.6. Summary

The current chapter mainly presented the simulation of a novel MAC protocol for decentralised CRNs (MCRN). The protocol promotes efficient use of unused licensed channels and enables Cognitive Users (CUs) to transmit their data successfully over licensed channels without any hindrance to Licensed Users (LUs). The status of the LUs over the licensed channels is determined before data transmission takes place. The protocol uses a dedicated Common Control Channel

(CCC) for only control information exchange among CUs and multiple Licensed Data Channels (LDCHs) are involved in the data transmission.

In addition, the chapter introduced two different phases of the comparative analysis, focusing on the communication time and throughput rate. The first involved a comparison of network performance for the proposed MCRN, and the benchmarks CREAM and RACRN protocols. It also included two different scenarios, i.e. with the LUs ON or OFF, to investigate the LUs impacts on the performance of the entire network. Thus, the proposed MCRN achieved better performance compared to the others, since it was based on fewer handshaking frames, which aimed to perform faster when switching to SLDCH to initiate the data transmission.

However, the second phase incorporates two different versions of the applied security features; a digital signature, and a shared key, for authentication procedures in the proposed and benchmark protocols. Therefore, although the differences in network performance are considerably obvious in the comparison task for the proposed and benchmarks protocols without incorporating security, this is not significant, since the security features are applied in them. The reason for this relates to the length of time for the applied security frames and the execution time for the security algorithms. Thus, it results in a small difference in obtained communication times and the throughput rate results for the proposed and benchmarks protocols, based on the digital signature and the shared key security versions.

Therefore, the highlighted contributions of this research that has been addressed in this chapter can be summarised as the follows:

- 1- Reserving the CCC for less communication time to make it available for the next pair of CUs in the MCRN, DSMCRN and SSMCRN as compared to the other benchmark protocols with and without security. This is achieved as the proposed protocols have less handshaking frames compared to the benchmark protocols.
- 2- Higher successful message delivery rate is accomplished by the MCRN, DSMCRN and SSMCRN as compared to those in the benchmarks protocols with and without security. This is obtained when the lower

## **Comparative** analysis of the proposed and benchmark protocols

latency of the complete control information exchange between a pair of CUs and subsequently led to less time being needed to switch to the SLDCH for initiating data transmission.

The next chapter will conclude the thesis. It includes three main parts: a summary of the research, a summary of the research contributions achieved, and future work.

# Chapter 7 CONCLUSIONS

This chapter concludes this thesis by first explaining what has been achieved by this research thus far, to meet the primary aim of deploying secure MAC protocols for the CRNs, then summarising the research contributions, and followed by proposing related future work.

## 7.1. Summary of the current research

Since CRNs have their own characteristics and functions to enable unlicensed users to communicate over a licensed band, it is crucial that LUs meet the condition of non-interference. This approach is considered highly advantageous for several reasons, such as;

- 1- The ability to improve the spectrum utilisations,
- 3- Increase wireless devices to establish communication,
- 4- Overcome issues with limited and under-utilised spectrums.

Thus, CR technology has become a successful research topic, aiming to address communication within the CRNs environment. Since spectrum sharing is considered one of the main functions CRNs must provide, the communication process among CUs is based on three classifications, which are variously recognised as Network architecture, Access technology and Allocation behaviour. These determine the methodology for successful communication and message transmission between the intended users.

Therefore, an effective improvement of the successful communication between CUs in decentralised CRNs was achieved by the proposed MAC protocol for Cognitive Radio Networks (MCRN). Since the related existing approaches in the literature require additional frames to be exchanged between the senders and receivers, the proposed protocols offered efficient functionality for the objective of gaining better communication among CUs through reducing the number of handshaking frames over the CCC. This has led to performing fast switching from the CCC to the selected data channel and offering the CCC availability to the next pair of CUs. Thus, the proposed MCRN protocol was designed (in sections 3.2), then simulated, successfully tested, and evaluated by performing comparison

## Conclusions

against two different related approaches (in section 6.4), in terms of time performance and throughput.

However, security is fundamental to maintaining a successful communication process among intended recipients, since an entire network performance can easily deteriorate as a consequence of malicious behaviours and attacks, such as the modification and forgery of transmitted messages, unauthorised access, DoS, masquerading, replay, and non-repudiation. Therefore, this research has successfully addressed the aim and objectives stated in section 1.7 for providing required security in CRNs to ensure the maintenance of effective secure communication among legitimate CUs, and providing protection and detection mechanisms against threats targeting spectrum sharing and spectrum management that lead to DoS attacks. This is accomplished by investigating the existing secure MAC protocols in CRNs and identifying different types of attacks that are possible in CRNs (see sections 2.2 and 2.3). This has led to the proposal and design of two different versions of hybrid secure MAC protocols based on digital signature and shared key (see section 3.3) to investigate and analyse the authentication mechanisms and how these different security algorithms can affect the network performance and throughput. Although, each attack employs a unique method and technique when launched, when combined, a variety of security features can provide effective defence against each malicious approach. Specifically, cryptographic algorithms provide great functionality to protect CRNs from the potential behaviours mentioned. Message Authentication Code, Symmetric and Asymmetric Keys, and digital signature algorithms are incorporated within the proposed MCRN protocol. In addition, the security analysis of the proposed protocol using the BAN formal logic is performed as an initial stage (3.3.6) to validate the protocols in terms of meeting the secure communication and the security requirements. A simulation was performed as discussed in Chapters 4 and 5 to analyse the performance of the proposed hybrid secure MAC protocols. The performance evaluation of the proposed hybrid secure MAC protocols against other secure protocols was completed in section 6.5. As a result, the proposed security protocols achieved better performance in perspective

## Conclusions

of fast communication time and higher throughput compared to the two other benchmark protocols.

The following section summarises the main contributions and points leading to achieving the aim of this research.

## 7.2. Contributions Revisited

The primary contributions of this thesis are based upon three proposed CRNs' MAC protocols that were classified into two categories: *Networking* and *Security* protocols and discussed as follows:

### 7.2.1. The proposed MCRN network protocol

The following points are the summary of the achieved contributions by the proposed MCRN protocol:

- **Reducing the number of handshaking frames over the CCC effectively improved the network efficiency.** The comparison results showed that the proposed MCRN achieved better performance related to less communication time and higher throughput compared to the benchmarks, since it aimed to reserve the CCC for a shorter time, due to exchanging fewer handshaking frames. The enhanced communication time among CUs led to speeding up the switch to SLDCH for initiating data transmissions, which in turn led to achieve higher throughput compared to the existing related protocols (as discussed in section 6.4.2).
- **The proposed protocol offers the network availability to a large number of CUs compared to the existing related approaches.** Therefore, each pair of CUs requires less communication time over the control channel. This led to performing speeding up the switch to SLDCH and resulting in vacating the current channel to the other CUs within the network.

### 7.2.2. Security protocols

A robust protection and detection security mechanisms are offered by both DSMCRN and SSMCRN proposed protocols for controlling the network and

## Conclusions

guarding its resources. The proposed security protocols overcome the limitations in the existing techniques in literature by improving the network performance and delivering a complete and efficient security approach that was experimentally validated and tested for ensuring successful secure communication. The proposed protocols incorporate appropriate security algorithms that remarkably ensure the objectives of maintaining the network operation and accomplish the CUs demand of performing successful secure communication with aim of improved network performance. These are achieved by utilising effective mitigation and defence procedures against the potential threats that commonly target the network communication and resources.

Thus, the following points are the contributions that are obtained by the proposed DSMCRN and SSMCRN protocols:

- **Protecting the channel sensing results and selected licensed data channels:** The proposed DSMCRN and SSMCRN protocols ensure the spectrum management performs the right decision and successfully defend against Spectrum Sensing Data Falsification attacks, which in turn cause a DoS. This is successfully accomplished by confirming the authenticity and integrity of the transmitted both sensing results and SLDCHs. Without insuring the control information authenticity and integrity, the network operation can be easily compromised by malicious users due its significant vulnerability to manipulation and malicious activities.
- **Reducing the possible interference over the selected data channels:** The proposed security protocols reduce the possible interference (jamming attacks) that can occur by malicious users over the selected licensed data channel. Thus, the proposed protocols consider the encryption procedure of the transmitted available channels between senders and receivers for the objective of making the exchanged channels unrecognised and hidden to the adversary users, who aim to disturb the communication.
- **Ensuring both authentication and authorisation procedures:** The propose security protocols limit the network access to only authorised CUs and address the mutual authentication factor by considering two different

## Conclusions

approaches related to digital signature and shared key. Hence, CUs are validated at the initial stage before performing spectrum sensing and spectrum sharing for determining and exchanging available channels. This safeguards the credibility of the network resources from any potential security threats that can lead to increasing the chance of DoS attacks.

- **Improving the network efficiency and connectivity:** The proposed security protocols grant a better and effective approach for secure communication between CUs. They successfully adopt a symmetric key approach and avoid the use of asymmetric key method, which is considered in the existing related techniques in literature, for secure communication between senders and receivers. This adoption is essential since the security execution time of the symmetric key approach is faster than asymmetric key algorithm. Consequently, the overall secure communication time over both the control and data channels is significantly reduced and led to both improving the network performance and the licensed channels availability.
- **Reducing the number of handshaking frames:** From the network performance side, the proposed security protocols have led to ensure the successful communication among CUs with improved network performance related to the communication time and throughput compared to the existing approaches in literature. The proposed protocols reduced the number of handshaking frames that efficiently decreased the communication time and improved throughput. This is significantly constructive and important in situations where a large number of CUs exist to utilise the CCC. Therefore, the proposed security protocols contributed in decreasing the probability of the CCC saturation. Hence, CUs are successfully offered with security and higher throughput by the DSMCRN and SSMCRN compared to the benchmarks protocols.
- **Protecting the network availability:** The SSMCRN performed fast detection process of the invalid transmitted messages over the control channel. This detection indicates the robust security features associated

## Conclusions

with the proposed protocol for the aim of decreasing the network and server's overhead.

### 7.3. Future work

Several aspects can be addressed in future to enhance this work, specifically to improve the communication among the CUs and to provide defence against attacks not considered in this research. These are as follows:

#### 7.3.1. Incorporating a backup data channel to improve network performance

Since the current research mainly focused on the security of spectrum sharing in CRNs and enabling secure communication among authorised CUs, the use of a backup data channel remains an effective approach to improving the communication process for exchange data. During the data transmission phase, both the sender and the receiver can switch to the backup data channel to resume the data exchange process, only if the LU is ON (LU's activities were detected), to utilise the licensed data channel. This will be beneficial to the network itself and for security reasons.

For example, on the network side, in the current work, if the LU's activities are detected over the SLDCHs then both senders and receivers are required to vacate the data channel (SLDCH) and restart the entire process to determine a different SLDCH for data exchange. This leads to an increase in the communication time between a pair of CUs over the CCC, resulting in decreasing the network throughput and increasing performance time. Moreover, restarting the communication process will affect the CCC's availability and lead to channel saturation, due to the increase of the contention for accessing the CCC by a number of CUs.

However, from a security perspective, the use of a backup data channel might increase the chance of data exchange between a pair of CUs if an attacker has attempted to misbehave by intercepting a communication or by busying the SLDCH. In this case, CUs can switch to the determined backup data channel to resume communications. For instance, if the sender has transmitted data and is

## Conclusions

waiting to receive the ACK frame, which is necessary to indicate successful message delivery, and an attacker has failed to deliver the ACK frame, then the sender can switch to the backup channel for frames exchange.

Conversely, the deployment of the backup data channel is a challenging task, since several factors need to be investigated. For example, the number of equipped transceivers and backup channel announcements required to keep the channel available to a particular pair of CUs. In cases of associated multiple transceivers, an additional transceiver approach is important here if the backup data channel is to observe any switching or receive information. Despite the fact that the additional transceiver leads to greater energy consumption it will increase the chance of successful data exchange between a pair of CUs. However, backup channel announcement is an issue that will arise since the encryption mechanism assists in hiding both the SLDCH and backup data channel from adversarial users who can manipulate or busy these channels. Therefore, it is recommended to encrypt the backup data channel and associate it with the SLDCH within the CTS frame in DSMCRN and SSMCRN so only a pair of CUs knows the backup exchange channel.

### 7.3.2. Detection of selfish activities

Another area requiring future work is the detection of selfish activities that adversely affect overall network performance by sending a fake channel list (FCL) to disturb the communication process and maximise throughput. However, work to date (Huayi & Baohua, 2011) and (Zou & Yoo, 2015) involves puzzle banishment and cooperative attack detection scheme (CADC) technique respectively to detect selfish users as discussed and detailed in section 2.3.2.1, which can be applied to MCRN, DSMCRN and SSMCRN protocols to detect CUs attempting to misbehave to maximise throughput.

### 7.3.3. Detection of Licensed/Primary User Emulation (PUE) Attacks

Since the PUE attack is out of the scope of this thesis as it belongs to the physical layer, it is significant to decrease the network's efficiency by resembling the LU

## Conclusions

signal, in order to mislead and deceive CUs. Therefore, the fake signals transmitted by attackers on the SLDCH lead to the launch of DoS attacks, which require the CUs to vacate the SLDCHs.

Therefore, the use of the public and private key encryption scheme can significantly assist to detect fake signals in DSMCRN and SSMCRN and deliver a certain advantage to the CUs, enabling legitimate users to differentiate between LUs' and CUs' signals during data transmission. Therefore, any malicious user aiming to deceive the CUs by launching a PUE attack over a licensed data channel will be detected. This can be done if a pair of public and private key is used by both LUs and CUs in which any transmitted signal by LUs should include a specific part that is used by only CUs and needs to be encrypted using the public key.

Therefore, before vacating the SLDCH both CUs who using the SLDCH perform the decryption procedure of the received signals and if they are able to decrypt then this indicates the appearance of the LU over the SLDCH. Consequently, both CUs require vacating the current data channel. However, if the encrypted signals cannot be decrypted due to the applied wrong public key then both CUs can confirm that the launched signals over the SLDCH is fake and generated by a malicious user. Thus, this process of the detection is substantially beneficial since it does not require any additional hardware or any changes in the network or system structure.

### 7.3.4. Threshold cryptography against DoS Attack

A DoS attack can easily be launched against a dedicated server, although this is outside the scope of this research since the issue has been arisen and existing in the traditional wireless network and not specific to the CRN, it is therefore considered as a future work. Since the dedicated server is involved as one of the network components and acted as trusted entity for only performing the authentication and providing security keys, it is prone to DoS attacks, which is not specific to only CRN environments. Therefore, protecting the dedicated server in DSMCRN and SSMCRN protocols from a DoS attack is strongly needed to maintain successful communication among CUs. One solution is through a

## **Conclusions**

technique called threshold cryptography (Tarmizi, et al., 2009) in which the secret information is divided into parts and distributed to a number of cooperating servers that shared a private key for performing the required sensitive functionalities, such as decryption and validation (Ertaul & Chavan, 2005). Therefore, the required process works with multiple servers instead of only a single one for providing defence against DoS.

## Chapter 8 REFERENCES

- Abusalah, L., Khokhar, A. & Guizani, M., 2008. A Survey of Secure Mobile Ad Hoc Routing Protocols. *IEEE communication survey & tutorials*, 10(4), pp. 78-93.
- Ahmad, A. T., Farhan, A. A., Sumit, K. & Muhammad, U. S., 2011. *Building Software-Defined Radios in MATLAB Simulink– A Step Towards Cognitive Radios.*, 2011 UKSim 13th International Conference on Modelling and Simulation, pp.492-497.
- Akkarajitsakul, K., Hossain, E., Niyato, D. & Kim, D. I., 2011. Game Theoretic Approaches for Multiple Access in Wireless Networks: A Survey. *Communications Surveys & Tutorials, IEEE*, 13(3), pp. 372,395.
- Akyildiz, I. F., Lee, W.-Y. & Chowdhury, K. R., 2009. CRAHNs: Cognitive radio ad hoc networks. *Ad Hoc Networks* 7, 7(5), pp. pp. 810-836.
- Akyildiz, I. F., Lee, W.-Y., Vuran, M. C. & Mohanty, S., 2008. A survey on spectrum management in cognitive radio networks. *Communications Magazine, IEEE*, 46(4), pp. 40-48.
- Alhakami, W. H., Ali, M. & Sijing, Z., 2012. *ESMCRN: An Enhanced Security Mechanism for Cognitive Radio Networks.*, Proceedings of the 7th IB2COM, PP., 61-65, November 5-8, 2012, Sydney, Australia.
- Alhakami, W., Mansour, A. & Safdar, G. A., 2014. Shared-key Based Secure MAC Protocol for CRNs., in *Next Generation Mobile Apps, Services and Technologies (NGMAST)*, 2014 Eighth International Conference on ., pp.266-271, 10-12 Sept. 2014.
- Alhakami, W., Mansour, A., Safdar, G. A. & Albermany, S., 2013. A secure MAC protocol for Cognitive Radio Networks (SMCRN)., in *Science and Information Conference (SAI)*, 2013., pp.796-803, 7-9 Oct. 2013.
- Anand, S., Jin, Z. & Subbalakshmi, K. P., 2008. An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks, in *New Frontiers in Dynamic Spectrum Access Networks*, 2008. *DySPAN 2008. 3rd IEEE Symposium on.*, pp.1-6, 14-17 Oct. 2008.
- Arkoulis, S., Kazatzopoulos, L., Delakouridis, C. & Marias, G., 2008. Cognitive spectrum and its security issues, in *Next Generation Mobile Applications, Services and Technologies*, 2008. *NGMAST '08. The Second International Conference on.*, pp.565-570, 16-19 Sept. 2008.
- Attar, A., Tang, H., Vasilakos, V; Yu, F. R; Leung, V, C. M., 2012. A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions. *Proceedings of the IEEE*, 100(12), pp. 3172-3186.
- Baayer, A., Enneya, N. & Elkoutbi, M., 2012. Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs. *Journal of Information Security*, 3(3), pp. 224-230.
- Baldini, G., Sturman, T., Biswas, A. R., Leschhorn, R., Godor, G., Street, M., 2012. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. in *IEEE Communications Surveys & Tutorials*, 14(2), pp. PP. 355- 379.
- Ball, S., Ferguson, A., 2005. "Consumer applications of cognitive radio defined networks," in *New Frontiers in Dynamic Spectrum Access Networks*, 2005. *DySPAN 2005. First IEEE International Symposium on*, pp.518-525, 8-11.

## References

- Bhattacharjee, S., Konar, A. & Bhattacharjee, S., 2011. Throughput Maximization Problem in a Cognitive Radio Network. *International Journal of Machine Learning and Computing*, 1(4), pp. 332 - 336.
- Bian, K. & Park, J.-M., 2006. MAC-layer misbehaviors in multi-hop cognitive radio networks., *US - Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)*, Aug. 2006., PP, 1- 8.
- Burrows, M., Abadi, M. & Needham, R., 1990. A logic of authentication. *ACM transactions on computer systems*, 8(1), pp. 18-36.
- Capkun, S., Cagalj, M., Rengaswamy, R., Tsigkogiannis, I., Hubaux, J., Srivastava, M., 2008. Integrity Codes: Message Integrity Protection and Authentication over Insecure Channels. *Dependable and Secure Computing IEEE Transactions on*, 5(4), pp. 208-223.
- Carlos, C. & Kiran, C., 2007. *C-MAC: A Cognitive MAC Protocol for Multi-Channel Wireless Networks*, in *New Frontiers in Dynamic Spectrum Access Networks*, 2007. DySPAN 2007. 2nd IEEE International Symposium on, pp.147-157, 17-20 April 2007.
- Chaczko, Z., Wickramasooriya, R., Klempous, R. & Nikodem, J., 2010. *Security threats in cognitive radio applications*, in *Intelligent Engineering Systems (INES)*, 2010 14th International Conference on., pp.209-214, 5-7 May 2010.
- Chen, R., Park, J.-M., Hou, Y. T. & Reed, J. H., 2008. Toward secure distributed spectrum sensing in cognitive radio networks. *Communications Magazine, IEEE*, 46(4), pp. pp. 50-55.
- Chen, R., Park, J.-M. & Reed, J. H., 2008. Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *Selected Areas in Communications, IEEE Journal on*, Jan, 26(1), pp. 25,37.
- Chen, R.-R., Teo, K. H. & Farhang-Boroujeny, B., 2011. Random access protocols for collaborative spectrum sensing in multi-band cognitive radio networks. *IEEE Journal Of Selected Topics In Signal Processing*, 5(1), pp. 124–136.
- Chen, Z., Guo, N. & Qiu, R. C., 2010. Demonstration of real-time spectrum sensing for cognitive radio. *IEEE Communications Letters*, 2010 milcom, 14(10), pp. 323-328..
- Chong, J. W., Sung, Y. & Sung, D. K., 2009. Multi-Band CSMA/CA-Based Cognitive Radio Networks, *IWCMC '09 Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*., PP, 298-303.
- Chong, J. W., Sung, Y. & Sung, D. K., 2009. RawPEACH: Multiband CSMA/CA-Based Cognitive Radio Networks. *Journal of communication and networks*, 11(2), pp. 175-186.
- Chauhan, K. K. & Sanger, A. K. S., 2014. Survey of Security threats and attacks in cognitive radio networks, *Electronics and Communication Systems (ICECS)*, 2014 International Conference on, Coimbatore, 2014, pp. 1-5.
- Ci, S. & Sonnenberg, J., 2007. A cognitive cross-layer architecture for next-generation tactical networks, in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pp.1-6, 29-31 Oct. 2007.
- Cordeiro, C., Challapali, K., Birru, D. & N, S. S., 2005. IEEE 802.22: The first worldwide wireless standard based on cognitive radios, in *New Frontiers in*

## References

- Dynamic Spectrum Access Networks. DySPAN 2005. First IEEE International Symposium on* ., pp.328-337.
- Dappuri, B. & Venkatesh, T. G., 2014. IEEE 802.11 DCF MAC Protocol for Cognitive Radio Networks: Cooperative Basic Access Vs RTS/CTS., *2014 International Symposium on Communications and Information Technologies (ISCIT)*, pp.45-50.
- Datla, D., Wyglinski, A. M. & Minden, G. J., 2009. A Spectrum Surveying Framework for Dynamic Spectrum Access Networks. *Vehicular Technology, IEEE Transactions*, 58(8), pp. pp. 4158-4168.
- David, M., 1999. *Decision procedures for the analysis of cryptographic Protocols by Logics of Belief.*, in Computer Security Foundations Workshop, 1999. Proceedings of the 12th IEEE, pp.44-54, 1999.
- Djahel, S., Naït-Abdesselam, F. & Turgut, D., 2009. *An effective strategy for greedy behavior in wireless ad hoc networks.* ., in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pp.1-6, Nov. 30 2009-Dec. 4 2009.
- Domenico, A. D., Strinati, E. C. & Benedetto, M.-G. D., 2012. A Survey on MAC Strategies for Cognitive Radio Networks. *IEEE Communications Surveys & Tutorials*, 14(1), pp. 21-44.
- Ejaz, W., Hasan, N. u., Kim, H. S. & Azam, M. A., 2011. *Fully distributed cooperative spectrum sensing for cognitive radio ad hoc networks.* ., in Frontiers of Information Technology (FIT), 2011, pp.9-13, 19-21 Dec. 2011.
- Enneya, N., Baayer, A. & ElKoutbi, M., 2011. A Dynamic Timestamp Discrepancy against Replay Attacks in MANET. *Informatics Engineering and Information Science*, Volume 254, pp. pp 479-489.
- Ertaul, L., Chavan, N., 2005. "Security of ad hoc networks and threshold cryptography," in *Wireless Networks, Communications and Mobile Computing, 2005 International Conference on*, vol.1, pp.69-74 vol.1, 13-16.
- Feng, W., Cao, J., Zhang, C. & Liu, C., 2009. *Joint optimization of spectrum handoff scheduling and routing in multi-hop multi-radio cognitive networks*, in Distributed Computing Systems, 2009. ICDCS '09. 29th IEEE International Conference on, pp.85-92, 22-26 June 2009.
- Fragkiadakis, A. G., Tragos, E. Z. & Askoxylakis, I. G., 2013. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. *Communications Surveys & Tutorials, IEEE*, 15(1), pp. 428,445.
- Gao, Z., Zhu, H., Li, S. & Du, S., 2012. Security and privacy of collaborative spectrum sensing in cognitive radio networks. *Wireless Communications, IEEE*, 19(6), pp. pp.106-112.
- Gavrilovska, L., Denkovski, D., Rakovic, V., Angelichinoski, M., 2014. "Medium Access Control Protocols in Cognitive Radio Networks: Overview and General Classification," in *Communications Surveys & Tutorials, IEEE*, vol.16, no.4, pp.2092-2124,
- Girraj, S. & Ritu, S., 2015. "A review on recent advances in spectrum sensing, energy efficiency and security threats in cognitive radio network"., *International Conference on Microwave, Optical and Communication Engineering (ICMOCE)*, Bhubaneswar, India, 2015, pp. 114-117.

## References

- Goyal, P., Batra, S. & Singh, A., 2010. A Literature Review of Security Attack in Mobile Ad-hoc Networks. *International Journal of Computer Applications*, 9(12), p. (0975 – 8887).
- Goyal, P., Parmar, V. & Rishi, R., 2011. MANET: Vulnerabilities, Challenges, Attacks, Application. *IJCEM International Journal of Computational Engineering & Management*, Volume 11, pp. 2230-7893.
- G, S. M., D'Souza, R. J. & Varaprasad, G., 2012. Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks. *IEEE Sensors Journal*, 12(10), pp. 2941-2949.
- Guo, Q., Luo, M., Li, L. & Yang, Y., 2010. Secure Network Coding against Wiretapping and Byzantine Attacks. *EURASIP Journal on Wireless Communications and Networking 2010*, Volume 2010, pp. 1-9.
- Hanen, I., Kevin, D. & Mustafa, S., 2014. *Security Challenges in Cognitive Radio Networks*. Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K., WCE.
- Harn, L. & Ren, J., 2011. Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications. *IEEE Transactions On Wireless Communications*, 10(7), pp. 2372-2379.
- Haythem, A., Salameh, B. & Krunz, M., 2009. Channel access protocols for multihop opportunistic networks: challenges and recent developments. *Network, IEEE*, 23(4), pp. 14-19.
- He, A., Bae, K. K., Newman, T. R., Gaedert, J. K., Kyouwoong; M. R., Morales-Tirado, L., Neel, J., Zhao, Y., Reed, J. H., Tranter, W. H., 2010. A Survey of Artificial Intelligence for Cognitive Radios. *Vehicular Technology, IEEE Transactions on*, 59(4), pp. 1578-1592.
- Huahui, W., Jian, R. & Tongtong, L., 2010. *Resource Allocation with Load Balancing for Cognitive Radio Networks*. in *Global Telecommunications Conference (GLOBECOM 2010)*, 2010 IEEE , pp.1-5, 6-10 Dec. 2010.
- Huang, L., Xie, L., Yu, H., Wang, W., Yao, Y., 2010. *Anti-PUE attack based on joint position verification in cognitive radio networks*. , in *Communications and Mobile Computing (CMC)*, 2010 International Conference on, vol.2, pp.169-173, 12-14 April 2010.
- Huayi, W. & Baohua, B., 2011. *An improved security mechanism in cognitive radio networks*, in *Internet Computing & Information Services (ICICIS)*, 2011 International Conference on, pp.353-356, 17-18 Sept. 2011.
- Hussein, H., Elsayed, H. A. & Elramly, S., 2013. *Performance Evaluation of Cognitive Radio Network Predictive MAC (P-MAC) Access Algorithm and its Enhancement*, in *Information Networking (ICOIN)*, 2013 International Conference on , pp.434-439, 28-30 Jan. 2013.
- Injosoft, A., 2015. *ASCII Code - The extended ASCII table*: Available at: <http://www.ascii-code.com/> [Accessed 27 Aug. 2015].
- Iyer, G. N. & Limt, Y. C., 2011. *Efficient Multi-channel MAC Protocol and Channel Allocation Schemes for TDMA Based Cognitive Radio Networks*, in *Communications and Signal Processing (ICCS)*, 2011 International Conference on , pp.394-398, 10-12 Feb. 2011.
- Jack, L. B., 2008. *Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security*, in *Cognitive Radio Oriented*

## References

- Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on, pp.1-7.
- Jakimoski, G. & Subbalakshmi, K. P., 2008. *Denial-of-Service Attacks on Dynamic Spectrum Access Networks*, Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference on, 19-23 May 2008, PP, 524 - 528.
- Jha, S. C., Rashid, M. M. & Bhargava, V. K., 2011. Medium Access Control in Distributed Cognitive Radio Networks. *IEEE Wireless Communications*, 18(4), pp. 41-51.
- Jhaveri, R. H., Patel, S. J. & Jinwala, D. C., 2012. *A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad Hoc Networks.*, in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on., pp.556-560, 7-8 Jan. 2012.
- Jhaveri, R. H., Patel, S. J. & Jinwala, D. C., 2012. *DoS attacks in mobile ad hoc networks: A survey*, in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on., pp.535-541, 7-8 Jan. 2012.
- Jia, J., Zhang, Q. & Shen, X., 2008. HC-MAC: A Hardware-Constrained Cognitive MAC for Efficient Spectrum Management. *IEEE Journal On Selected Areas In Communications*, VOL. 26, NO. 1, January 2008, 26(1), pp. 106 - 117.
- Jie, L., Lianggui, L., Ting, S. & Huiling, J., 2013. A Novel Performance Analysis of the IEEE 802.11 DCF with Hidden Stations. *International Journal of Smart Home*, 7(4), pp. 399-411.
- Jinhyung, O. & Wan, C., 2010. *A Hybrid Cognitive Radio System: A Combination of Underlay and Overlay Approaches.* , in Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd, pp.1-5, 6-9 Sept. 2010.
- Jin, Z., Anand, S. & Subbalakshmi, K. P., 2012. Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks. *IEEE Transactions on communications*, 60(9), pp. 635-2643.
- Jiwen, C. et al., 2010. *An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network.* , in Advanced Information Networking and Applications (AINA), 24th IEEE International Conference on, pp.775-780, 20-23 April 2010.
- Ji, Z. & Liu, K. J. R., 2007. Cognitive Radios For Dynamic Spectrum Access - Dynamic Spectrum Sharing: A Game Theoretical Overview. *Communications Magazine, IEEE*, 45(5), pp. pp. 88-94..
- Joe, I. & Son, S., 2008. *Dynamic Spectrum Allocation MAC Protocol based on Cognitive Radio for QoS*, in Frontier of Computer Science and Technology, 2008. FCST '08. Japan-China Joint Workshop on, pp.24-29, 27-28 Dec. 2008.
- José, M., Jorge, G. & Monteiro, a. E., 2015. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP Journal on Information Security*, vol 4, pp. 1-14.
- Joshi, A., Agrawal, K. K., Arora, D. & Shukla, S., 2011. Efficient Content Authentication in Ad-Hoc Networks Mitigating DDoS Attacks. *International Journal of Computer Applications*, 23(4), pp. 0975 – 8887.
- Joshi, G. P., Kim, S. W. & Kim, B.-S., 2009. An Efficient MAC Protocol for Improving the Network Throughput for Cognitive Radio Networks", in *Next*

## References

- Generation Mobile Applications, Services and Technologies*, 2009. NGMAST '09. Third International Conference on, pp.271-275.
- Kahraman, B. & Buzluca, F., 2010. *Protection and fairness oriented cognitive radio MAC protocol for ad hoc networks (PROFCR)*, in Wireless Conference (EW), 2010 European., pp.282-287, 12-15 April 2010.
- Kamruzzaman, S., 2010. An Energy Efficient Multichannel MAC Protocol for for Cognitive Radio Ad Hoc Networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 2(2), pp. 112-119.
- Kamruzzaman, S. M. & Alam, M. S., 2010. *Dynamic TDMA Slot Reservation Protocol for QoS Provisioning in Cognitive Radio Ad Hoc Networks. in Computer and Information Technology (ICCIT), 2010 13th International Conference on., pp.142-147, 23-25 Dec. 2010.*
- Kamruzzaman, S.M.; Hossain, M.A.; Alghamdi, A., 2015. "Energy efficient cognitive radio MAC protocol for battlefield communications," in *Electrical and Computer Engineering (CCECE), IEEE 28th Canadian Conference on*, vol., no., pp.1101-1108, 3-6 May 2015.
- Kanth, V. U., Chandra, K. R. & Kumar, R. R., 2013. Spectrum Sharing In Cognitive Radio Networks. *International Journal of Engineering Trends and Technology (IJETT)*, 4(4), pp. 1172-1175.
- Kariya, D. G., Kathole, A. B. & Heda, S. R., 2012. Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method. *International Journal of Emerging Technology and Advanced Engineering*, 2(1), pp. 37-41.
- Kaur, A., 2013. Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method. *International Journal of Scientific & Engineering Research*, 4(5), pp. 2212-2216.
- Khasawneh, M. & Agarwal, A., 2014. A Survey on Security in Cognitive Radio Networks. *2014 6th International Conference on CSIT, IEEE Computer Society*, PP. 64-70.
- Kim, H. & Kang G. Shin, 2008. Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks. *IEEE Transactions on mobile computing*, 7(5), pp. 533-545.
- Kleinjung, T., Aoki, K., Franke, J., Arjen, K. L., Emmanuel, T., Joppe, W. B., Pierrick, G., Alexander, K., Peter, L. M., Dag, A. O., Herman, T. R., 2010. Factorization of a 768-Bit RSA Modulus. In: v.6.o.L.N.i.C.S. Crypto 2010, ed. *Advanced*. Springer, Heidelberg, pp. 333-350.
- Kondareddy, Y. R. & Agrawal, P., 2008. *Synchronized MAC protocol for multi-hop cognitive radio networks*, in Communications, 2008. ICC '08. IEEE International Conference on, pp.3198-3202, 19-23 May 2008.
- Kondareddy, Y. R., Agrawal, P. & Sivalingam, K., 2008. *Cognitive Radio Network setup without a Common Control Channel.*, in Military Communications Conference, 2008. MILCOM 2008. IEEE, pp.1-6, 16-19 Nov. 2008.
- Koopman, P. & Szilagyi, C., 2013. Integrity in embedded control networks. *Security & Privacy, IEEE*, 11(3), pp. 61,63,.
- Krishna, M. B. & Doja, M. N., 2011. *Symmetric key management and distribution techniques in wireless ad hoc networks.*, in Computational Intelligence and

## References

- Communication Networks (CICN), 2011 International Conference on ., pp.727-731, 7-9 Oct. 2011.
- Kumar, M. S., & Rajalakshmi, S. (2014). "High Efficient Modified MixColumns in Advanced Encryption Standard using Vedic Multiplier". *Coimbatore: 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14.*, pp 462-466.
- Lee, W.-Y. & Akyildiz, I. F., 2008. Optimal spectrum sensing framework for cognitive radio networks. *IEEE Transactions On Wireless Communications*, 7(10), pp. 3845- 3857.
- Lee, Y.-h. & Kim, D., 2012. *A Slow Hopping MAC Protocol for Coordinator-based Cognitive Radio Network*. in Consumer Communications and Networking Conference (CCNC), 2012 IEEE., pp.854-858, 14-17 Jan. 2012.
- Leon, O., Hernandez-Serrano, J. & Soriano, M., 2010. Securing cognitive radio networks. *International Journal Of Communication Systems*, 23(5), pp. 633-652.
- Liang, S & M. K. K., 2009. Handling Multi-channel Hidden Terminals Using a Single Interface in Cognitive Radio Networks. In: *Emerging Intelligent Computing Technology and Applications. With Aspects of Artificial Intelligence*. Springer, pp. Volume 5755, 2009, pp 1039-1048.
- Li, H. & Han, Z., 2010. Catching attacker(s) for collaborative spectrum Sensing in Cognitive Radio Systems: An Abnormality Detection Approach. *New Frontiers in Dynamic Spectrum, IEEE Symposium*, pp. 1-12.
- Li, J., Feng, Z., Feng, Z. & Zhang, P., 2015. A survey of security issues in Cognitive Radio Networks. in *Communications, China*, 12(3), pp. 132-150.
- Li, L., Kidston, D. & Vigneron, P., 2011. Replay attacks and detection in tactical MANETs, in *Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference on.*, pp.226-231, 23-26 Aug. 2011.
- Li, X., Chen, J. & Ng, F., 2009. Secure transmission power of cognitive radios for dynamic spectrum access applications, *Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on*, PP, 213 - 218, 19-21 March 2008.
- Lin, F., Hu, Z., Hou, S., Yu, J., Zhang, C., Guo, N., M, Wicks, R.C, Qiu., K, Currie., 2011. *Cognitive radio network as wireless sensor network (II): Security consideration. in Aerospace and Electronics Conference (NAECON), Proceedings of the 2011 IEEE National.*, pp.324-328, 20-22 July 2011.
- Lin, Z., Liu, H., Chu, X. & Leung, Y.-W., 2011. *Jump-stay based channel-hopping algorithm with guaranteed rendezvous for cognitive radio networks.*, in INFOCOM, 2011 Proceedings IEEE, pp.2444-2452, 10-15 April 2011.
- Liu, Y., Hu, S., Xiao, Y. & Liu, X., 2010. *CSMA/CA-based MAC protocol in Cognitive Radio network*, in Wireless, Mobile and Multimedia Networks (ICWMNN 2010), IET 3rd International Conference on., pp.163-167, 26-29 Sept. 2010.
- Ma, L., Shen, C.-C. & Ryu, B., 2007. *Single-Radio Adaptive Channel Algorithm for Spectrum Agile Wireless Ad Hoc Networks*, in New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on, pp.547-558, 17-20 April 2007.

## References

- Mao, H. & Zhu, L., 2011. *An investigation on security of cognitive radio networks*, in Management and Service Science (MASS), 2011 International Conference on, pp.1-4, 12-14 Aug. 2011.
- Mathur, C. N. & Subbalakshmi, K. P., 2007. *Digital signatures for centralised DSA networks*, Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE, PP, 1037 - 1041.
- Mathur, C. & Subbalakshmi, K., 2007. *Security issues in cognitive radio networks*. In: *Cognitive networks: towards self-aware networks*.: John Wiley and Sons, Ltd; 2007 [chapter 11].
- Maziar, N., 2010. Cognitive Radio Access to TV White Spaces: Spectrum Opportunities, Commercial Applications and Remaining Technology Challenges., in *New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on* ., pp.1-10, 6-9 April 2010.
- Minho, J., Longzhe, H., Dohoon, K. & Hoh, P., 2013. Selfish attacks and detection in cognitive radio Ad-Hoc networks. *Network, IEEE*, 27(3), pp. 46, 50.
- Mitola, J., Maguire, G.Q., Jr., 1999, "Cognitive radio: making software radios more personal," in *Personal Communications*, IEEE, vol.6, no.4, pp.13-18.
- Naidu, A. A. & Joshi, P. K., 2015. "FPGA Implementation of Fully Pipelined Advanced Encryption Standard". *Melmaruvathur, Communications and Signal Processing (ICCSP), 2015 International Conference on*, pp. 0649-0653.
- Parvin, S., Han, S., Tian, B. & Hussain, F. K., 2010. *Trust-based authentication for secure communication in cognitive radio networks*., 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing., PP, 589 - 596.
- Parvin, S. & Hussain, F. K., 2011. *Digital signature-based secure communication in cognitive radio networks*. 2011 International Conference on Broadband and Wireless Computing, Communication and Applications.
- Parvin, S. & Hussain, F. K., 2012. *Trust-based Security for Communitybased Cognitive Radio Networks*., 2012 26th IEEE International Conference on Advanced Information Networking and Applications, 518-525.
- Parvin, S. et al., 2012. Cognitive radio network security: A survey. *Journal of Network and Computer Applications* 35 (2012), 35(6), p. 1691–1708.
- Prasad, N. R., 2008. *Secure Cognitive Networks*, in *Wireless Technology*, 2008. EuWiT 2008. European Conference on, pp.107-110, 27-28 Oct. 2008.
- Qian, C., Wai-Choong, W., Mehul, M. & Ying-Chang, L., 2013. MAC Protocol Design and Performance Analysis for Random Access Cognitive Radio Networks. *IEEE Journal on selected areas in communications*, 31(11), pp. 2289-2300.
- Rai, A. K., Tewari, R. R. & Upadhyay, S. K., 2010. Different Types of Attacks on Integrated MANET-Internet Communication. *International Journal of Computer Science and Security (IJCSS)*, 4(3), pp. 265 - 274.
- Rakhshanda, S., Shoab, A. K. & Attiq, A., 2008. *Augmented security in IEEE 802.22 MAC layer protocol*, in *Wireless Communications, Networking and Mobile Computing, WiCOM '08. 4th International Conference on*, pp.1-4, 12-14 Oct. 2008.

## References

- Reddy, Y. B., 2012. *Solving Hidden Terminal Problem in Cognitive Networks Using Cloud Technologies.* , SENSORCOMM 2012: The Sixth International Conference on Sensor Technologies and Applications., PP 235-240.
- Ren, P., Wang, Y., Du, Q. & Xu, J., 2012. A survey on dynamic spectrum access protocols for distributed cognitive wireless networks. *EURASIP Journal on Wireless Communications and Networking*, 2012(60), pp. 1687-1499.
- Rizvi, S., Mitchell, J. & Showan, N., 2014. Analysis of Security Vulnerabilities and Threat assessment in Cognitive Radio (CR) networks., *Application of Information and Communication Technologies (AICT)*, 2014 IEEE 8th International Conference on, Astana, 2014, pp. 1-6.
- Robles, R. S., Haas, J. J., Chiang, J. T., Hu, Y-C., Kumar, P. R., 2010. *Secure topology discovery through network-wide clock synchronization.*, in Signal Processing and Communications (SPCOM), 2010 International Conference on ., pp.1-5, 18-21 July 2010.
- Romero, E. et al., 2012. Simulation framework for security threats in cognitive radio networks. *Communications, IET*, 6(8), p. 984 –990.
- Pavithra, S. & Ramadevi, E., 2012. Performance Evaluation of Symmetric Algorithms. *Journal of Global Research in Computer Science*, 3(8), pp. 43 - 45.
- Safdar, G. & O'Neill, M., 2009. Common Control Channel Security Framework for Cognitive Radio Networks. in *Vehicular Technology Conference, VTC Spring 2009. IEEE 69th*, pp.1-5, 26-29 April 2009.
- Salameh, H. A. B., Krunz, M. M. & Younis, O., 2009. MAC protocol for opportunistic cognitive radio networks with soft guarantees. *IEEE Transactions on mobile computing*, 8(10), p. 1339–1352.
- Salameh, H. A. B., Krunz, M. & Younis, O., 2010. Cooperative adaptive spectrum sharing in cognitive radio networks. *Networking, IEEE/ACM Transactions on* , 18(4), pp. 1181 - 1194.
- Salameh, H. B., Krunz, M. & Younis, O., 2008. *Distance- and TrafficAware Channel Assignment in Cognitive Radio Networks.* , in Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON '08. 5th Annual IEEE Communications Society Conference on, pp.10-18, 16-20 June 2008.
- Sampath, A., Dai, H., Zheng, H. & Zhao, B. Y., 2007. *Multi-channel jamming attacks using cognitive radios.* , in Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on, pp.352-357, 13-16 Aug. 2007.
- Sanyal, S., Bhadauria, R. & Ghosh, C., 2009. *Secure communication in cognitive radio networks.* , n Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference on, pp.1-4, 14-16 Dec. 2009.
- Sazia, P., Farookh, K. H. & Omar, K. H., 2012. *Digital Signature-based Authentication Framework in Cognitive Radio Networks.*, MoMM '12 Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia; pp.,136-142.
- Sharma, K. R. & Rawat, D. B., 2015. "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey" in *IEEE Communications Surveys & Tutorials*,, 17(2), pp. 1023-1043.

## References

- Shin, K. G., Kim, H., Min, A. W. & Kumar, A. A., 2010. Cognitive radios for dynamic spectrum access: from concept to reality. *Wireless Communications, IEEE*, 17(6), pp. pp.64-74.
- Soleimani, M. T. & Ghasemi, A., 2011. *Detecting black hole attack in wireless ad hoc networks based on learning automata.*, in Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on., pp.514-519, Nov. 29 2011-Dec. 1 2011.
- Song, Y. & Xie, J., 2012. ProSpect: A Proactive Spectrum Handoff Framework for Cognitive Radio Ad Hoc Networks without Common Control Channel. *IEEE Transactions on mobile computing*, 11(7), pp. 1127-1139.
- Song, Y., Zhou, K. & Chen, X., 2012. Fake BTS Attacks of GSM System on Software Radio Platform. *Journal of networks*, 7(2), pp. 7, 275-281.
- Sood, V. & Singh, M., 2011. On the Performance of Detection based Spectrum Sensing for Cognitive Radio. *International Journal of Electronics & Communication Technology*, 2(3), pp. 140-143.
- Sorrells, C., Potier, P., Qian, L. & Li, X., 2011. *Anomalous spectrum usage attack detection in cognitive radio wireless networks*, in Technologies for Homeland Security (HST), 2011 IEEE International Conference on., pp.384-389, 15-17 Nov. 2011.
- Sowmya, N. K., Bhuvaneswari, H. & Nuthan, A., 2013. *Implementation of advanced encryption Standard-192 bit using multiple keys.*, Research & Technology in the Coming Decades (CRT 2013), National Conference on Challenges in, pp.1,7,.
- Stevenson, C. R., Chouinard, G., Lei, Z., Hu, W., Shellhammer, S. J., Caldwell, W., 2009. IEEE 802.22: The first cognitive radio wireless regional area network standard. *Communications Magazine, IEEE*, 47(1), pp. 130 - 138.
- Su, H. & Zhang, X., 2008. Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks. *IEEE journal on selected areas in communications*, 26(1), pp. 118-129.
- Sushma, M. & Dijiang, H., 2010. *IEEE 802.11 Wireless LAN Control Frame Protection*, Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE, pp.1-5.
- Taejoon, K. & Jong-Tae, L., 2009. Throughput Analysis Considering Coupling Effect in IEEE 802.11 Networks with Hidden Stations. *IEEE Communications letters*, 13(3), pp. 175-177.
- Tang, L. & Wu, J., 2012. Research and analysis on Cognitive Radio Networks Security. *Wireless Sensor Network*, 4(4), pp. 120-126.
- Tan, Y., Sengupta, S. & Subbalakshmi, K., 2011. Analysis of Coordinated Denial-of-Service Attacks in IEEE 802.22 Networks. *Selected Areas in Communications, IEEE Journal on*, 29(4), pp. 890,902.
- Tarmizi, S., Veeraraghavan, P., Ghosh, S., 2009. "Extending the collaboration boundary in localized threshold cryptography-based schemes for MANETs," in *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on*, pp.290-294, 15-17.
- Terence J, S., 2011. *Secure route discovery against wormhole attacks in Sensor Networks using Mobile Agents.*, in Trendz in Information Sciences and Computing (TISC), 2011 3rd International Conference on, pp.110-115, 8-9 Dec. 2011.

## References

- Theis, N. C., Thomas, R. W. & DaSilva, L. A., 2011. Rendezvous for Cognitive Radios. *IEEE Transactions on mobile computing*, 10(2), pp. 216 - 227.
- Timalsina, S. K., Moh, S., Chung, I. & Kang, M., 2013. A concurrent access MAC protocol for cognitive radio ad hoc networks without common control channel. *EURASIP Journal on Advances in Signal Processing*, 2013(69), pp. 1-13.
- Toldinas, J; Stuikys, V; Damasevicius, R; Ziberkas, G; Banionis, M., 2011. Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices. *Electronics & Electrical Engineering*, 108(2), pp. 11-14.
- Ucek, T. Y. & Arslan, H., 2009. A survey of spectrum sensing algorithms for cognitive radio applications. *Communications Surveys & Tutorials, IEEE*, 11(1), pp. 116-130.
- Uk.mathworks.com, 2009. *Uk.mathworks.com*. [Online] Available at: <http://uk.mathworks.com/products/matlab/?refresh=true> [Accessed 28 08 2015].
- Umamahesw, Ari. A; V, S Ubashini.; Subharriy, A. P., 2012. *Survey on performance, reliability and future proposal of cognitive radio under wireless computing*. in Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on., pp.1-6, 26-28 July 2012.
- Venkateswaran, P., Shaw, S., Pattanayak, S. & Nandi, R., 2012. Cognitive Radio Ad-Hoc Networks: Some New Results on Multi-Channel Hidden Terminal Problem. *Communications and Network*., 4(4), pp. 342-348.
- Vu, H. L. & Sakurai, T., 2006. Collision Probability in Saturated IEEE 802.11 Networks, *Australian Telecommunication Networks & Applications Conference (ATNAC)*, Australia, December, 2006.
- Wang, H., Qin, H. & Zhu, L., 2008. A survey on MAC protocols for opportunistic spectrum access in cognitive radio networks, in *Computer Science and Software Engineering, 2008 International Conference on* , vol.1., pp.214-218, 12-14 Dec. 2008, pp. 214-218.
- Wang, J., Ghosh, M., Challapali, K., 2011. "Emerging cognitive radio applications: A survey," in *Communications Magazine, IEEE*, vol.49, no.3, pp.74-81.
- Wang, L.-C., Wang, C.-W. & Adachi, F., 2011. Load-Balancing Spectrum Decision for Cognitive Radio Networks. *IEEE journal on selected areas in communications*, 29(4), pp. 757,769.
- Wang, W., 2009. *Spectrum sensing for cognitive radio*, Third International Symposium on Intelligent Information Technology Application Workshops, pp: 410-412. .
- Wang, Z., Wang, H, Feng, G., Li, B., Chen, X., 2010. *Cognitive networks and its layered cognitive architecture*., in Internet Computing for Science and Engineering (ICICSE), 2010 Fifth International Conference on., pp.145-148, 1-2 Nov. 2010.
- Wan, W., Lit, H., Sun, Y. & Han, Z., 2009. *Attack-proof collaborative spectrum sensing in cognitive radio networks*, in Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on pp.130-134, 18-20 March 2009.

## References

- Wei, W., 2011. *The research of cognitive communication networks*. in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on., pp.1-5, 27-29 May 2011.
- Wu, Y., Wang, B., Liu, K. J. R. & Clancy, T. C., 2012. Anti-Jamming Games in Multi-Channel Cognitive Radio Networks. *IEEE journal on selected areas in communications*, 30(1), pp. 4-15,.
- Wyglinski, A. M., Nekovee, M. & Hou, Y. T., 2010. *Cognitive Radio Communications and Networks: Principles and Practice*. California: ELSEVIER Inc.
- Xiang, J., Zhang, Y. & Skeie, T., 2010. Medium access control protocols in cognitive radio networks. *Journal of Wireless Communications and Mobile Computing—Recent Advances in Wireless Communications and Networks*, 10(1), p. 31–49.
- Xiaopeng, G. & Wei, C., 2007. *A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks*, in Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on, pp.209-214, 18-21 Sept. 2007.
- Yi, P., Zhu, T., Liu, N., Wu, Y., Li, J., 2012. Cross-layer Detection for Black Hole Attack in Wireless Network. *Journal of Computational Information Systems*: 8(10), p. 4101–4109.
- Yin, S., Chen, D., Zhang, Q. & Li, S., 2011. Prediction-based throughput optimization for dynamic spectrum access. *IEEE Transactions on vehicular technology*, 60(30), pp. 1284–1289.
- Yoo, S.-J., Nan, H. & Hyon, T.-I., 2009. DCR-MAC: distributed cognitive radio MAC protocol for wireless ad hoc networks. *Wireless Communications and Mobile Computing*, 9(5), p. 631–653.
- Yuan, Z. et al., 2012. Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks. *IEEE Journal on selected areas in communications*, 30(10), pp. 1850-1860.
- Yu, F. R., Tang, H., Wang, F. & Leung, V. C., 2010. Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks. *Springer Science+Business Media, LLC*, 16(8), p. 2169–2178.
- Zhang, X. & Li, C., 2009. *The security in cognitive radio networks: A survey*. , Proceedings of the 2009 ACM International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC '09), New York, 2009, pp.309-313.
- Zhang, X. & Su, H., 2011. Cream-mac: cognitive radio-enabled multi-channel mac protocol over dynamic spectrum access networks. *IEEE Journal of selected topics in signal processing*, 5(1), pp. 110-123.
- Zhang, Y., Xu, G. & Geng, X., 2008. *Security threats in cognitive radio networks*, in High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on, pp.1036-1041.
- Zhang, Y., Yu, G., Li, Q., Wang, H., Zhu, X., Wang, B., 2014. Channel-Hopping-Based Communication Rendezvous in Cognitive Radio Networks. *IEEE/ACM Transactions on networking*, 22(3).
- Zhang, Y. & Lazos, L., 2013. "Vulnerabilities of Cognitive Radio MAC Protocols and Countermeasures". in *IEEE Network*, 27(3), pp. 40-45

## References

- Zhao, Q. & Swami, A., 2007. *A survey of dynamic spectrum access: Signal processing and networking perspectives*, in Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on , vol.4, pp.IV-1349-IV-1352, 15-20 April 2007.
- Zhao, Q., Tong, L., Swami, A. & Chen, a. Y., 2007. Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework. *Selected Areas in Communications, IEEE Journal on*, 25(3), pp. pp. 589-600.
- Zheng, Cao, L. & Haitao, 2008. Distributed Rule-Regulated Spectrum Sharing. *Selected Areas in Communications, IEEE Journal on*, 26(1), pp. pp. 130-145.
- Zhou, X., Xiao, Y. & Li, Y., 2011. *Encryption and displacement based scheme of defense against primary user emulation attack.*, in Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on ., pp.44-49, 27-30 Nov. 2011.
- Zhu, L. & Mao, H., 2010. *Research on authentication mechanism of cognitive radio networks based on certification authority*, Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on , pp.1,5, 10-12 Dec. 2010.
- Zhu, L. & Mao, H., 2011. *An Efficient Authentication Mechanism for Cognitive Radio Networks.*, Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific., pp.1,5, 25-28 March 2011.
- Zhu, L. & Mao, H., 2011. *Unified Layered Security Architecture for Cognitive Radio Networks.*, n Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific, pp.1-4, 25-28 March 2011.
- Zhu, L. & Zhou, H., 2008. *Two types of attacks against Cognitive radio network MAC protocols.* in Computer Science and Software Engineering, 2008 International Conference on , vol.4., pp.1110-1113.
- Zou, Y. & Yoo, S., 2015. "A cooperative attack detection scheme for common control channel security in cognitive radio networks," in Ubiquitous and Future Networks (ICUFN), 2015 Seventh International Conference on. pp. 606-611.