SECURE SPECTRUM SENSING for SATELLITE ASSISTED COGNITIVE RADIO NETWORKS

by

Seda Demirağ Ersöz

B.S. in Computer Science, Bilgi University, 2005

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Department of Computer Engineering

Boğaziçi University

2010

SECURE SPECTRUM SENSING for SATELLITE ASSISTED COGNITIVE RADIO NETWORKS

APPROVED BY:

Assoc. Prof. Fatih Alagöz (Thesis Supervisor)	.....
Prof.Dr. Emin Anarım	.....
Prof.Dr. M. Ufuk Çağlayan	.....

DATE OF APPROVAL: 22.04.2010

ACKNOWLEDGEMENTS

I would like to express my deep and sincere gratitude to my supervisor, Assoc. Prof. Fatih Alagöz. His wisdom and logical way of thinking have been of great value for me. His understanding, encouraging and personal guidance have provided a good basis for this thesis.

This thesis would not have been possible without the support of Suzan Bayhan. I wish to express my gratitude to her for her abundant help and invaluable assistance, support and guidance.

I would like to express my sincere thanks to my employers in TUBİTAK-UEKAE for their support in my graduate study along with my professional life. I am really grateful to all of my colleagues for encouraging me throughout this journey.

I owe my heartfelt thanks to my loving husband, Doğan Ersöz. Without his encouragement and understanding it would have been impossible for me to finish this thesis. He was right here by my side whenever I felt down with his endless patience and love. I am also grateful to him for making all his plans by considering my graduate study.

I wish to express my gratitude to my mother, Münevver Demirağ for embracing me with her endless love and care and my sister Serap Demirağ and brother Murat Demirağ for their valuable advices. Finally, I would like to express my love to my little niece Deren and nephew Maxime Demir for being so cute and making my all stress go away.

ABSTRACT

SECURE SPECTRUM SENSING for SATELLITE ASSISTED COGNITIVE RADIO NETWORKS

In this thesis study, we propose a security structure for spectrum sensing and decision scheme for a satellite assisted Cognitive Radio Network (CRN). The main goal of Cognitive Radio (CR) is to provide agility in the spectrum access and operations parameters. Hence, performance of wireless transmission can be optimized. Additionally, CR facilitates more efficient spectrum utilization which is a fundamental issue in the emerging communications paradigm of anytime-anywhere access. In order to provide spectrum agility, CRs have some additional functionalities (eg. remote configurability, spectrum analysis, primary user detection) different from the ones in wireless networks. These functionalities come at the expense of various challenges such as spectrum management and reliable primary user detection. In an infrastructure-based CRN where the network is divided into cells, spectrum management and resource allocation in each cell is managed by the base station (BS) of each cell. However, these may require extensive message exchanges among the BSs. Instead, a satellite with its wide coverage can assist the BSs to provide a more reliable spectrum environment map. Additionally, it can provide the management functionalities and regular policy updates by message broadcasts. Different from the conventional wireless networks, this structure–referred to as *satellite assisted CRN*, may be exposed to new security attacks. We investigate these security threats, evaluate their risk levels and provide cryptographic and non-cryptographic counter-measures. This investigation points out which security services need to be employed in order to design a robust security scheme for this structure. Considering the properties and the restrictions of the CRN segment and the satellite segment, we design a two-tiered security structure. We apply confidentiality, entity and data origin authentication, cryptographic nonce and integrity security services to our security structure. Since these security services can be provided by using different

security solutions, we present a detailed security and performance evaluation of the proposed security solution. The performance of proposed structure is analyzed under varying number of CRs in the network and varying CR handover frequency. The performance results show that the proposed approach is secure and efficient in terms of bandwidth usage and processing cost.

ÖZET

UYDU SİSTEMLERİ YÖNETİMİNDEKİ BİLİŞSEL AĞLAR için GÜVENLİ SPEKTRUM ALGILAMA

Bu tez çalışmasında, uydu sistemleri yönetimindeki bilişsel ağlarda spektrum algılama ve karar verme prosedürü için bir güvenlik mimarisi tanımlıyoruz. Bilişsel ağların temel amacı spektrum kullanımına ve operasyon parametrelerine çeviklik getirmektir. Böylece, kablosuz iletişimin performansı arttırılmaktadır. Buna ek olarak, bilişsel ağlar, yeni gelişen bir paradigma olan her zaman her yerde iletişim için olmassa olmaz olan verimli spektrum kullanımını sağlamaktadır. Spektrum kullanımında çeviklik sağlayabilmek için bilişsel ağlar koblosuz ağlardan farklı olarak, yeni özellikler (uzaktan ayarlanabilme, spektrumu analiz etme ve kullanım kararı verme, lisanslı kullanıcının iletişimini algılama v.b.) barındırmaktadırlar. Bu yeni özellikler, spektrum yönetimi ve güvenilir lısanslı kullanıcı bulma gibi yeni sorunlar ile gelmektedir. Ağ yapısının hücrelere bölündüğü bilişsel ağlarda, spektrum yönetimi ve kaynak kullanımı her hücrenin baz istasyonu tarafından gerçekleşmektedir. Bu yapının yerine, baz istasyonlarını geniş kapsama alanı ile uydu kontrol ederek, spektrum için daha güvenilir bir çevre haritası çıkarabilmektedir. Bunlara ek olarak, uydu yayın yaparak yönetimsel yararlılık ve politika güncellemeyi sağlamaktadır. Uydu sistemleri yönetimindeki bilişsel ağlar olarak tanımladığımız yapımız, geleneksel kablosuz ağlara göre yeni güvenlik açıklarına yol açmaktadır. Biz, bu yeni güvenlik ataklarını, risk derecelerini ve bu ataklara karşı alınabilecek önlemleri araştırdık. Yapılan bu araştırma ile geliştireceğimiz güvenlik mimarisi güçlü kılmak için gerekli olan tüm güvenlik servislerini belirledik. Bilişsel ağlardan oluşan kısım ile uydu ağlarından oluşan kısmın özelliklerini ve kısıtlarını göz önünde bulundurarak, iki katmanlı bir ağ yapısı tanımlıyoruz. Tasarlanan güvenlik mimarisinde, gizlilik, taraf ve veri kaynağı asıllama, kriptografik pul ve bütünlük servislerini kullanıyoruz. Bu güvenlik servisleri farklı yöntemler kullanılarak sağlanabildiğinden, detaylı performans ve güvenlik

değerlendirmesi yapıyoruz. Önerilen mimarinin performansı, değisen bilişsel radyo sayısı ve bu radyoların hücre değiştirme sıklığı kullanılarak analiz edilmektedir. Yapılan performans analizleri gösteriyor ki, önerilen mimari band genişliği kullanımı ve işlem maliyetine göre verimli ve güvenli olduğunu göstermektedir.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS . . . iii
ABSTRACT . . . iv
ÖZET . . . vi
LIST OF FIGURES . . . x
LIST OF TABLES . . . xiii
LIST OF ABBREVIATIONS . . . xiv
1. INTRODUCTION . . . 1
2. COGNITIVE RADIO NETWORKS . . . 3
2.1. CR Architecture . . . 4
2.2. CR Functionalities . . . 5
2.2.1. Spectrum Sensing . . . 5
2.2.2. Spectrum Analysis . . . 6
2.2.3. Spectrum Access . . . 7
2.2.4. Spectrum Mobility . . . 7
2.3. CR Components . . . 7
2.4. Applications of CR . . . 9
2.5. CR Standardization . . . 11
2.5.1. IEEE Standards Coordinating Committee 41 . . . 11
2.5.2. IEEE 802.22 . . . 13
3. FOUNDATIONS OF COMMUNICATION SECURITY . . . 16
3.1. Availability . . . 16
3.2. Integrity and Message (Data Origin) Authentication . . . 16
3.3. Identification and Entity Authentication . . . 19
3.4. Confidentiality . . . 20
3.5. Group Key Management Techniques . . . 21
4. COGNITIVE RADIO NETWORKS SECURITY ISSUES . . . 23
4.1. CRNs Security Related Works in Literature . . . 23
4.2. Security Vulnerabilities, Threat Analysis, and Countermeasures . . . 37
4.2.1. Primary User Emulation Attack . . . 38

4.2.2. Eavesdropping and Traditional Jamming Attack 39
4.2.3. Faulty Data Injection 40
4.2.4. Intentional / Non-intentional Modifications 40
4.2.5. Replay Attack 41
4.3. IEEE 802.22 Security Sublayer 41
4.3.1. RSA-based Authentication and Key Derivation 43
4.3.2. EAP Authentications 46
4.3.3. Critiques on IEEE 802.22 Security Structure 47
5. PROPOSED SECURITY STRUCTURE 51
5.1. Security Structure for Communication Tier 1 52
5.1.1. Initialization 54
5.1.2. Join Network 54
5.1.3. Sending Sensing Data and Multicast Decision 56
5.1.4. Inter-cell Communications 57
5.2. Security Structure for Communication Tier 2 58
5.2.1. Initialization 59
5.2.2. Join Operation 59
5.2.3. Sending Sensing Data and Multicast Decision 62
5.2.4. Handover between Base Stations 63
5.2.5. Re-keying 63
5.3. Analysis of Proposed Security Structure 64
5.3.1. Key Management Techniques - Performance Analysis 64
5.3.2. Cryptographic Algorithms - Performance Analysis 77
5.3.3. Cryptographic Protocols and Structural Design - Performance Analysis 83
6. CONCLUSION AND FUTURE DIRECTION 88
REFERENCES 90

LIST OF FIGURES

Figure 2.1. CR Protocol Architecture 5

Figure 2.2. CR Cycle 9

Figure 3.1. Classification of Hash Functions 18

Figure 3.2. Classification of Encryption Algorithms 20

Figure 4.1. Steps of Security Protocol 34

Figure 4.2. RSA Based Authentication and Key Distribution in IEEE 802.22 . 44

Figure 4.3. RSA Based Authentication - AK from PAK 45

Figure 4.4. HMAC/CMAC/KEK derivation from AK 46

Figure 4.5. AK derivation from EAP authentication 47

Figure 4.6. AK derivation from RSA based authentication followed by EAP authentication 48

Figure 4.7. AK derivation from EAP-in-EAP authentication 48

Figure 4.8. HMAC/CMAC/KEK derivation from EIK 49

Figure 5.1. Satellite Assisted Network Model 51

Figure 5.2. Communication Tiers 52

Figure 5.3. Tier 1 Security Structure - Join Network 56

Figure 5.4. Tier 1 Security Structure - Spectrum Sensing and Decision 57

Figure 5.5. Tier 2 Security Structure - Join Network 61

Figure 5.6. Tier 2 Security Structure - Spectrum Sensing and Decision 61

Figure 5.7. Tier 2 Security Structure - Handover between Cells 61

Figure 5.8. LKH Key Management Scheme - Re-keying 65

Figure 5.9. Initial processing costs for KDC 69

Figure 5.10. Initial processing costs for Members 70

Figure 5.11. Join processing costs for KDC 70

Figure 5.12. Join processing costs for Members 71

Figure 5.13. Leave processing costs for KDC 71

Figure 5.14. Leave processing costs for Members 72

Figure 5.15. Initial bandwidth costs of key management schemes 73

Figure 5.16. Join bandwidth costs of key management schemes 74

Figure 5.17. Leave bandwidth costs of key management schemes 74

Figure 5.18. Storage costs for KDC 75

Figure 5.19. Storage costs for Members 75

Figure 5.20. Total Re-Keying Bandwidth Cost 76

Figure 5.21. Total Rekeying Processing Cost 77

Figure 5.22. Execution times of encryption/decryption algorithms 80

Figure 5.23. Processing and bandwidth costs of Tier 1 and Tier 2 join operations 85

Figure 5.24. Join vs. Handover Bandwidth and Processing Cost 86

Figure 5.25. Total time spent during join protocol 87

LIST OF TABLES

Table 4.1. Risk Analysis 39

Table 4.2. Risk Countermeasures 39

Table 4.3. Spectrum Sensing and Decision Security Risk Analysis 41

Table 4.4. Spectrum Sensing and Decision Countermeasures 42

Table 5.1. Bandwidth Cost of Key Management Schemes 66

Table 5.2. Storage Cost of Key Management Schemes 66

Table 5.3. Initialization - Processing Cost of Key Management Schemes . . . 66

Table 5.4. Join/Leaving - Processing Cost of Key Management Schemes . . . 67

Table 5.5. Notations in Tables 5.1, 5.2, 5.3 67

Table 5.6. Comparable key sizes for equivalent security levels 78

Table 5.7. Execution times (in ms) of encryption with different packet size . . 79

Table 5.8. Execution times (in ms) of decryption with different packet size . . 80

Table 5.9. Bandwidth and Processing Costs of Tier 1 and Tier 2 84

Table 5.10. Notations in Table 5.9 85

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
AES-CCM	AES, Counter mode with CBC-MAC
AP	Access Point
BS	Base Station
CPE	Customer Premises Equipment
CRHF	Collision Resistant Hash Functions
CRN	Cognitive Radio Network
DES	Data Encryption Standard
DoS	Denial of Service
DSA	Dynamic Spectrum Access
DSS	Dynamic Spectrum Access
EAP	Extensible Authentication Protocol
EAP-SIM	EAP Method for GSM Subscriber Identity
EAP-SRP	EAP Method for Secure Remote Password Protocol
EAP-TLS	EAP Method for Transport Layer Security
EIK	EAP Integrity Key
ESR	Environment Status Report
FCC	Federal Communications Commission
GKEK	Group Key Encryption Key
GPS	Global Positioning System
GTEK	Group Traffic Encryption Key
ITS	Intelligent Transportation System
KDC	Key Distribution Center
KEK	Key Encryption Key
MAC	Message Authentication Code
MPDU	Message Protocol Data Unit
MSDU	Message Service Data Unit
MSK	Master Session Key
OBU	Onboard Unit

OFDMA	Orthogonal Frequency-Division Multiple Access
OWHF	One-Way Hash Functions
PAK	Primary Authentication Key
PU	Primary User
PUE	Primary User Emulation
QoS	Quality of Service
QP	Quite Period
RSU	Roadside Unit
SBS	Secondary Base Station
SCC	IEEE Standards Coordinating Committee
SDR	Software Defined Radio
SU	Secondary User
TDMA	Time Division Multiple Access
TEK	Traffic Encryption Key
VANET	Vehicular Ad-hoc Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WRAN	Wireless Regional Area Network
WSPRT	Wald's Sequential Probability Ratio Test

1. INTRODUCTION

The key idea of cognitive radio (CR) networks is to allow the secondary, unlicensed users to detect and access unused portions of the spectrum (white spaces) opportunistically. The two main constraints in the design of CR networks (CRNs) are to make sure that this opportunistic access is done without any disruption of service to the primary users (PUs) and without any modifications to the primaries themselves. The main functions of the CRNs over traditional radios are remote reconfigurability, spectrum sensing, spectrum decision (spectrum policy) and geo-location. These new functionalities enable a CR to identify unlicensed bands and decide opportunistic secondary use in these bands without causing interference to PUs.

CRNs are classified into two depending on their network architecture: centralized and distributed. In a centralized architecture, the network is divided into cells and each cell is managed through a secondary base station (SBS). The secondary users (SUs) are synchronized with their base stations (BSs) and may perform periodic spectrum-sensing operations. The SBSs can be interconnected through a wired backbone network. In distributed CRNs, SUs make decisions on spectrum bands, transmit power, etc., based on either local observations or cooperatively through some utility functions to get optimum performance for all the SUs.

Most architectures and protocols for CR networks in the literature assume that all parties are honest and that there are no attackers. However, in addition to utilities of traditional radios, CRs have the ability of sensing spectrum activities and deciding in what band and how they may communicate. While this ability is an answer to overwhelm inefficient usage of available spectrum, this ability of it comes with lots of new security threats.

We consider the satellite assisted CRN architecture which is proposed in [1] as our network architecture. This architecture consists of a LEO satellite, SBS, SU and PU. The satellite is the main controller of the network. It is in charge of the spec-

trum allocation and management, policy updates and software updates. SBSs have a direct duplex communication link with the LEO satellite and they are capable of opportunistically using the spectrum. SBSs gather status information in the form of a Environment Status Report (ESR) and send this information to the satellite. ESRs consist of Secondary User Reports (SURs), which contain interference values sensed at each frequency by the corresponding SU. The LEO satellite does the spectrum allocation based on the ESR values by maximizing an objective function, such as the total throughput.

In this thesis we focus on basic security concepts like availability, confidentiality, integrity, non-repudiation, identification, authentication and authorization which are detailed in Chapter 3. We examine security related work in literature and define possible threats for CRNs by also giving their countermeasures in Chapter 4. Furthermore, we propose a two-tiered secure spectrum sensing and decision structure in Chapter 5. Additionally, the performance of proposed structure is analyzed under varying number of CRs in the network and varying CR handover frequency in this chapter. Chapter 6 concludes this thesis study.

2. COGNITIVE RADIO NETWORKS

The Software Defined Radio (SDR) forum and IEEE approved this definition of a CR [2]:

- Radio in which communications systems are aware of their environment and internal state, and can make decisions about their radio operating behavior based on that information and predefined objectives. The environment information may or may not include location information related to communication systems.
- CR(as defined above)that uses SDR, adaptive radio, and other technologies to automatically adjust its behavior or operations to achieve desired objectives.

CRs are proposed as a solution to the problem of efficient utilization of the overcrowding spectrum and opening space for the new wireless communication technologies. Since, most of the available radio spectrum has already been allocated to existing wireless systems, only small parts of radio spectrum can be licensed to new wireless applications. The major factor that leads to inefficient use of the radio spectrum is the spectrum licensing scheme itself. In the current spectrum licensing scheme, the type of spectrum usage cannot be dynamic. For example, a TV band which is allocated to analog TV cannot be used by digital TV broadcast or broadband wireless access technologies. However, this TV band could remain largely unused in many locations due to cable TV systems. Since frequency spectrum is usually allocated to a particular user or wireless service provider in a large region, the allocated frequency spectrum remains unused in other areas. A wireless service provider is generally licensed with a large chunk of radio spectrum. However, there can exist some wireless technologies which may require smaller bandwidth in order to provide temporary wireless access service. In the current spectrum licensing scheme, only a licensed user (LU) can access the corresponding radio spectrum and unlicensed users are prohibited from accessing the spectrum even though it is unoccupied by the LUs. For example, in a cellular system, there could be areas in a cell without any users. In such a case, unlicensed users with short-range wireless communications would not be able to access the spectrum, even

though their transmission would not interfere with cellular users. All of these limitations can be overcome by modifying the spectrum licensing scheme to make spectrum access more flexible by allowing unlicensed users to access the spectrum under some restrictions [3].

The main goal of CR is to provide adaptability to wireless transmission through dynamic spectrum access so that the performance of wireless transmission can be optimized, as well as enhancing the utilization of the frequency spectrum. The major functionalities of a CR system are spectrum sensing, spectrum analysis, spectrum access, and spectrum mobility. Through spectrum sensing, the information of the target radio spectrum has to be obtained so that it can be utilized by the CR user. The spectrum sensing information is exploited by the spectrum analysis function to analyze the spectrum opportunities and make decisions on spectrum access. If the status of the target spectrum changes, the spectrum mobility function controls the change of operational frequency bands for the CR users.

2.1. CR Architecture

Since the SDR supports multiband, multistandard, multiservice, and multichannel operations, RF front-end is designed based on SDR in physical layer of CRs. While most of the components in SDR (i.e. data processing, analog-to-digital converter, and baseband processing) are similar to those in traditional transceivers, the difference is that each component can be controlled from the protocols in the upper layers or can be reconfigured by the cognitive radio module. The MAC, network, transport, and application layers which are also called as adaptive protocols should be aware of the variations in the CR environment. In particular, the adaptive protocols should consider the traffic activity of primary users, the transmission requirements of secondary users, and variations in channel quality, etc. To link all modules, a CR control is used to establish interfaces among the SDR transceiver, adaptive protocols, and wireless applications and services. This cognitive radio module uses intelligent algorithms to process the measured signal from the physical layer, and to receive information on transmission requirements from the applications to control the protocol parameters in

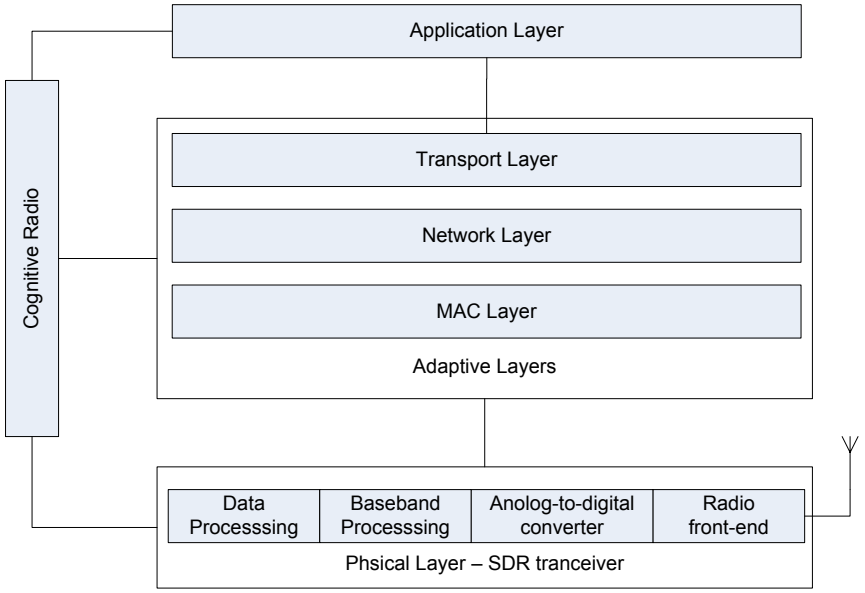


Figure 2.1. CR Protocol Architecture

different layers [3].The protocol architecture of CR is shown in Figure 2.1.

2.2. CR Functionalities

2.2.1. Spectrum Sensing

The goal of spectrum sensing is to determine the status of the spectrum and the activity of the LUs by periodically sensing the target frequency band. In particular, a CR transceiver detects an unused spectrum (also called spectrum hole) and also determines the method of accessing it without interfering with the transmission of a LU. Spectrum sensing can be either centralized or distributed. In centralized spectrum sensing, a sensing controller (e.g. access point(AP) or BS) senses the target frequency band, and the information thus obtained is shared with other nodes in the system. Centralized spectrum sensing can reduce the complexity of user terminals, since all the sensing functions are performed at the sensing controller. However, centralized spectrum sensing suffers from location diversity. For example, the sensing controller may not be able to detect an unlicensed user at the edge of the cell. In distributed spectrum sensing, unlicensed users perform spectrum sensing independently, and the spectrum sensing results can be either used by individual CRs (i.e. non-cooperative

sensing) or shared with other users (i.e. cooperative sensing). Although cooperative sensing incurs a communication and processing overhead, the accuracy of spectrum sensing is higher than that of non-cooperative sensing. Due to the type of sensing method, hidden node issue may occur. An unlicensed transmitter may not always be able to detect the signal from a licensed transmitter due to its geographic separation and channel fading. This is referred to as the *hidden node problem*. In this case, when the unlicensed user transmits, it will interfere with the receiver of the LU. To solve the *hidden node problem* in non-cooperative transmitter sensing, cooperative spectrum sensing can be used. In cooperative sensing, spectrum sensing information from multiple unlicensed users are exchanged among each other to detect the presence of LUs. The cooperative spectrum sensing architecture can be either centralized or distributed. Using cooperative exchange of spectrum sensing information, the *hidden node problem* can be solved and the detection probability can be significantly improved in a heavily shadowed environment. However, this is possible at the expense of communication and computation overhead compared with non-cooperative sensing. For cooperative sensing, two different networks (i.e. a sensor network and an operational network) can be deployed to perform spectrum sensing and access, respectively. In this case, the sensor network collects spectrum usage information of licensed users which can be processed by a central controller. Then a spectrum usage map is created and distributed to the operational network of unlicensed users for optimizing the spectrum access.

2.2.2. Spectrum Analysis

The information obtained from spectrum sensing is used to schedule and plan spectrum access by the unlicensed users. In this case, the communication requirements of unlicensed users are also used to optimize the transmission parameters. Major components of spectrum management are spectrum analysis and spectrum access optimization. In spectrum analysis, information from spectrum sensing is analyzed to gain knowledge about the spectrum holes (e.g. interference estimation, duration of availability, and probability of collision with a licensed user due to sensing error). Then, a decision to access the spectrum (e.g. frequency, bandwidth, modulation mode, transmit power, location, and time duration) is made by optimizing the system performance

given the desired objective (e.g. maximize the throughput of the unlicensed users) and constraints (e.g. maintain the interference caused to licensed users below the target threshold).

2.2.3. Spectrum Access

After a decision is made on spectrum access based on spectrum analysis, the spectrum holes are accessed by the unlicensed users. Spectrum access is performed based on a cognitive medium access control (MAC) protocol, which intends to avoid collision with LUs and also with other unlicensed users. The CR transmitter is also required to perform negotiation with the CR receiver to synchronize the transmission so that the transmitted data can be received successfully. A cognitive MAC protocol could be based on a fixed allocation MAC (e.g. FDMA, TDMA, CDMA) or a random access MAC (e.g. ALOHA, CSMA/CA).

2.2.4. Spectrum Mobility

Spectrum mobility is a function related to the change of operating frequency band of CR users. When a LU starts accessing a radio channel which is currently being used by an unlicensed user, the unlicensed user must vacate this band and switch to another band which is idle. This change in operating frequency band is referred to as spectrum handoff. During spectrum handoff, the protocol parameters at different layers in the protocol stacks, have to be adjusted to match the new operating frequency band. Spectrum handoff must ensure that the data transmission by the unlicensed user can continue in the new spectrum band. New channel for SU transmission should be found as quick as possible. otherwise, SU communication suffers from service disruption, during these channel switchings.

2.3. CR Components

The main components of CR are as follows [3]:

- **Transmitter/Receiver:** An SDR-based wireless transceiver is the major component with the functions of data signal transmission and reception. In addition, a wireless receiver is also used to observe the activity on the frequency spectrum (i.e. spectrum sensing). The transceiver parameters in the CR node can be dynamically changed as dictated by higher layer protocols.
- **Spectrum Analyzer:** The spectrum analyzer uses measured signals to analyze the spectrum usage (e.g. to detect the signature of a signal from a LU and to find spectrum holes for unlicensed users to access). The spectrum analyzer must ensure that the transmission of an LU is not interfered with if an unlicensed user decides to access the spectrum. In this case, various signal-processing techniques can be used to obtain spectrum usage information.
- **Learning/Knowledge Extraction:** Learning and knowledge extraction use the information on spectrum usage to understand the ambient RF environment (e.g. the behavior of LUs). A knowledge base of the spectrum access environment is built and maintained, which is subsequently used to optimize and adapt the transmission parameters to achieve the desired objective under various constraints. Machine learning algorithms from the field of artificial intelligence can be applied for learning and knowledge extraction.
- **Decision Making:** After the knowledge of the spectrum usage is available, the decision on accessing the spectrum has to be made. The optimal decision depends on the ambient environment that is, it depends on the cooperative or competitive behavior of the unlicensed users. Different techniques can be used to obtain an optimal solution. For example, optimization theory can be applied when the system can be modeled as a single entity with a single objective. In contrast, game theoretical models can be used when the system is composed of multiple entities each with its own objective. Stochastic optimization may be applied when the states of the system are random.

The components in CR nodes are shown in Figure 2.2.

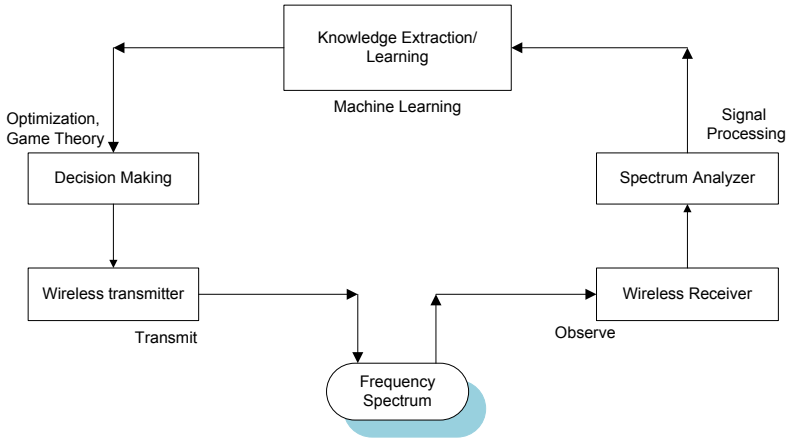


Figure 2.2. CR Cycle

2.4. Applications of CR

Some of the applications of CR can be categorized as follows [3]:

- **Emergency Networks:** Public safety and emergency networks can take advantage of the CR concepts to provide reliable and flexible wireless communication. For example, in a disaster scenario, the standard communication infrastructure may not be available, and therefore, an adaptive wireless communication system may need to be established to support disaster recovery. Such a network may use the CR concept to enable wireless transmission and reception over a broad range of the radio spectrum.
- **Military Networks:** With CR, the wireless communication parameters can be dynamically adapted based on the time and location as well as the mission of the the soldiers. For example, if some frequencies are jammed or noisy, the CR transceiver can search for and access alternative frequency bands for communication. Also, location-aware CR can control the transmitted waveform in a particular region to avoid interference to the high priority military communication systems.
- **Next Generation Wireless Networks:** CR is expected to be a key technology for next generation heterogeneous wireless networks. CR will provide intelligence to both the user-side and provider-side equipments to manage the air interface and network efficiently. At the user-side, a mobile device with multiple air inter-

faces (e.g. WiFi, WiMAX, cellular) can observe the status of the wireless access networks (e.g. transmission quality, throughput, delay, and congestion) and make a decision on selecting the access network to connect with. At the provider-side, radio resource from multiple networks can be optimized for the given set of mobile users and their QoS requirements. Based on the mobility and traffic pattern of the users, efficient load balancing mechanisms can be implemented at infrastructure of the service provider to distribute the traffic load among multiple available networks to reduce network congestion.

- **Coexistence of Different Wireless Networks:** New wireless technologies (e.g. IEEE 802.22-based WRANs) are being developed to reuse the radio spectrum allocated to other wireless services (e.g. TV service). CR is a solution to provide coexistence between these different technologies and wireless services. For example, IEEE 802.22-based WRAN users can opportunistically use the TV band when there is no TV user nearby or when a TV station is not broadcasting. Spectrum sensing and spectrum management will be crucial components for IEEE 802.22 standard-based WRAN technology to avoid interference to TV users and to maximize throughput for the WRAN users.
- **E-health Applications:** Various types of wireless technologies are adopted in healthcare services to improve efficiency of the patient care and healthcare management. However, using wireless communication devices in healthcare application is constrained by EMI (electromagnetic interference) and EMC(electromagnetic compatibility) requirements. Since the medical equipments and biosignal sensors are sensitive to EMI, the transmit power of the wireless devices has to be carefully controlled. Also, different biomedical devices (e.g. surgical equipment, diagnostic and monitoring devices) use RF transmission. The spectrum usage of these devices has to be carefully chosen to avoid interference with each other. In this case, CR concepts can be applied. For example, many wireless medical sensors are designed to operate in the ISM (industrial, scientific, and medical) band, which can use CR concepts to choose suitable transmission bands to avoid interference.
- **Intelligent Transportation System:** Intelligent transportation systems (ITS) will increasingly use different wireless access technologies to enhance the efficiency and safety of transportation by vehicles. Two different types of communica-

tions scenarios arise in an ITS system (vehicle-to-roadside (V2R) communication and vehicle-to-vehicle (V2V)) communication. In vehicle-to-roadside communications, information is exchanged between the roadside unit (RSU) and the onboard unit (OBU) in a vehicle. In vehicle-to-vehicle communications, a special form of ad hoc network, namely, a vehicular ad hoc network (VANET), is formed among vehicles to exchange safety-related information. High mobility of the vehicles and rapid variations in network topologies pose significant challenges to efficient V2R and V2V communications. CR concepts can be used in both OBUs and RSUs so that they can adapt their transmissions to cope with the rapid variations in the ambient radio frequency environment. With multi-radio capabilities at the OBUs, they should be able to adaptively choose the radio to communicate with the RSUs.

2.5. CR Standardization

In this section, the standardization processes for the development and implementation of CRNs are explained.

2.5.1. IEEE Standards Coordinating Committee 41

The IEEE Standards Coordinating Committee (SCC) 41 on Next Generation Radio and Spectrum Management has been established to initiate a series of related standards, namely, IEEE 1900. IEEE SCC 41 is composed of four working groups and one study group. Each of these groups is responsible for initiating standardization processes for different aspects of a CR system. The standardization procedure ensures that the standard will be applicable to a variety of products related to CR. The major components of the IEEE 1900 standards are as follows [3]:

- **IEEE 1900.1:** The major part of this standard is to identify and explain a glossary of terms and concepts related to spectrum management, SDR, adaptive radio, and other relevant technologies. Also, the standard describes the interrelation between the key terms and concepts. The IEEE 1900.1 standard is used

as a connection to other IEEE SCC 41 working groups, since all working groups will rely on the definitions provided by this standard.

- **IEEE 1900.2:** This standard relates to the recommended practice for interference and coexistence analysis. In CR, many wireless devices and services are allowed to coexist in the same location at the same time. Optimization of the operating parameters of these devices and services is a crucial issue to manage and avoid interference. The IEEE 1900.2 standard will recommend the criteria for interference analysis. Also, a framework for measuring, investigating, and analyzing the interference between wireless devices and services will be introduced. This working group aims to develop a common standard platform to resolve any conflict occurring in CR (e.g. between the devices working in the same spectrum).
- **IEEE 1900.3:** This standard relates to the recommendation of conformance evaluation of the software modules in SDR. The working group will develop and define the test methods for conformance evaluation of software components in SDR-based wireless devices. The main objective of this standard is to guarantee coexistence and compliance in the software part. This compliance is required for validation and certification of the final CR products.
- **IEEE 1900.4:** This standard relates to the coexistence support for the reconfigurable heterogeneous air interface. Heterogeneity will be a key feature in next generation wireless systems in which a mobile device will be able to use multiple wireless technologies simultaneously (e.g. reconfigurable terminal). Therefore, dynamic spectrum access (DSA) to support service selection and optimization will be a key component. The working group will define an overall system architecture as well as the major system functionalities. The definitions of the corresponding protocol will also be addressed by this working group.
- **IEEE 1900.A:** Responsibility of this study group relates to the certification of DSA based devices. The study group will emphasize the dependability and evaluation of regulatory compliance for wireless devices with DSA. Since a CR device will have more flexibility than a legacy device, the certification process becomes more challenging. New methodologies and testing procedures need to be developed to ensure that the certified device will not interfere with the transmission of a licensed device. The studies will include a hazard analysis listing the potential

causes of interference. The manufacturer will need to avoid these to ensure that the device will conform to the regulations.

There are also other IEEE projects/standards which relate to the next generation wireless systems and CR, i.e. IEEE 802.18, 19, 21, and 22. IEEE 802.18 is a radio regulatory technical advisory group responsible for participating and monitoring the evolution of the radio regulatory activities in different projects (e.g. for IEEE 802.11 WLAN, IEEE 802.15 WPAN, IEEE 802.16 WMAN, IEEE 802.20 Mobile WMAN, and IEEE 802.22 WRAN). IEEE 802.19 is a technical advisory group for coexistence. This group will address the issues of coexistence between unlicensed wireless networks based on IEEE 802 standards (e.g. IEEE 802.11 and Bluetooth). IEEE 802.21 is a new standard to support seamless mobility management (e.g. handoff) for both homogeneous and heterogeneous wireless technologies. It will be a fundamental standard for next generation wireless systems in which a mobile user can use multiple wireless technologies concurrently. IEEE 802.22 is a new wireless technology to support data communication in a large coverage area. This technology detailed in the next section, will operate on TV bands which are largely unoccupied.

2.5.2. IEEE 802.22

IEEE 802.22 for Wireless Regional Area Network (WRAN) is an emerging CR standard for spectrum access on a noninterference basis. The WRAN premise is the reuse of television bands(54-862 MHz in roughly 6 MHz bandwidth) without interfering with PUs. The IEEE standard committee and FCC are pursuing a centralized spectrum discovery (BS) approach and fixed, GPS-enabled APs, or customer premises equipment (CPE). The CPEs send remote spectrum sensing information to the BS for evaluation, control, and assignment of channels. The PHY layer uses OFDMA and may occupy multiple TV channels. The MAC layer approach is a TDMA structure using frames and superframes.

In 802.22, both BS and CPE perform periodic channel sensing. Since channel sensing can be either in-band or out-of-band, two interfaces are required at the CPE. A

directional antenna is used for communication with the BS, and an omnidirectional antenna is used for channel sensing. The BS instructs the CPE to sense TV bands, and the sensing results are sent back to the BS to construct a spectrum occupancy/availability map for each cell, which is used for spectrum management. The MAC protocol should be designed to support the required spectrum management functions including channel switching, channel suspension/resuming, and inclusion/removal of channels from a channel access list.

To detect an incumbent TV service, IEEE 802.22 supports fast and fine in-band sensing mechanisms. Fast sensing (e.g. energy detection) is performed over a small time interval to reduce the interruption to data transmission. Results of this sensing are used to analyze the occupancy of channels. If a high transmission energy is detected, fine sensing is performed in the target channel.

To protect incumbent services and achieve coexistence between incumbent users and SUs (incumbent coexistence), IEEE 802.22 employs various incumbent protection mechanisms. The IEEE 802.22 standard mandates that CPEs perform distributed spectrum sensing (DSS) under the control of the BS. In this cooperative spectrum sensing approach, each CPE executes spectrum sensing on its own and sends its local spectrum sensing report to the BS, which then makes a final spectrum sensing decision.

In IEEE 802.22, ensuring the congruous coexistence among overlapping WRAN cells (a.k.a. self-coexistence) is of paramount importance. Unlike other IEEE 802 standards, where self-coexistence is considered only after the specifications are essentially finalized, 802.22 takes a proactive approach and mandates that the MAC include self-coexistence mechanisms as part of the initial standard definition. In 802.22, the self-coexistence problem is exacerbated by the fact that a coverage range of BS may be as large as 100 km. Multiple BSs and a number of CPEs under their control may operate in large overlapping regions. Without proper mechanisms to handle self-coexistence in such a situation, the resulting self- interference may render the 802.22 systems useless. There are two main technical challenges in self-coexistence: (1) minimizing the self-interference between overlapping cells and (2) satisfying the QoS of admitted ser-

vice of the cell workloads in a DSA environment. The CMAC of 802.22 addresses self-coexistence using the inter-BS dynamic resource sharing mechanisms.

In an effort to provide subscribers with confidentiality, authentication, and data integrity, IEEE 802.22 prescribes a security sublayer that applies cryptographic transformations to MAC data units. Most of the features of the security sublayer are inherited from the security sublayer of IEEE 802.16e [4]. IEEE 802.16e is an amendment to the base standard, IEEE 802.16, and it addresses some of security flaws of the base standard by incorporating new security mechanisms. Specifically, 802.16e incorporates the privacy key management scheme, PKMv2, as part of the standard. The PKMv2 and the encapsulation protocol form the foundation of security sublayer of IEEE 802.22.

3. FOUNDATIONS OF COMMUNICATION SECURITY

In this chapter, building blocks of CRNs security such as availability, integrity and message authentication, identification and entity authentication, confidentiality, and key management are presented.

3.1. Availability

Most of the attacks like the denial of service (DoS, traditional jamming, buffer overflow on network queues are all targeted towards rendering the network unavailable either temporarily or permanently [5]. In the context of CRNs, availability refers to the ability of PUs and SUs to access the spectrum. For primary (licensed) users, availability refers to being able to transmit in the licensed band without harmful interference from the SUs. From the definition of DSA policies, spectrum availability for the PUs is guaranteed. For the secondary (unlicensed) users, availability refers to the existence of chunks of spectrum, where the SU can transmit without causing harmful interference to the PUs. Although studies have shown that large chunks of licensed spectrum are available for opportunistic use, availability of spectrum to the SUs is not guaranteed. In centralized CRNs, availability also refers to the availability of SBSs. Security mechanisms should ensure that DoS attacks against SBSs are appropriately countered.

3.2. Integrity and Message (Data Origin) Authentication

Data that is in transit in the network needs to be protected from malicious modification, insertion, deletion or replay. Integrity is an assurance that the data received is exactly as sent by an authorized entity. Integrity is extremely important in wireless networks because, unlike their wired counterparts, the wireless medium is easily accessible to intruders. It is for this reason that in wireless LANs an additional layer of security is added at the link layer, to make the wireless links as secure as the wired links. Cryptographic hash functions are employed to provide data integrity and mes-

sage authentication.Cryptographic hash functions are classified into message authenticated codes (MAC), one-way hash functions (OWHF), collision resistant hash functions (CRHF). The classifications of cryptographic hash functions is shown in Figure 3.1.

The basic idea of cryptographic hash functions is that a hash-value serves as a compact representative image (sometimes called an imprint, digital fingerprint, or message digest) of an input string, and can be used as if it were uniquely identifiable with that string. Cryptographic hash functions are used for data integrity in conjunction with digital signature schemes, where for several reasons a message is typically hashed first, and then the hash-value, as a representative of the message, is signed in place of the original message. A distinct class of cryptographic hash functions, called MACs, allows message authentication by symmetric techniques. MAC algorithms may be viewed as hash functions which take two functionally distinct inputs, a message and a secret key, and produce a fixed-size (say n-bit) output, with the design intent that it be infeasible in practice to produce the same output without knowledge of the key. MACs can be used to provide data integrity and message authentication, as well as identification in symmetric-key schemes.

The ideal cryptographic hash function has four main properties [6]:

- It should be easy to compute the hash value for any given message.
- It should be infeasible to find a message that has a given hash.
- It should be infeasible to find two different messages with the same hash.
- It should be infeasible to modify a message without changing its hash.

A cryptographic hash function must be able to withstand all known types of cryptanalytic attack. As a minimum, it must have the following properties [6]:

- *Preimage resistance:* Given a hash h it should be hard to find any message m such that $(h = hash(m))$. This concept is related to that of one way function. Functions that lack this property are vulnerable to preimage attacks.
- *Second preimage resistance:* Given an input m_1, it should be hard to find another

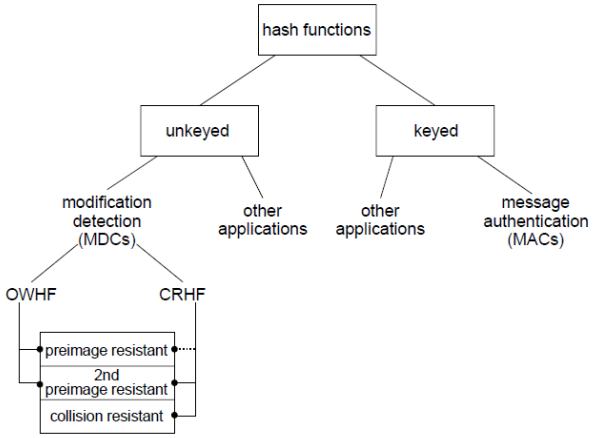


Figure 3.1. Classification of Hash Functions

input, m_2 (not equal to m_1) such that hash $(m_1) = hash(m_2)$. This property is sometimes referred to as weak collision resistance. Functions that lack this property are vulnerable to second preimage attacks.

- *Collision resistance:* It should be hard to find two different messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. Such a pair is called a (cryptographic) hash collision, and this property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as what is required for preimage-resistance, otherwise collisions may be found by a birthday attack.

Message authentication is a term used analogously with data origin authentication. It provides data origin authentication with respect to the original message source. Methods for providing data origin authentication include the following: (1)message authentication codes (MACs), (2) digital signature schemes, (3) appending (prior to encryption) a secret authenticator value to encrypted text.

Message authentication mechanisms based on a shared secret like MACs, do not allow a distinction to be made between the parties sharing the key, and thus do not provide non-repudiation of data origin. Non-repudiation can be provided by using a digital signature as a method of message authentication.

3.3. Identification and Entity Authentication

Authentication is an assurance that the communicating entity is the one that it claims to be. The primary objective of an authentication scheme is to prevent unauthorized users from gaining access to protected systems. It is a necessary procedure for verifying both an entity's identity and authority. Identification and entity authentication techniques may be divided into three main categories, depending on which of the following the security is based [6]:

- *Something known:* Include standard passwords (sometimes used to derive a symmetric key), Personal Identification Numbers (PINs), and the secret or private keys whose knowledge is demonstrated in challenge-response protocols.
- *Something possessed:* This is typically a physical accessory, resembling a passport in function. Examples include magnetic-striped cards, chipcards (plastic cards the size of credit cards, containing an embedded microprocessor or integrated circuit; also called smart cards or IC cards), and hand-held customized calculators (password generators) which provide time-variant passwords.
- *Something inherent:* This category includes methods which make use of human physical characteristics and involuntary actions (biometrics), such as handwritten signatures, fingerprints, voice, retinal patterns, hand geometries, and dynamic keyboarding characteristics.

Since only challenge-response protocols will be considered as a solution to perform entity authentication in CRs, the other methods will not be detailed in this section.

Challenge-response protocols can be held by using symmetric or public key technique. Challenge-response mechanisms based on symmetric-key techniques require the claimant and the verifier to share a symmetric key. For closed systems with a small number of users, each pair of users may share a key a priori; in larger systems employing symmetric-key techniques, identification protocols often involve the use of a trusted on-line server with which each party shares a key. Public-key techniques may be used for challenge-response based identification, with a claimant demonstrating knowledge

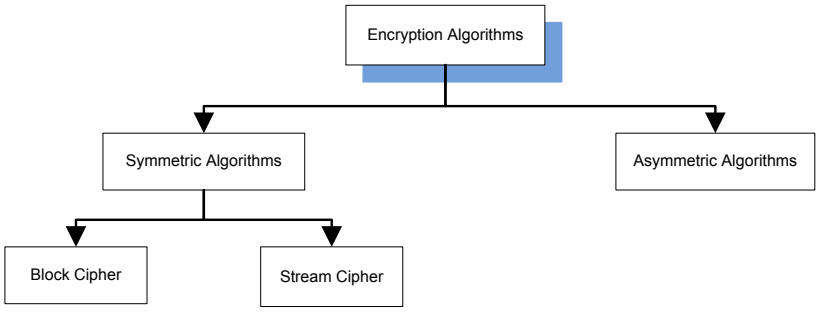


Figure 3.2. Classification of Encryption Algorithms

of its private key in one of two ways:(1) the claimant decrypts a challenge encrypted under its public key, or (2) the claimant digitally signs a challenge.

3.4. Confidentiality

Confidentiality is closely linked with integrity. While integrity assures that data is not maliciously modified in transit, confidentiality assures that the data is transformed in such a way that it is unintelligible to an unauthorized (possibly malicious) entity. This is achieved by employing ciphers and encrypting the data to be transmitted with a secret key which is shared only with the recipients. The encrypted data is then transmitted and only the recipients with a valid key can decrypt and read the data. Confidentiality can be achieved by either symmetric or asymmetric (Public Key) encryption algorithms. Symmetric algorithms divide into two groups: (1) block ciphers, and (stream ciphers). Block ciphers operate with a fixed transformation on large blocks of plaintext data; stream ciphers operate with a time-varying transformation on individual plaintext digits.

A block cipher is a function which maps n bit plaintext blocks to n bit ciphertext blocks; n is called the blocklength. It may be viewed as a simple substitution cipher with large character size. The function is parameterized by a k bit key K taking values from key space of all k bit vectors V_k. It is generally assumed that the key is chosen at random. Use of plaintext and ciphertext blocks of equal size avoids data expansion.

The public key encryption algorithms are used to create a mathematically related

key pair: a private key and public key. The private key is kept secret, whilst the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The keys are related mathematically, but the private key cannot be feasibly derived from the public key.

3.5. Group Key Management Techniques

In the literature, there exists several different approaches to group key management. We can divide them into three main classes [7]:

- *Centralized group key management:* A single entity is employed for controlling the whole group, hence a group key management protocol seeks to minimize storage requirements, computational power on both client and server sides, and bandwidth utilization.
- *Decentralized group key management:* The management of a large group is divided among subgroup managers, trying to minimize the problem of concentrating the work in a single place.
- *Distributed key management:* There is no explicit Key Distribution Center (KDC), and the members themselves do the key generation. All members can perform access control and the generation of the key can be either contributory, meaning that all members contribute some information to generate the group key, or done by one of the members.

We will briefly detail different approaches to key management. A simple scheme for rekeying a group with n members has the key distribution center (KDC) assigning a secret key to each member of the group. In order to distribute the group key, the KDC encrypts it with each member's secret key. In the Group Key Management Protocol (GKMP), when the first member joins group, it creates a Group Key Packet (GKP) that contains a group traffic encryption key (GTEK) and a group key encryption key (GKEK). The first member shares GKP with KDC. When a new member wants to join the group, the KDC sends it a copy of the GKP. When a rekey is needed, the GC generates a new GKP and encrypts it with the current GKEK. As all members know

the GKEK, there is no solution for keeping the forward and backward secrecy when a member leaves the group.

In Logical Key Hierarchy (LKH) approach, a KDC maintains a tree of keys. The nodes of the tree hold KEK. The leaves of the tree correspond to group members and each leaf holds a KEK associated with that one member. Each member receives and maintains a copy of the KEK associated with its leaf and the KEKs corresponding to each node in the path from its parent leaf to the root. The key held by the root of the tree is the group key. When a member leaves the group, its parent node's KEK and all KEKs held by nodes in the path to the root are compromised and should be updated (forward secrecy). One-way function tree (OFT), the KEKs held by a node's children are blinded using a one-way function and then mixed together using a mixing function. The result of this mixing function is the KEK held by the node. There is also another method called One-way function chain tree (OFCT) which uses pseudo random functions(PRFs) instead of one-way function to obtain KEKs. The other parts are the same with OFT. Efficient Large-group Key (ELK) protocol. The ELK protocol uses a hierarchical tree and is very similar to the OFT in the sense that a parent node key is generated from its children keys. ELK uses (PRFs) to build and manipulate the keys in the hierarchical tree. ELK employs a timely rekey, which means that the key tree is completely updated in each time interval. Clustering, is a key management method by dividing the group with n member into clusters of size m and assigning a cluster to a unique leaf node. When a member leaves, the cluster holding it receives a new cluster KEK. The new KEK is encrypted with the individual KEKs of all remaining members. A flat table (FT) has one entry for the Traffic Encryption Key (TEK) and $2w$ more entries for KEKs, where w is the number of bits in the member id. There are two keys available for each bit in the member id, one associated with each possible value of the bit. Group Diffie Hellman key exchange is an extension for the DH key agreement protocol that supports group operations. The DH protocol is used for two parties to agree on a common key. In this protocol, instead of two entities, the group may have n members. The group agrees on a pair of primes (q and r) and starts calculating in a distributive fashion the intermediate values.

4. COGNITIVE RADIO NETWORKS SECURITY ISSUES

In this chapter, security related issues, security vulnerabilities, threat analysis, and countermeasures are detailed. Then, IEEE 802.22 security sublayer will be given.

4.1. CRNs Security Related Works in Literature

While a traditional radio allows minimal user interaction and has unalterable receiver transmitter operations, the CRs have advanced functionalities of remote reconfigurability, spectrum sensing, spectrum decision and primary user detection. These new functionalities open new denial of service vulnerabilities. Therefore the security solutions given in the field of CRNs are mainly based on the new denial of service vulnerabilities. In the rest of this section, all these given solutions are detailed.

In [8], authors present the potential security attacks to CRN and give some solutions to avoid these DoS attacks like traditional jamming, policy failure and primary user emulation (PUE) attack. The attacks they mention in this work are especially DoS attacks. They also give the techniques which can be used as a solution to these security vulnerabilities. The basic cryptography concepts like confidentiality, privacy, integrity, authentication, authorization and non-repudiation are cryptographic techniques. These techniques as they relate to CR user's traffic are not directly be considered. They mention that these areas would be useful in preventing DoS attacks to the extent that they protect the signaling and communication between networked CR elements. Another concept given in this work is low probability of which is concerned with masking the physical signal so that its presence cannot be detected, low-duty cycle communication transmitting from multiple location.

In the last section of [8] authors present the remedies for DoS attack. In compromised cooperative CR scenario, a compromised node can produce false sensor information, false geo-location information and invalid policies. They can also inhibit the forwarding and dissemination of valid information among CR nodes. Authors state

that authentication and integrity checks can mitigate the corruption of one user's data by other. However, a compromised user can still originate corrupted data. One of the possibilities authors state to avoid this problem is to have "black-box" sensors that report measurements with their own authentication and integrity check. A public key scheme could allow any user to recover the measurements from a known class of sensors and prevent any intermediaries including a compromised CR associated with the sensor from corrupting data. If time stamps are included the replay attacks can be avoided.

For common control channel attacks, which is a target for DOS attacks since successful jamming of this one channel may prevent or hinder communication across a large frequency range; authors state a solution by using robust spread spectrum coding. For spectrum occupancy failures where the attacker spoofs or masks a licensed transmitter, authors state that in cooperative networks, the attacker would need to appear as a LU to multiple CR that may be widely distributed which reduces the effectiveness of the attacks. Policy failures can be prevented by using authentication and integrity certificates traceable to a trusted authority associated with each policy.

In [9], authors introduce a class of attacks specific to CRNs on PHY layer issues. Authors claim that sensory input statistics can be altered, faulty sensory statistics can lead to belief manipulation, manipulated individual statistics and beliefs may be distributed through a CRN and behavior algorithms based on manipulated statistics and beliefs can result in suboptimal performance or malicious behavior. Then authors give the precautions to mitigate the effectiveness of these attacks. The first precaution is to assume sensory input statistics are noisy and subject to manipulation. The other one is to be programmed with some amount of common sense to attempt to validate learned beliefs. The third one is to compare and validate learned beliefs with other devices on the network. The fourth one is to expire learned beliefs to prevent long-term effects of attacker and the last precaution is to attempt and perform learning in known-good environments.

Authors classify the CR attacks as dynamic spectrum access, objective function and malicious behavior attacks. The first attack can be effective in DSA environment

is PUE attack. All an attacker need do is to create a waveform sufficiently similar to that of the PU to trigger a false positive in the spectrum sensing algorithm. The secondary devices within range will believe a PU is active, and will cause the system to vacate the channel. This gives the adversary unrivaled access to the frequency band. Fortunately the effects of this attack are transient, as it is only a sensory-manipulation attack. Once the attacker vacates the frequency, the SUs notice the spectrum being once again idle, and can resume using it.

Since Objective function attacks mentioned in this paper apply to learning engines, they are called as belief manipulation attacks. Some possible input parameters which are used to reach the multi-goal objective functions, could be center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size. The radio might then have three goals: low-power, high-rate, and secure communication. Depending on the application, each of these goals has a different weight. For example, if using the system for instant messages or email, low-power and secure would have higher weights than high-rate. For voice or video applications, high-rate and secure would have higher weights than secure. There are a few different types of attacks possible on a system like this. When radios are in a learning phase, they try different combinations of input parameters, measure the observed statistics such as bit error rate, and then evaluate the objective functions to see which inputs give the best results for their application. It is very important to note that this type of attack only works when the radio is performing online learning, that is the radio is performing some sort of online optimization of the search space. Radios that perform offline learning observe the environment once, and then perform an offline search to find the optimal configuration; such radios assume independence of their observations and configuration, and consequently are immune to these attacks.

The last type of attacks mentioned in this paper is malicious behavior attack which is an extension of objective function attacks. The desired result is a SU will only communicate when the PU is idle. However, if an adversary uses a jamming waveform that cannot be detected by the SU's sensing algorithms, he can artificially decrease throughput when the PU is idle. As a result, the CR will learn that the only time it

can achieve useful communications is when the PU is active. This effectively turns the CR into a jammer.

[10] describes the key challenges in providing security in cognitive networks, discusses the current security posture of the emerging IEEE 802.22 cognitive radio standard, and identifies potential vulnerabilities along with potential mitigation approaches. In this paper, the fundamental differences between cognitive and non-cognitive wireless networks are given and the security issues for cognitive radios over non-cognitive ones are defined. A security threat classification is constructed by considering the motivations of the attackers.

In [10] the key characteristics that are possessed by CR networks to mitigate malicious manipulation of CRs and CR networks into forced behaviors are also given. These characteristics are as follows: the ability to authenticate the local observations that are used to form perceived environments, the ability to strongly secure collaboration exchanges between CR elements, the ability to authenticate the validity of observations exchanged between CR elements, the ability to perform self analysis of behavior. The author claims that all of these security features relate to the need for the CR to exhibit good judgment and at this point, it is important to recognize that the CR paradigm imposes human characteristics onto the radio device. As such, it may be beneficial for the designers of CR network security models to examine (at least in part) social and science and human behavior, and consider the characteristics that protect humans from manipulation, primarily relationships, judgment, and wisdom.

[10] has attempted to illustrate the multi-discipline nature of developing CR security models, and has attempted to draw analogies and comparisons to applicable research communities. This paper has attempted to show that the traits of a CR (awareness, adaptation, etc.) are human traits that we as designers are attempting to impose on machines. Finally they claims that regardless of the actual approaches and techniques employed, it is important to realize the key differences in developing secure CR networks, and that it requires a change in mindset and an evolution in how the problem of wireless network security is approached.

In [11],authors describe how adversaries can exploit or undermine incumbent and self coexistence mechanisms to degrade the performance of 802.22 WRANs and increase the likelihood of those networks interfering with incumbent networks. The standard includes a security sublayer to provide subscribers with privacy, authentication,and confidentiality. Their investigation, however, revealed that the security sublayer falls short of addressing all of the key security threats. They also discuss countermeasures that may be able to address those threats.

Authors state that the security vulnerabilities of IEEE 802.22 are partly due to the fact that the designers of the standard attempted to reuse the security sublayer designed for IEEE 802.16 networks. IEEE 802.22 networks are composed of cognitive radio nodes, and thus face unique security threats not faced by conventional networks. They claim that one of the most significant security oversights in IEEE 802.22 is the lack of protection provided to inter-cell beacons. Inter-cell beacons play a vital role in incumbent and self coexistence mechanism. Two types of inter-cell beacons are defined in IEEE 802.22: (1) BS beacons which are used to provide information about the BS's traffic schedule, the current operation channel of the cell, etc., and (2) CPE beacons which are used to provide information about a CPE's current cell of attachment as well as information on the traffic flows between the CPE and its BS. All inter-cell control messages are vulnerable to unauthorized modification, forgery, or replay. Since, the IEEE 802.22's security sublayer does not take into account the important difference between IEEE 802.16e and IEEE 802.22, the incumbent and self-coexistence mechanisms, IEEE 802.22's security sublayer fails to protect the inter-cell beacons used to carry out coexistence mechanisms.

In [12], the differences between traditional radios and CR are explained and an analysis of how vulnerable are victim CRs to potential DoS attacks is presented along different axis, namely the network architecture employed, the spectrum access technique used and the spectrum awareness model(which a CR may become aware of spectrum usage and availability in its vicinity through different models like Geo-location/database approach, the beacon/control signal approach and the detection/sensing approach). In the threat model explained in this paper, they assume

that an attacker can create different types of signals including false signals that can be perceived as signal of PUs, message that can be received by the victim CRs and jamming signals that can prevent messages from being received by a receiver. The non-radio-based attacks like a node of CR could be compromised, are not part of the threat model in this paper.

In the terms of the potential DoS vulnerabilities of CR networks, authors categorize the attacks into denial and induce attacks. The denial attacks can prevent communication through placing the victim CR in some states. The states are as follows: All available spectrum appears to be occupied by licensed transmitters, no policy is available that enables it to transmit, location information is unavailable or has too low accuracy, the sensor is unavailable or has incorrect measurements, the cognitive engine cannot connect to radio and the operating system cannot connect to the cognitive engine. The induce attacks is when the CR is stimulated to cause interference with a licensed transmitter. While the result is not an immediate DoS, it may cause permission policies to be tightened or eliminated potentially denying service over the long term. A CR may cause interference with a licensed transmitter under one or more of the following conditions: The licensed spectrum appears unoccupied, the policy is incorrect, the location is incorrect and the sensor provides incorrect measurements. After construction the threat model, authors present the potential failures like spectrum occupancy failures, policy failures, location failures, sensor failures, transmitter/receiver failures, operating system disconnect, compromised cooperative CR and common control channel attacks.

In the rest of the paper they propose a multi-dimensional analysis in terms of security in CRNs. Authors present a qualitative analysis of how vulnerable are victim CRs to a potential DoS attack depending on these three dimensions; the network architecture employed, the spectrum access technique used and the spectrum awareness model.

In literature there are lots of works based on the PUE attacks. These works based on some mathematical formulations and localization of the PU transmitter. These

works are not directly in the scope of our thesis. However we will also roughly mention them. In [13], authors study DoS attack on SUs in a CR network by PUE. Authors propose an analytical approach based on Fenton's approximation and Markov inequality and obtain a lower bound on the probability of a successful PUEA on a SU by a set of co-operating malicious users. Authors consider a fading wireless environment and discuss the various parameters that can affect the feasibility of a PUEA and show that the probability of a successful PUEA increases with the distance between the primary transmitter and SUs. In [14] a solution to the PUE attack base on transmitter localization is given. In this attack, an adversary's CR transmits signals whose characteristics emulate those of incumbent signals. The highly flexible, software-based air interface of CRs makes such attacks possible. Authors show that a PUE attack can severely interfere with the spectrum sensing process and significantly reduce the channel resources available to legitimate unlicensed users. To counter this threat, authors propose a transmitter verification scheme, called LocDef (localization-based defense), which verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. To estimate the location of the signal transmitter, LocDef employs a non-interactive localization scheme. The security analysis and simulation results suggest that LocDef is effective in identifying PUE attacks under certain conditions. In [15], authors present an analytical model as well as a practical mechanism to detect DoS attacks on SUs in DSA networks. Authors claim that there are no studies available that detect PUE attack using analytical models. Authors present an analysis using Fenton's approximation and Wald's sequential probability ratio test (WSPRT) to detect PUE attack. Simulation results demonstrate that it is possible to keep the probability of missing the primary below a desired threshold while at the same time keeping the probability of successful PUE attack low.

Since the PU detection process is the backbone of the CRs, securing this process can be helpful to be able to make spectrum decision correctly. There are many works in the literature which secure PU decision by using mathematical approximations and transmitter localizations. However in this thesis our main concern is to secure CRs by using cryptographic protocols and algorithms. In [16], authors propose a solution which secures the primary user detection process by using digital signatures.

In this paper, authors consider a DoS attack on centralized DSA networks where a malicious SU masquerades as a PU and effectively shuts off access to all other SUs. This problem is unique to CR due to the distinction between primary and secondary users. They propose a public key cryptography based PU identification mechanism that prevents malicious SUs from masquerading as PUs. Authors show that the proposed identification mechanism and the associated key management are computationally light weight and also discuss some advantages and limitations of the proposed identification mechanism. Since the public key cryptography is used to secure the PU detection process, we will give the main properties of public key cryptography. Public key ciphers [17] rely on one key for encryption and a different but related key for decryption. The key that is revealed is called the public key (denoted by P) and the key that is kept secret is called the private key (denoted by S). The encryption and decryption algorithms of public key ciphers satisfy the following properties:

$$X = D_P(E_S(X))$$
$$X = D_S(E_P(X))$$

Here, X is a message consisting of letters from a finite alphabet. E and D are encryption and decryption algorithms respectively. Therefore, the encryption operation with one key is inverted by the decryption operation with the other key. Some of the well known public key ciphers are RSA, ElGamal, Rabin and Elliptic curve cryptosystems.

Public key ciphers can be used to provide confidentiality, as digital signature and to exchange secret keys. In this paper, authors use public key ciphers as digital signatures. To use a public key cipher as a digital signature, the transmitter signs the message using its private key and the receiver verifies the signature using the transmitter's public key. Since only the transmitter possesses its private key, it is computationally infeasible for an imposter to sign the transmitter's message. To maintain public keys used by all PUs, a certification authority is needed. Authors assume that certification authority is connected to the PUs and SBSs through a wired backbone.

The proposed security protocol is as follows. Each PU generates a pair of public and private keys using a key generation algorithm. The public keys are securely registered with the corresponding certification authority. The data to be transmitted by the PU at its link layer is called the message service data unit (MSDU). MSDUs are often broken down into many message protocol data units (MPDUs), where each MPDU consists of MAC (Medium Access Control) header and a data payload. The MAC header consists of the primary user identity (P_{ID}) and the time stamp (T_S). The primary user computes a digital signature, S, by encrypting its identity and the time stamp with its private key.

$$M = E_S(P_{ID}||T_S)$$

The signature is appended to the MPDU to obtain a signed MPDU. The signed MPDUs are then transmitted over the wireless medium.

$$MPDU_{signed} = MPDU||M$$

The SUs look for the presence of a PU's transmission during their fine sensing operation. If a transmission is detected, then the SUs decode the signal to obtain the corresponding MPDU's. The MPDU's are then scanned for the presence of signatures. If the signatures are found, they are detached from the MPDUs and stored by the SUs. These stored signatures are periodically transmitted to the SBS through an established control channel. The SBS securely obtains the public keys and the identities of the PUs within its vicinity from the CA. Whenever, the SUs detect transmissions with signatures during their sensing periods, the corresponding signatures are transmitted to the SBS. The SBSs maintain only one copy of duplicate signatures. The set of unique signatures are then sequentially decrypted with the public key, P_i, of each PU, i, within its vicinity.

$$PID_i||T_S = D_{P_i}(M)$$

If the decrypted PU's identity matches with one of the PU identities in the list obtained from the CA, the BS checks for the validity of the time stamp. To do this, the BS selects a network delay parameter, d, which defines the window of acceptable time stamps. If the absolute difference between the BS's current time and the decrypted time stamp is d, the time stamp is accepted as a valid time stamp and the SBS is assured of the presence of a licensed PU. The value of d should be chosen such that the signature does not expire before it is decrypted by the SBS.

In the proposed security protocol, the SBS make all signature verification process and for each verification process BS contact with the certification authority in order to get the primary's public key. In the performance point of view it is not an appropriate way to make an entity doing all verifications. In the architecture defined in [1], there is also a satellite which is directly connected to all BS. To improve the performance satellite can give a ticket which is encrypted with its private key and a time interval to define the validity of the ticket. Primary users only append these tickets to their data and when the SUs collect these tickets, they eliminate the same tickets and send the unique tickets to BSs. Since the SBSs have already known the public key of the satellite, they can easily validate the signatures in the tickets and check the validity of the tickets without connecting the certification authority. However this proposed security protocol makes some modifications in the PUs' structures and to make CRNs secure, any modification in PUs is not a proper way. Since the two main constraints in the design of DSA networks is to make sure that this opportunistic access is done without any disruption of service to the primary users and without any modifications to the primaries themselves, we decided to secure the CRNs without any modification in PUs' structures.

Since by using non-cryptographic methods explained in [13–15], the PU detection process can be made secure, we will focus on other process especially spectrum decision and we assume the primary user detection process will be secure by using these non-cryptographic methods.

In [18], a secure spectrum decision process is defined by considering spectrum

decision protocols in clustered infrastructure-based DSA networks. The spectrum decision in each cluster is coordinated by some central authority and propose an efficient and provably secure protocol that can be used to protect the spectrum decision process against a malicious adversary.

In this work, a clustered infrastructure-based DSA network is considered. Each cluster consists of a cluster head and mobile nodes that are within the range of the cluster head. The cluster head has the role of a CA that exerts some control over the other nodes in the cluster. A BS and an access point are examples of such authorities. Authors assume that there is an infrastructure that connects different cluster heads, and this infrastructure is used to establish communication between any two mobile nodes in the network. The channel availability is decided by the cluster head based on the sensing data provided by the nodes in the cluster. The cluster nodes sense the spectrum periodically, and send measurement data to the cluster head. The cluster head uses the received information to determine which channels are not used by the PUs, and then it notifies the cluster nodes about the communication channels they should use for uplink and downlink communication.

In initialization period, cluster heads and nodes are all given a public and private key pairs generated by a CA. Moreover, they all generate their key chain as shown in Figure 4.1 which are used as key derivation and commitment parameter for keys of message authentication code (MAC) algorithms.

Join protocol provides the data origin authentication service by using digital signature. To join the spectrum sensing period, CR node A sends a digitally signed join message to the cluster head. This message contains the current interval (t_s), identity of the cluster head (ID_H), identity of the node A (ID_A), the final value of key chain (K_0) and an additional data (D). Cluster head sends back a digitally signed message containing the current interval (t_s), its identity (ID_H), the key derivation used in the previous interval (t_{s-1}) and some information M.

Sending spectrum sensing data provides data origin authentication by using the

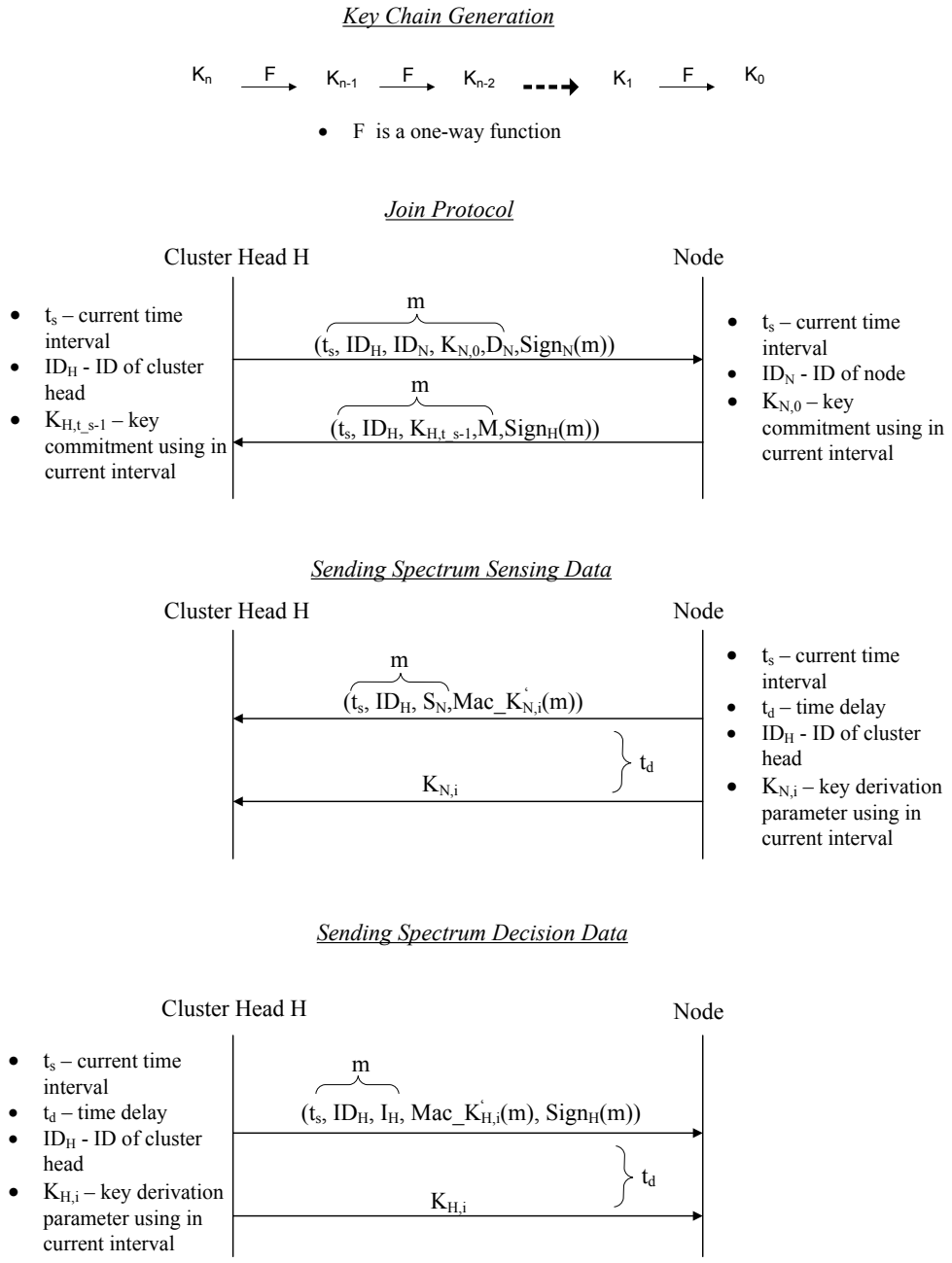


Figure 4.1. Steps of Security Protocol

MAC algorithm. Node A constructs a message that contains current interval t_i, ID_H, ID_A and sensing information (S). Then node A calculates MAC of the message by using key K_i' which is derived from K_i. The derivation function is performed by flipping the value of the last bit of the corresponding key K_i. After some time delay, node A also sends K_i to the cluster head.

By the time the cluster head receives the K_i, by using the previous cycle key derivation parameter K_{i-1}, it validates if F (K_{i-1}) is equal to K_i or not (commitment). Then it derives K_i' by flipping the value of the last bit of the corresponding key K_i. After the key derivation, the cluster head calculates the MAC of the message.

Once the cluster head decides which channels are available, it constructs a message which contains current interval, ID_H and spectrum decision I. Then the cluster head broadcasts the message by appending the MAC of the message and its digital signature. After some time delay it reveals the key K_s which will be used in the key derivation of the MAC algorithm. The new nodes which have not performed the join protocol verify the authenticity of the message using the digital signature.

While the integrity and source authentication of the messages are achieved by the proposed protocol in [18], confidentiality is not provided. However, eavesdropping of the messages in the spectrum analysis and decision protocols is an efficient way of performing some denial of service attacks like traditional jamming.

For an effective jamming scenario in CRNs, a traditional jammer needs to have certain advanced jamming techniques. Since CRs have the ability to operate in many different bands for communicating in the presence of LUs; the jammer has to jam many different communication bands simultaneously or have a reliable technique to detect CR as it switches between many bands. This is an advantage of the CRNs over traditional jamming attacks only if there is a strong confidentiality mechanism in the spectrum sensing and decision protocol [12]. Otherwise, as it is an issue in the proposed protocol, an attacker can easily capture the spectrum decision message which is broadcast by the cluster head. Next, it can obtain all the available communication frequencies in

order to jam the communication of SUs or to perform a primary user emulation attack. Therefore to achieve a secure and robust spectrum sensing and decision procedure, confidentiality, integrity, entity and data origin authentication should be all considered as the building blocks of the security structure [6].

After sending spectrum sensing or spectrum decision messages, senders reveal the key commitment and derivation parameters without any security services whatsoever. Therefore an attacker can easily change these parameters. Then the messages which are prepared by using these modified data are rejected by the receiver. If this attack is applied in spectrum sensing messages, then the cluster head performs a spectrum decision without a strong contribution of all nodes in its coverage area. Authors also give a solution for byzantine faults by performing a majority voting and this scheme is resistant up to $\lceil N_m/2 \rceil$ -1 byzantine faulty nodes where N_m stands for the number of nodes in the cluster. However the modified key commitments could also be used to attack the proposed solution for the byzantine faults. The byzantine nodes can change commitments of the other healthy nodes, and then cluster head can perform the spectrum decisions by using only the spectrum analysis messages of byzantine nodes which cause a spectrum decision failure.

In [18] freshness of the messages are not properly handled. Authors state that since a node sends only one message per interval, the pair (ID_{BS}, t) can be used as a nonce for message of the node. Since the cluster head can perform more than one messages in a given interval, triple (Message Type Field, ID_{BS}, t) can be used as a nonce. In join operation, the message sent by the cluster head is not an identical response for the join attempt. The cluster head provides the same message for every join attempt in a given interval. Since the message types are the same, freshness could not be performed by the triple (Message Type Field, ID_{BS}, t) for these messages. A cryptographic nonce should be seriously provided to propose a security structure which has resistance for replay attacks.

Join operation defined in [18], only provides message authentication by using digital signature. Since the proposed join protocol does not provide entity authentication

and cryptographic nonce, an adversary can easily capture the join message sent by a node to a cluster head. Then, it can replay this message to another cluster head during the same time interval. This replay attack leads to a situation in which an adversary joins the spectrum sensing period by impersonating a legal SU and send faulty spectrum analysis messages to cluster head.

In [18], authors claim that the main advantage of the proposed protocol is that since the key derived from the commitment is used to construct only one MAC tag which is sent before revealing the commitment, it does not require providing secrecy of the commitment. However, one-time usage limitation of the commitments affects the spectrum decision by prohibiting retransmission of any erroneous spectrum analysis messages.

The length of the generated key chain is an important trade-off parameter for the efficiency of the proposed protocol. While small key chains facilitate rapid regeneration of short real-time delays; long ones lead to larger initialization delays and memory requirements.

Nodes and cluster heads have to wait for some time to reveal the key commitments, this causes some real-time delays. Another efficiency problem occurs when nodes and cluster heads check the validity of the authentication tag. They need to verify the correctness of the key commitment and then generate the message authentication key by applying a function on this commitment before checking the authentication tag. These operations also cause real-time delays in spectrum sensing protocol.

4.2. Security Vulnerabilities, Threat Analysis, and Countermeasures

The basic purpose of CRN is to facilitate the spectrum access in an agile way so that spectrum holes can be utilized by SU whenever a PU does not use it. Determining the spectrum holes and identification of PUs are achieved by sensing all available spectrum bands. Spectrum sensing and decision protocols must ensure harmless inference with PU signals. Additionally, these protocols must not require any modification in the

primary network. Hence, all SUs must adhere to the rules specified by the cognitive protocols. Securing spectrum sensing and decision protocol could help to provide these two main constraints of CRNs. In the literature, there is a plethora of research on spectrum sensing and decision protocols most of which do not consider the security issues and assume that there is no corrupted insider or malicious adversary. However, there is also a plethora of research showing how easily an attacker can cause a denial of service in CRNs which do not provide security services [8, 12, 19]. This shows that to assure the persistence of PUs' service, it is important to introduce cryptographic protection for spectrum sensing and decision protocols, which therefore should be one of the main design characteristics for CRNs.

Before constructing a security structure for CRNs, security vulnerabilities, threat analysis, and their countermeasures are needed to be discussed. The threat analysis is inspired from a methodology described in [20] and is summarized in Table 4.1 and Table 4.2. Threats are evaluated by using the occurrence likelihood which is assessed by the motivation of the attacker or technical difficulties, and impact which is calculated by the level of the dramatic consequences of an attack related to threats. The threats related to the spectrum analysis and decision protocol and their countermeasures are explained in this section [21]. Furthermore, threat analysis is presented in Table 4.3 and Table 4.4.

4.2.1. Primary User Emulation Attack

In primary user emulation attacks, attacker creates a waveform similar to that of the PU to trigger a false positive in the spectrum sensing algorithm. SU which senses the PU signal can correctly identify the PU signal by only applying a cryptographic authentication protocol between PUs and SUs. Since one of the main constraints in the design of CRs is to assure that this opportunistic access is done without any modifications to the PUs, mitigating PU emulation attack should be achieved by using non-cryptographic methods, such as [13–15].

Table 4.1. Risk Analysis

		Impact		
		Low	Medium	High
Likelihood	Unlikely	Minor	Minor	Major
	Possible	Minor	Major	Critical
	Likely	Major	Critical	Critical

Table 4.2. Risk Countermeasures

Risk	**Countermeasure**
Minor	No primary need for countermeasures
Major	Threat cannot be ignored
Critical	Should be minimized with highest priority

4.2.2. Eavesdropping and Traditional Jamming Attack

Traditional jamming attack is a simple denial of service attack which is performed by transmitting a continuous high-power signal to prevent the reception of the original signal. There are robust transmission security techniques like spread spectrum and frequency hopping to mitigate this attack. Since the available signal bandwidth for CRNs is mostly limited and not predictable, it is hard to implement a robust transmission security technique on these networks.

CRNs are designed to operate in a range of frequency bands to be able to communicate in the presence of PUs. Therefore, a traditional jammer needs to simultaneously jam a set of bands or have the ability of detecting the CR as it switches between a set of bands. This advantage of CRNs against traditional jamming attack, only holds when the spectrum analysis and decision procedure are sufficiently secured to provide the confidentiality of available band list for SU communications. Otherwise, an attacker can easily eavesdrop the available band list and only jam these bands to prevent the communication of SUs.

4.2.3. Faulty Data Injection

Malicious adversary or insider node may send false spectrum sensing data to the BS, causing faulty spectrum sensing decision. Since CRs have ability to learn from the past events, this type of attack also has long-term effects on CRNs and can be called as *belief manipulation attacks* [9]. Furthermore, a malicious adversary may act as a BS and broadcast a faulty spectrum decision message, thereby resulting in the blockage of SU communications. In case of malicious adversaries, cryptographic solutions like entity and message authentication can easily prevent this type of attacks. For an insider attacker (byzantine attacker), cryptographic protocols may not provide a solution without robust data fusion which is used to combine spectrum analysis data from multiple CR nodes and gather that information in order to achieve efficient inferences. Therefore, mandatory cryptographic services to prevent faulty data injection by a malicious adversary should be provided and a robust data fusion technique against byzantine attack [22] should be addressed.

4.2.4. Intentional / Non-intentional Modifications

In this thesis, intentional modification means that an attacker modifies a transmitted data in a way that the modified data is also a meaningful data which is intended by the attacker. On the other hand non-intentional modification is a random change in data which can be caused either by jamming or interference of medium. Integrity which is an assurance that the data received is exactly as sent by an authorized entity, is a very important security service in wireless networks. This is due to the reason that, unlike their wired counterparts, the wireless medium is easily accessible to adversaries. Since the modified spectrum sensing and decision messages cause faulty available band list, spectrum sensing and decision data needs to be protected during the transmission from intentional or non-intentional modifications by a malicious adversary/noisy channel.

Table 4.3. Spectrum Sensing and Decision Security Risk Analysis

Threats	**Likelihood**	**Impact**	**Risk**
Primary User Emulation	Possible	High	Critical
Traditional Jamming	Likely	High	Critical
Faulty Data Injection	Likely	High	Critical
Intentional Data Modification	Unlikely	High	Major
Non-intentional Data Modification	Likely	High	Critical
Message Replay	Likely	High	Critical
Eavesdropping	Likely	High	Critical

4.2.5. Replay Attack

Replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated. If an attacker captures a spectrum sensing data and replays it in another spectrum sensing period, it may result in faulty spectrum decision by the BS. If an adversary sends the previously captured spectrum decision data and replays it to the nodes in its range, then it may also result in faulty spectrum decision.

Replay attacks can be prevented by inserting a cryptographic nonce (number used once) in messages. Nonce is often a random or pseudo-random number issued in a protocol to ensure that old communications cannot be reused to perform replay attacks. To ensure that a nonce is used only once, it should be time-variant (timestamp) or generated with enough random bits to ensure a probabilistically insignificant chance of repeating a previously generated value [6].

4.3. IEEE 802.22 Security Sublayer

Since most of the features of IEEE 802.22 security sublayer is inherited from the security sublayer of IEEE 802.16e [11], and the standardization of IEEE 802.22 is still under development, we will assume that the security sublayer of IEEE 802.22 is identical to that of IEEE 802.16e [4].

Table 4.4. Spectrum Sensing and Decision Countermeasures

	Countermeasure	
Threats	**Cryptographic Service**	**Non-Cryptographic Service**
Primary User Emulation	Can be provided by some modification in primary users like in [16], not suggested	One of the robust methods [13–15]
Traditional Jamming	Confidentiality	Apply a robust transmission security techniques (like spread spectrum or frequency hopping)
Faulty Data Injection	Entity and data origin authentication	Robust data fusion technique
Intentional Data Modification	Integrity	Error detecting/correcting codes
Non-intentional Data Modification	Integrity	Error detecting/correcting codes
Message Replay	Cryptographic nonce	-
Eavesdropping	Confidentiality	Apply a robust transmission security techniques

IEEE 802.22 security sublayer provides confidentiality, authentication and integrity services. The security sublayer consists of two main components: (1) An encapsulation protocol which defines a set of the cryptographic suites and a set of rules to apply one of these suites to MAC PDU payload, and (2) A key management protocol (PKMv2) providing the secure distribution of keying data from the BS to the CPE.

PKMv2 supports four different protocols to provide mutual authentication. Authentication can be provided by RSA-based, EAP based, RSA and EAP based, or EAP in EAP based authentications. All authentication protocols yield in a shared key which will be used to derive the session keys. A noted as defined in [4], any of suitable EAP methods can be employed as EAP authentication in IEEE 802.22, we will only focus on RSA-based authentication only to keep the performance analysis as simple as possible. We will discuss different EAP methods that can be employed in IEEE 802.22 and key derivation methods in case of EAP authentications occurs in an upcoming section.

4.3.1. RSA-based Authentication and Key Derivation

All the CPEs that use RSA authentication have factory installed private/public key pairs together with factory installed X.509 certificates. In the RSA based authentication, a BS authenticates the CPE by using its unique X.509 digital certificate which has been issued by the CPE manufacturer. The X.509 certificate contains the CPE's Public Key (PK) and its MAC address. When requesting pre-primary authorization key (pre-PAK), the CPE sends its digital certificate and a random number CPE-random to the BS. The BS validates the certificate and then uses the verified PK to encrypt pre-PAK. Then BS sends a message which contains encrypted pre-PAK, CPE-random, BS-random, BS X.509 certificate and digital signature of BS over entire message. CPE authenticates BS by using its unique X.509 certificate to validate the signature. pre-PAK is used to generate PAK which is used to generate authentication key (AK).

After mutual authentication and AK negotiation, BS sends a message to request traffic encryption key (TEK). This message contains information of CPE and a

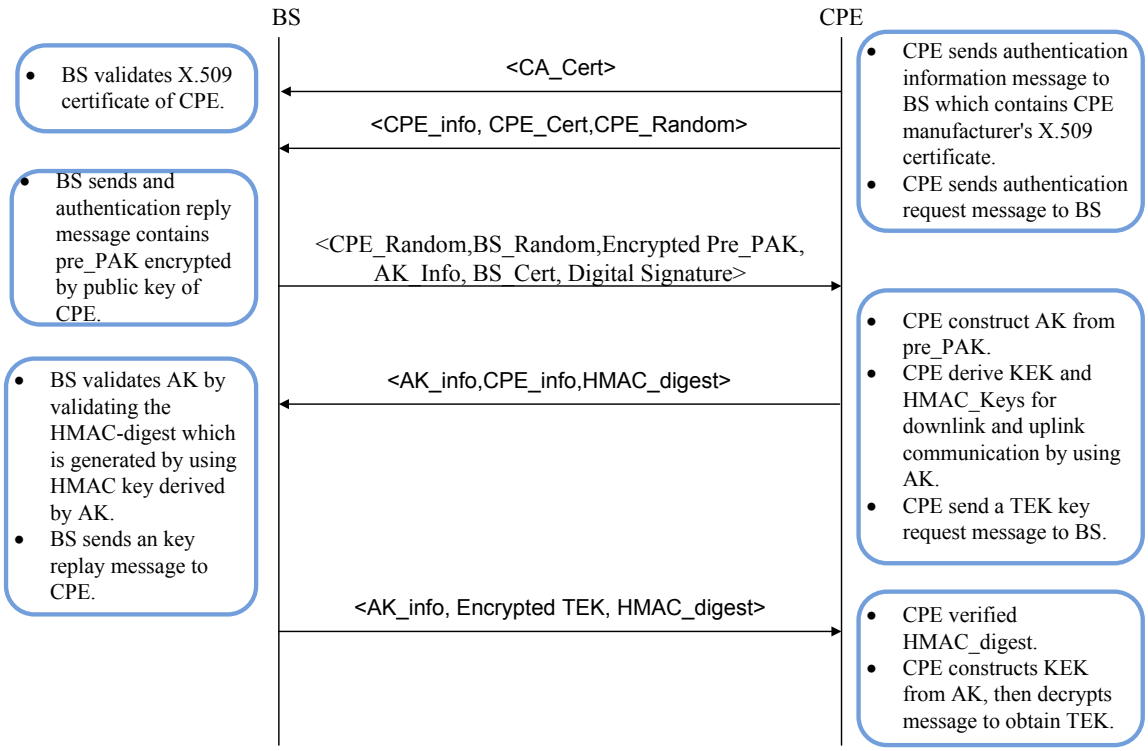


Figure 4.2. RSA Based Authentication and Key Distribution in IEEE 802.22

CMAC/HMAC-digest which is generated by using a message authentication key(MAC-KEY) derived from AK. BS validate the message by CMAC/HMAC-digest. By this validation AK can be also verified. BS sends back a message which contains TEK encrypted by KEK. KEK is derived by using AK and a CMAC/HMAC-digest. There are two different CMAC/HMAC keys for uplink and downlink communications. Authentication and key distribution steps are shown in Figure 4.2.

All PKMv2 key derivations are based on the Dot16KDF algorithm [4]. The Dot16KDF algorithm is a CTR mode construction that may be used to derive an arbitrary amount of keying material from source keying material.

After RSA authentication protocol, CPE can also request the group keys. Upon a request, BS sends a message that contains Group Key Encryption Key (GKEK) encrypted by previously derived KEK. GKEK is a multicast key which is shared among all members of the group and Group Traffic Encryption Key (GTEK)is distrubuted by using GKEK in a multicast message. Message authentication key for multicast group is derived from GKEK by using the Dot16KDF algorithm. RSA-based authentication

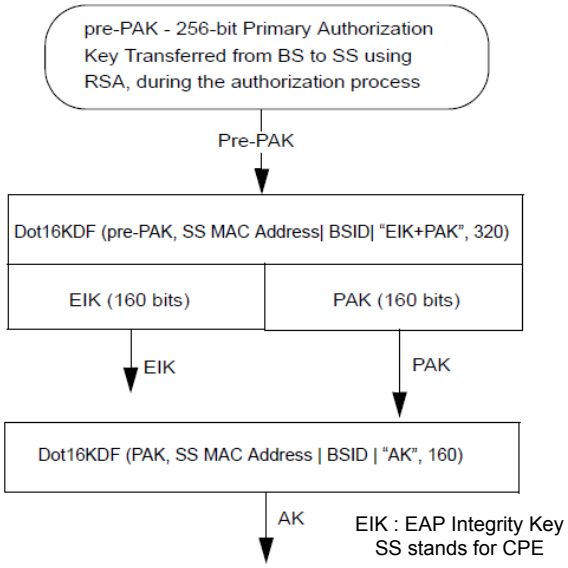


Figure 4.3. RSA Based Authentication - AK from PAK

key derivation scheme is detailed in 4.3 and 4.4.

TEKs and KEKs may be either 64 bits or 128 bits long. Security associations (SAs) employing any ciphersuite with a basic block size of 128 bits shall use 128-bit TEKs and KEKs. Otherwise 64-bit TEKs and KEKs shall be used. For SAs using a ciphersuite employing DES-CBC, the TEK in the Key Reply is triple DES (3-DES) (encrypt-decrypt-encrypt or EDE mode) encrypted, using a two-key, 3-DES KEK derived from the AK.

For SAs using a ciphersuite employing 128 bits keys, such as AES-CCM mode, the TEK in the key Reply is AES encrypted using a 128-bit key derived from the AK and a 128-bit block size. For SAs using a ciphersuite employing CBC mode encryption the Key Reply provides the requesting CPE, in addition to the TEK and CBC initialization vector, the remaining lifetime of each of the two sets of keying material. For SAs using a ciphersuite employing AES-CCM mode, the Key Reply provides the requesting CPE, in addition to the TEK, the remaining lifetime of each of the two sets of keying material. The receiving CPE uses these remaining lifetimes to estimate when the BS will invalidate a particular TEK, and therefore when to schedule future Key Requests such that the CPE requests and receives new keying material before the BS expires the keying material the CPE currently holds.

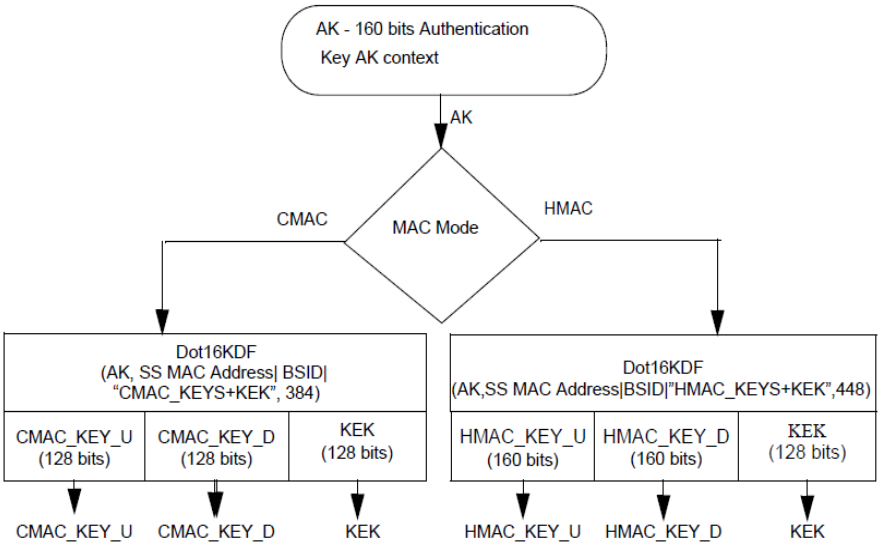


Figure 4.4. HMAC/CMAC/KEK derivation from AK

4.3.2. EAP Authentications

Extensible authentication protocol is a universal authentication mainly used in wireless systems and point-to-point networks. PKMv2 EAP Authentication uses EAP in conjunction with an operator-selected EAP Method (e.g. EAP-TLS, EAP-SIM, EAP-SRP). The EAP method will use a particular kind of credential. For EAP-TLS method the credential is an X.509 certificate, or for EAP-SIM method a Subscriber Identity Module is a credential. The EAP method selected should fulfill the "mandatory criteria" listed in Section 2.2 of RFC 4017 [23].

In PKMv2, authentication can be provided by RSA-based which is detailed previous section, EAP based, RSA followed by EAP based, or EAP followed by EAP based authentications. EAP authentication pocedure yields in a Master Session Key (MSK) which is used to construct Pairwise Master Key (PMK) and EIK. If a RSA mutual authorization took place before the EAP exchange or if the first EAP took place during EAP-in-EAP mode, the integrity of EAP messages may be protected using EIK derived from pre-PAK or construct with first EAP authentication. The process to calculate the AK when only the EAP based authentication exchange has taken place, yielding an MSK shown in Figure 4.5. The process to calculate the AK when both the RSA-based authorization exchange has taken place, yielding a PAK and the EAP

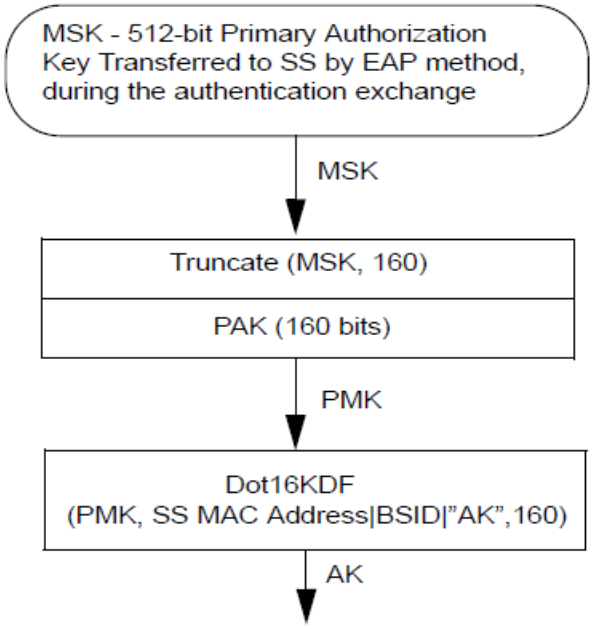


Figure 4.5. AK derivation from EAP authentication

based authentication exchange has taken place, yielding an MSK is shown in Figure 4.6. The process to calculate the AK when EAP in EAP mode authentication exchange has taken place, first EAP yielding EIK and MSK and second EAP yielding MSK2 is shown in Figure 4.7. The process to derive HMAC/CMAC and KEK keys from EIK is shown in Figure 4.8

4.3.3. Critiques on IEEE 802.22 Security Structure

IEEE 802.22 security structure provides mutual authentication, integrity and confidentiality services. Mutual authentication can be provided by RSA-based, EAP based, RSA and EAP based, or EAP in EAP based authentications. EAP-TLS, EAP-SIM and EAP-TTLS are recommended methods for EAP authentications. Triple-DES with CBC mode or AES-CCM mode can be applied to provide confidentiality. Since AES-CCM mode is called authenticated encryption and provides not only confidentiality but also integrity, HMAC/CMAC is used to provide integrity only with PKMv2 or Triple-DES encryption. PKMv2 also provides AES-KeyWrap.

In [11], two types of beacon messages (inter-cell and intra-cell) used in IEEE 802.22 are detailed. Beacons are mainly employed for preventing incumbent coexis-

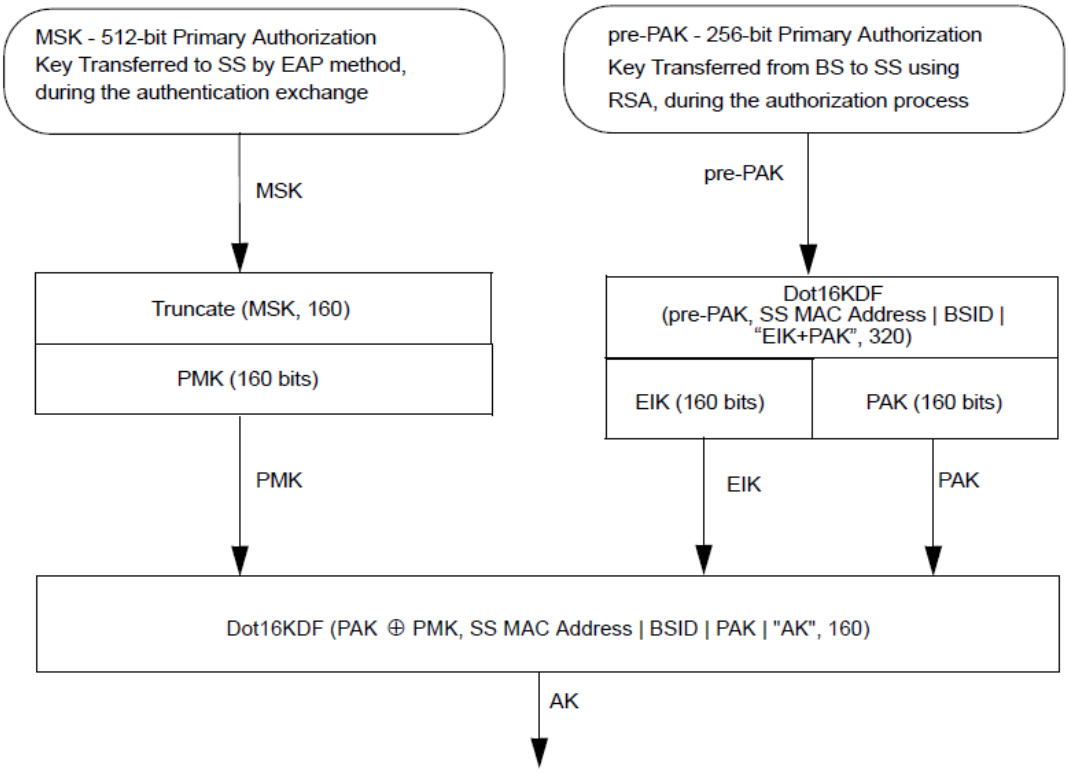


Figure 4.6. AK derivation from RSA based authentication followed by EAP authentication

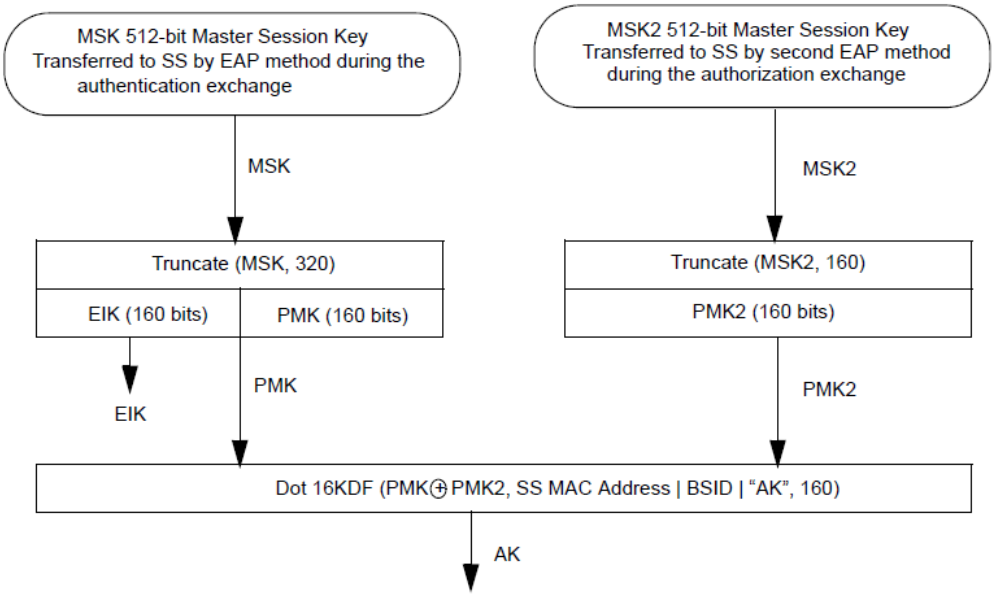


Figure 4.7. AK derivation from EAP-in-EAP authentication

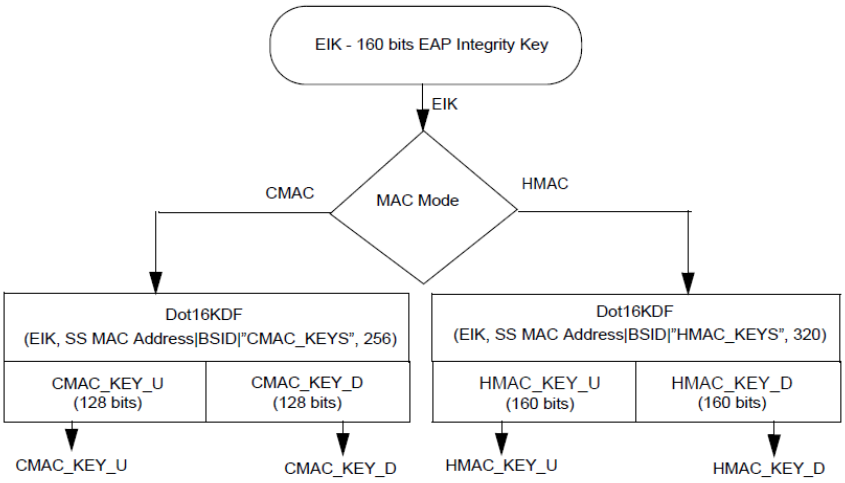


Figure 4.8. HMAC/CMAC/KEK derivation from EIK

tence or self-coexistence. By intra-cell beacons, BS and its CPEs share their communication information. By inter-cell beacons, nodes (BSs and CPEs) of different cells especially neighbors can share current communication schedules. The security sublayer of IEEE 802.22 can only protect intra-cell beacons by using shared GTEK and message authentication keys. However, inter-cell messages could not be protected in terms of security. Because of the lack of protection provided to inter-cell beacons, all inter-cell control messages are vulnerable to unauthorized modification, forgery, or replay. IEEE 802.22 recommends that neighboring BSs, if possible, synchronize their quite periods (QPs) to improve the reliability of incumbent signal detection. During these QPs, all network traffic is suspended, and 802.22 entities sense the channel for incumbent signals. Since neighboring cells coordinate QPs synchronization by exchanging inter-cell beacons, any modification in inter-cell beacons can cause a significant failure in incumbent signal detection. Therefore, a security mechanism is needed to thwart the forgery and unauthorized modification of inter-cell beacons.

Multicast communication is one of the fundamental needs in CRNs to share spectrum decision. Rather than unicast distribution, multicasting is a more efficient way to send spectrum decision. GKEK which is used to encrypt GTEK is shared among all group members in IEEE 802.22 and encrypted by shared KEK derived in authentication protocol. If any member of a secure group leaves or joins group, all shared group keys are needed to be changed immediately in order to protect confidentiality of

previous and forward communications. In IEEE 802.22, if a member joins or leaves the group, BS sends new GKEK to all members by encrypting with each CPEs'KEK. In highly mobile CRNs, this group key management scheme can cause severe performance failure.

5. PROPOSED SECURITY STRUCTURE

In this thesis we consider a infra-structure based DSA network. This network model is firstly given and detailed in [1]. In this model each cluster consists of a cluster head and mobile nodes, and is controlled by a LEO satellite. Satellite with inherent broadcast and multicast capabilities is used as spectrum decision maker.

Satellites with long life times could not adapt to rapid changes in technology, since updating a satellite which is already in orbit is a very difficult task. In [1], authors state that applying SDR and CR in space segment can improve the functionalities of a satellite segment by introducing software updates for new standards and concepts (e.g. adaptive coding and modulation). Details of our network model is given in Figure 5.1.

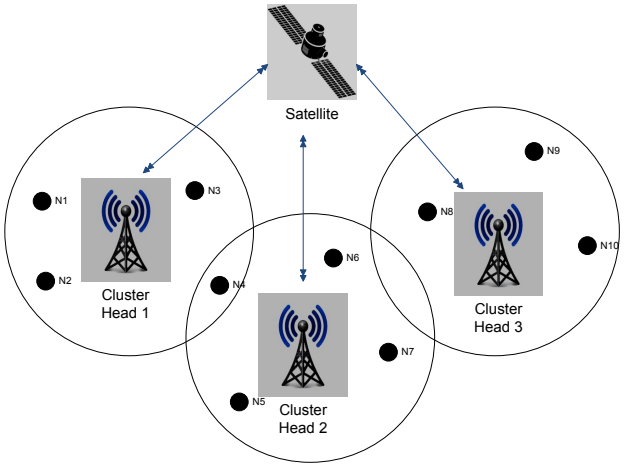


Figure 5.1. Satellite Assisted Network Model

We divide our network model into two communication tier: (1) communication group of Satellite and BSs, and (2) communication group of BSs and CPEs. Separating communication into two different tiers improves system-wide performance and security by giving a chance to apply different security structures to networks with different kinds of constraints. Satellites have some storage, processing and bandwidth usage constraints, while CR nodes have some constraints because of their dynamic nature. By dividing the networks into two communication tier, we could apply symmetric cryptographic structure and an appropriate key management scheme to the Communication Tier 1, and an hybrid cryptographic structure and an appropriate key

management scheme to the Communication Tier 2. Two communication tier of our proposed network is shown in Figure 5.2.

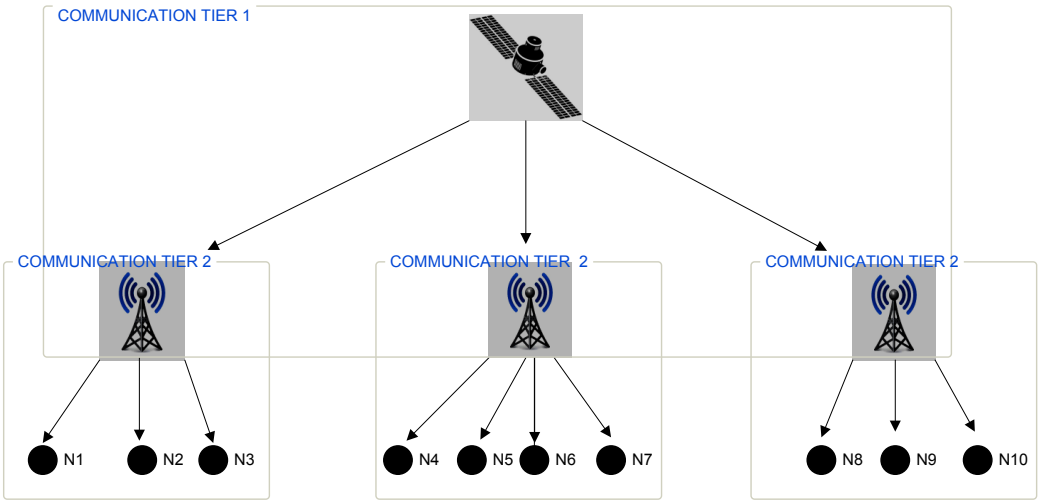


Figure 5.2. Communication Tiers

Spectrum sensing and decision threat analysis mentioned in Section 4.2, points out that confidentiality, entity and data origin authentication, cryptographic nonce and integrity services are needed to be employed in order to provide a robust security structure. We consider and apply all these cryptographic services in cryptographic structure design of each communication tier. By employing these cryptographic services, we overcome all security threat which are mentioned in Section 4.2.

5.1. Security Structure for Communication Tier 1

Security structure for this tier of communication provides confidentiality, integrity, data origin and entity authentication, message freshness, and key management functionalities. Satellite network has some strict constraints like storage, processing and bandwidth usage. Since, asymmetric techniques in cryptography have expensive exponential operations and need more storage space to keep long asymmetric keys and parameters, we prefer to use symmetric techniques at Tier 1 security structure. In this network, satellite is Key Distribution Center (KDC). Whenever a BS wants to join the network, satellite and BS mutually construct a session key (contains encryption and message authentication (MAC) key), shared only between these two entities. Key establishment protocol base on symmetric techniques which use the pre-distributed

symmetric keys which is called initial session key (ISK) throughout this thesis. The constructed session key is used in the unicast communications between satellite and BS. After constructing the session key, satellite sends group communication keys which are used in multicast communication between satellite and BSs.

Since BSs are stationary, multicast group re-keying will be no longer a constraint for our key management design of Communication Tier 1. In terms of storage, processing and communication requirements, GKMP is the most effective key management protocol as shown in Table 5.1, 5.2, 5.2. The main drawback is that as all members know the GKEK, there is no solution for keeping the forward secrecy when a member leaves the group since key re-keying message is encrypted by using current GKEK which has been already known by the leaving entity. However, we assume that member of Tier 1 network are stationary and once they join the group, they stay as long as the group is active. Therefore, for Tier 1 group communication we will employ a group key management scheme based on GKMP key management protocol.

In GKMP [24] key management protocol, when the first member joins group, KDC creates a Group Key Packet (GKP) that contains a group traffic encryption key (GTEK) and a group key encryption key (GKEK). When a new member wants to join the group, the KDC sends it a copy of the GKP. When a rekey is needed, the group controller KDC generates a new GKP and encrypts it with the current GKEK. In our network, group key generation (GKP) is handled by the satellite which is also the KDC of the network. GKP contains GTEK and GKEK. Satellite prepare the GKP and sends all new member by the session keys construct between satellite and individual BS during join operation. BSs derive $GTEK_E$ and $GTEK_{MAC}$ from GTEK and $GKEK_{n+1}$ and $GTEK_{MAC_{n+1}}$ from GKEK by applying some mathematical functions. If a rekeying is needed, satellite prepare a new GKP and multicast it by encrypting the current GKEK and appending MAC value which calculates by using $GTEK_{MAC_{n+1}}$.

In this network Tier, we assume that all entities have a true random number generator with high entropy. Therefore, using these true random number generator, we can achieve high quality (in terms of security) key materials (i.e. random numbers, group

keys). In the cryptographic structure of this tier of network, we use Blowfish(64 bits block size and 128 bits of key size) with CBC mode [25] as encryption and CMAC [26] as a message authentication code algorithm. We also assume a robust Error Detection/Correction Code is employed for satellite communication in which random error in bits of transferred data occurs in a high probability.

5.1.1. Initialization

Initialization scheme proceeds as follows:

1. Satellite as KDC has GKP which contains $GTEK$ and $GKEK$. BS derives $GTEK_{E_n}$ and $GTEK_{MAC_n}$ from $GTEK$ and $GKEK_{n+1}$ and $GKEK_{MAC_{n+1}}$ from $GKEK$ by applying some mathematical functions.
2. Before launching, Initial Symmetric Keys (ISKs)(the amount of these keys are the number of the potential BSs that can join to network during the lifetime of the satellite) are loaded on a temper proof memory of satellite. ISKs is used in key establishment protocol which occurs between satellite and BSs and stored on a secure unit like Hardware Security Module (HSM) on the ground.
3. To each BS which attempts to join Tier 1 communication, ISK and index of ISK is securely loaded.
4. ISK key contains two symmetric key, ISK_E for encryption and ISK_{MAC} for message authentication.

5.1.2. Join Network

The basic steps of the protocol proceed as follows:

1. BS generates random r_A and constructs a join request message which contains r_A, index of ISK, BS_{ID}, SAT_{ID} and a MAC which is generated by using ISK_{MAC}.
2. Satellite retrieves the ISK corresponding with the index number in authentication request and validates the MAC value. If successful, Satellite constructs a replay which contains r_A, r_B,ID_{BS}, ID_{SAT}, encrypted with ISK_E, and then MAC value

is generated by ISK_{MAC}.

3. BS validates MAC value in replay and checks the random number r_A. If these checks are successful, then it constructs a replay containing r_B+1,,ID_{BS}, ID_{SAT}, encrypted with ISK_E, and then MAC value is generated by ISK_{MAC}. BS derives session keys (SKs) by using $r_A XOR r_B$. Output of key derivation function is two symmetric session keys to encryption(SK_E) and MAC algorithm(SK_{MAC}).
4. Satellite validates MAC value. If successful, satellite decrypts the message and checks r_B. If successful, then satellite derives session keys (SK_E, SK_{MAC}) by using r_B. Satellite constructs a key distribution message which contains ID_{BS}, $GTEK$ and $GKEK$, encrypts it, and calculates the MAC value.
5. BS validates the MAC value and then decrypts the message to retrieve the $GTEK$ and $GKEK$ keys.

The first step is a request to join the network. Since the data transferred in this step has not any confidentiality, we do not apply encryption on this message. Besides the integrity of the data is crucial and it is protected by applying MAC on this data. The random number r_A guarantees the freshness of the key establishment protocol. Moreover it is used with r_B to construct the session keys. Since the second step contains the random number r_B (which is the second entity of session key derivation function), the confidentiality has to be protected. Therefore, we apply an encryption over this message while the integrity of the message is also protected by MAC algorithm.

In the third step r_A is retransmitted to prove the BS these random number received by satellite correctly. In the third step also contains random number $r_B + 1$, the cryptographic service of confidentiality and integrity are also applied. After this step, each entity knows that the opponent one has received random number correctly. BS sends the random number r_B increased by one, in order to prevent replay attacks by guaranteing the freshness of the transactions. Sending r_B, r_A is another option to provide the freshness. For the bandwidth efficiency, we prefer to use the first option (r_B increased by one). Since the last step contains group keys, confidentiality and integrity are employed. The freshness of these steps is provided by using freshly constructed session keys in encryption and MAC algorithms. Using of these session keys in this

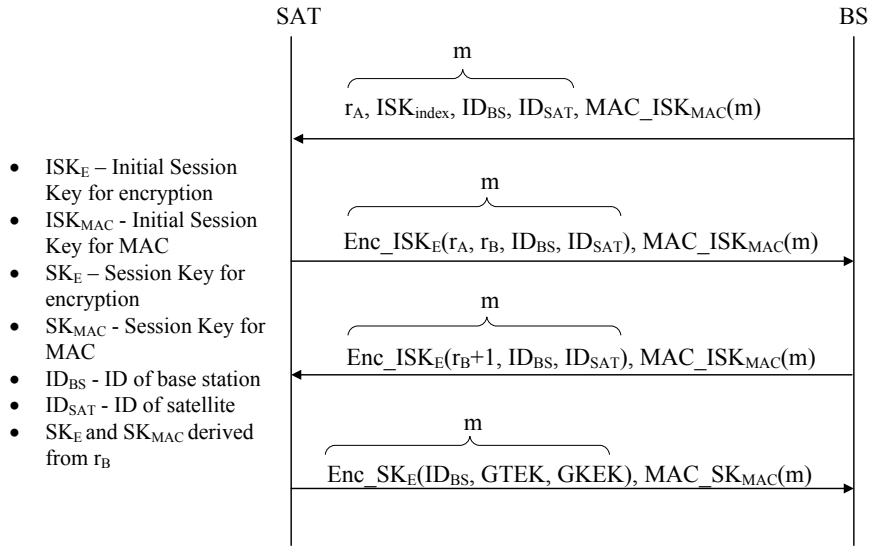


Figure 5.3. Tier 1 Security Structure - Join Network

step is also called as a key agrement (each party make sure about the correctness of the construction of session keys.). BS assures the correctness of the session key by checking the ID_{BS} in the message. Satellite assures the correctness of the session key, if it does not receive any join request initiated by the same BS.

The details of join network protocol are shown in Figure 5.3.

5.1.3. Sending Sensing Data and Multicast Decision

Each BS periodically collects the spectrum sensing data from CRs in its coverage area and relays this spectrum information to the satellite. Satellite analyzes all spectrum decisions coming from different BSs and constructs a spectrum decision. By using Tier 1 multicast channel, spectrum decision is sent to all BSs.

The basic steps of the protocol proceed as follows:

1. BS constructs a message containing spectrum sensing data D and a timestamp t_s, encrypted with SK_E with calculated MAC value generated by SK_{MAC}.
2. Satellite validates the MAC value in spectrum sensing data message coming from BS. If it is successful, satellite takes the data as a valid one.

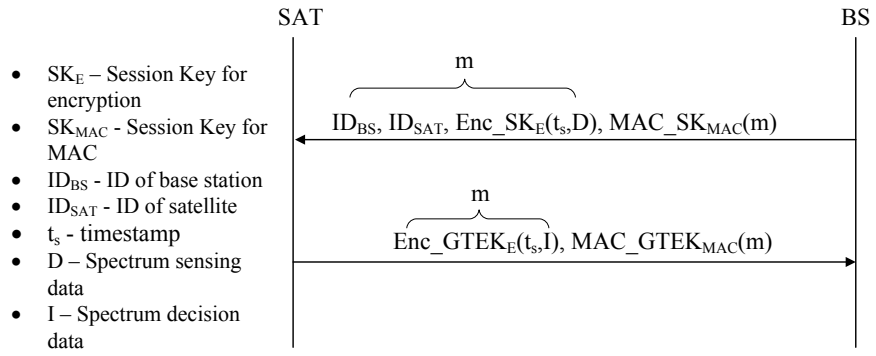


Figure 5.4. Tier 1 Security Structure - Spectrum Sensing and Decision

3. After satellite retrieves all D messages, satellite constructs the spectrum decision with a timestamp t_s and multicasts this decision by using $GTEK_E$ and $GTEK_{MAC}$.
4. BS validates MAC value in spectrum decision. If it is successful, then BS relays the spectrum decision to all CRs in its range.

In this protocol, timestamps are used for providing the freshness of spectrum sensing and decision messages. Confidentiality of these message should also be provided in order to prevent traditional jamming and PUE attacks which are detailed in Section 4.2. In these protocol message authentication and integrity are ensured by using MAC. Since MAC as a message authentication technique, could not satisfy non-repudiation, any entity who knows the $GTEK$ and $GTEK_{MAC}$ (any BS in the network) can construct the spectrum decision message and multicast it as satellite. However, we assume that all BSs in the Communication Tier 1 are honest. Therefore this network tier does not need non-repudiation service.

The details of spectrum sensing and decision protocol are shown in Figure 5.4.

5.1.4. Inter-cell Communications

The importance of applying security to inter-cell communication (communication between BSs) is discussed in Section 4.1 and also mentioned in [11]. In our Communication Tier 1 security structure, inter-cell communication security is provided by multicasting capabilities of BSs. Information about the BS's traffic schedule, the current

operation channel of BS are some of the messages which are shared between neighbor BSs.

5.2. Security Structure for Communication Tier 2

In this communication tier, confidentiality is provided by employing a symmetric encryption algorithm. To ensure entity authentication, key establishment and key agrement protocol a modified version of Station-to-Station protocol which is a variation of Diffie-Hellman protocol is proposed. Integrity which is a guarantee that the data received is exactly as sent by authorized entity is provided by using either a digital signature or a MAC algorithm which also provides data origin authentication. The freshness of the messages are ensured by using cryptographic random number in entity authentication protocols, and timestamps for other protocols. Initialization, join network, sending spectrum sensing data, multicast spectrum decision, handover between base stations and re-keying are six main events that are handled by the spectrum sensing and decision protocol. We will define our security structure by considering these six events.

Since the confidentiality of the messages are needed to mitigate some type of attacks explained in Table 4.3 and Table 4.4, CR node and BS need to establish a key with a mutual entity authentication protocol. This key is used as a secret key between CR node and BS. Furthermore, a derivation of this secret key is used for distributing the MAC algorithm symmetric key which will be shared between the node and BS, and group encryption keys. Entity authentication, key establishment and agrement protocol used in this security structure is a modified version of Station-to-Station protocol which is a variation of Diffie-Hellman protocol [6].

Since each BS multicasts its spectrum decision, a group key management scheme should be also provided. We decide to use Logical Key Hierarchy (LKH) as a solution to the group key management to take advantage of the efficiency over dynamic networks [7, 27]. In LKH a central server (key server) holds a key tree which is used for key distribution and key updates. The leaf nodes represent nodes whereas the root node

represents the key server (BS). In the key setup phase, each node is authenticated to the key server and ends up sharing a key with the server. These keys are cryptographically symmetric keys shared between the two parties and are denoted as leaf keys. The secret key between node and the BS (leaf key) is K in Figure 5.5. The other keys in LKH, related to the node are denoted as K_{LKH} in Figure 5.5.

We use Blowfish (64 bits block size and and 128 bits of key size) with CBC mode [25] as symmetric encryption algorithm and CMAC [26] as message authentication code in order to be compatible with cryptographic algorithms used in Communication Tier 1. Elliptic Curve Digital Signature Algorithm (ECDSA) is employed as digital signature algorithm. One of the hash function in SHA-2 family is used in our Tier 2 cryptographic structure.

5.2.1. Initialization

Initialization scheme proceeds as follows:

1. All nodes and BSs are given their public and private key pairs which are issued by a certification authority.
2. Diffie-Hellman key exchange parameter a and p are given all CR entities. They are both public and used by all CR entities. Parameter p is a prime number and parameter a (usually called a generator) is an integer less than p, with the following property: for every number n between 1 and $p-1$ inclusive, there is a power k of a such that $n = a^k \bmod p$
3. All nodes and BSs have a unique ID and time synchronization with other CR entities.
4. All nodes are given an individual MAC algorithm key while the BSs construct their individual spectrum decision group encryption key.

5.2.2. Join Operation

The basic steps of the protocol proceed as follows:

- CR node generates a secret random x which satisfies $1 \leq x \leq p-2$ and sends a^x mod p to BS.
- BS generates a secret random y which satisfies $1 \leq y \leq p-2$ and a random r_1, then computes the shared key $K = (a^x)^y$. Furthermore, BS signs (ID_{BS}, r_1, a^y, a^x) and encrypts ID_{BS}, r_1 and signature by using K. Then BS sends a^y mod p and encrypted message to CR node.
- CR node also computes the shared key $K = (a^y)^x$ and decrypts the received message and verifies the signature of BS. If successful, CR node accepts that K is actually shared with the BS. CR node sends an analogous message which contains r_1, r_2. Then constructs the key encryption key, $KEK = K$ XOR r_1 XOR r_2.
- BS similarly decrypts the received message and verifies CR node's signature. If successful, BS accepts that K is actually shared with CR node and construct key encryption key $KEK = K$ XOR r_1 XOR r_2. BS sends r_2, and the group keys K_{LKH} appending a hash value of these items, encrypted by KEK.
- CR nodes sends MAC algorithm symmetric key K_{MAC} appending a hash value encrypted by KEK.

First three steps of this protocol is a version of Station-to-Station key establishment protocol in which two random number (r_1 and r_2)are added. By using digital signature in the second and third step, the entities ensure the identity of the opponents. The encryption and the signature in the second and third step also ensure the opponents construct the session key correctly. The correctness of the random number shared between entities is achieved by sending the received random number to the opponent in the response in the third and fourth steps. The message authentication is achieved by digital signature in the second and third step and by encryption over data and the hash of data in the fourth and fifth steps.

The details of join network protocol are shown in Figure 5.5.

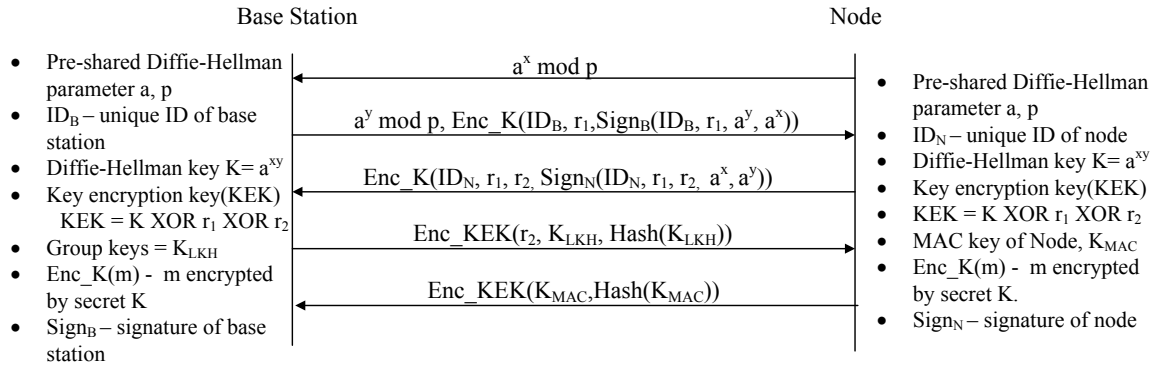


Figure 5.5. Tier 2 Security Structure - Join Network

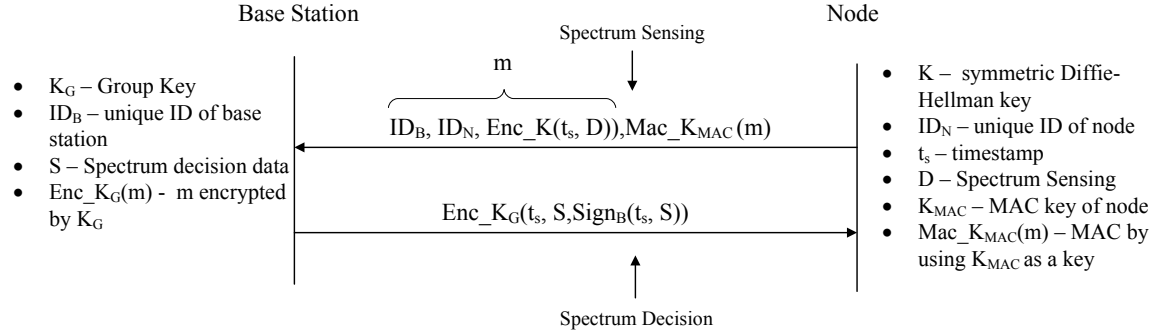


Figure 5.6. Tier 2 Security Structure - Spectrum Sensing and Decision

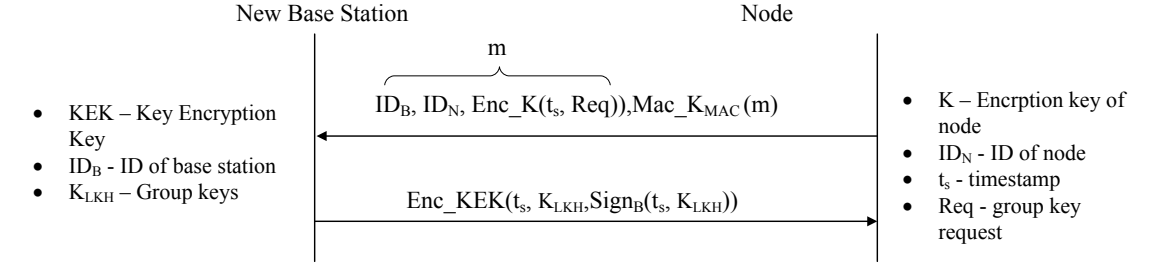


Figure 5.7. Tier 2 Security Structure - Handover between Cells

5.2.3. Sending Sensing Data and Multicast Decision

Nodes sense the spectrum in sensing period to detect spectrum holes. Then they prepare the channel availability data and send it to relevant BS. Next, BS takes all channel availability data and relays them to the satellite in which some cognitive methods to construct the spectrum decision is applied on these data. After completion of the spectrum decision satellite multicast the decision to BSs,then each BS multicasts the decision to the CR nodes in its range. The Spectrum sensing and decision scheme proceeds as follows:

1. CR node encrypts timestamp t_s and spectrum sensing data D by using secret key K, calculate the MAC value of ID of BS, ID of CR node and encrypted data by using K_{MAC} as a key. Then, CR node sends this message to BS.
2. BS calculates the MAC value of the received message. If it is exactly same as the received one, BS decrypts the encrypted data. If timestamp is valid, then BS takes the spectrum sensing data as a valid one. After receiving the spectrum decision from satellite, BS constructs a spectrum decision message. Then, BS signs timestamp t_s and spectrum decision S. Furthermore, BS encrypts t_s, S and signature by using the group key K_G and multicasts this encrypted message.
3. CR node decrypts the received multicast message, checks the validity of t_s and signature, if successful, CR node takes the spectrum decision data as a valid policy.

In this protocol, freshness of the spectrum sensing and decision messages are provided by timestamps. The message authentication is achieved by applying MAC in first step and digital signature in the second step. The reason we decide to use a digital signature instead of MAC in the second step, is the need of non-repudiation service besides message authentication. The decision message could only be constructed by BSs. The digital signature proves the origin identity for this multicast message. In order to apply MAC in a multicast message, a group MAC key is needed to be shared among all the entities of the group. Since all entities knows the multicast encryption and MAC keys, each entity could be able to construct a spectrum decision message and

multicast this message. When the entities in a group are not honest, it is better to use digital signature in order to provide a message authentication of a multicast message.

In Figure 5.6 security structure for sending sensing data and multicast spectrum decision is detailed.

5.2.4. Handover between Base Stations

As stated in the previous sections, our network model is divided into cells which contain a BS and mobile CR nodes. Therefore these mobile nodes can easily switch between network cells. We assume that each BS sends information of new nodes including their encryption, key encryption and MAC keys to its neighbor BSs. Therefore nodes do not have to establish join protocol, each time they cross into a new cell. CR node, crosses into a new cell, sends a request to new BS in order to obtain group keys. Handover schemes proceed as follows:

1. CR node encrypts timestamp t_s and request data Req by using secret key K, calculate the MAC value of ID of new BS, ID of CR node and encrypted data by using K_{MAC} as a key. Then, CR node sends this message to the new BS.
2. BS checks the validity of the of the MAC value. If successful, BS decrypts the received message and checks the validity of t_s. If timestamp is valid, BS checks the request. BS signs t_s and group keys, encrypts concatenation of t_s, group keys and signature by using KEK and sends to CR node.
3. CR node decrypts the received message, checks the validity of timestamp and signature. If successful, CR node accepts the group keys.

In Figure 5.7 handover protocol is detailed.

5.2.5. Re-keying

In order to protect forward and backward communication secrecy of groups, whenever a mobile node enters or leaves the group, all group keys needs to be re-keyed. We

try to decrease the re-keying cost by employing the LKH scheme as a key management protocol in Communication Tier 2. The re-keying cost of different key management scheme is detailed in Section 5.3.1.

5.3. Analysis of Proposed Security Structure

In this section we give the security and performance analysis of the proposed security structure. The analysis is detailed under three subsection. We present the security and performance analysis of the key management techniques in Subsection 5.3.1. Then, in Subsection 5.3.2 and 5.3.3 we give the results of our security and performance analysis of the cryptographic algorithms, and structural design and protocols which are employed in the proposed security structure respectively.

5.3.1. Key Management Techniques - Performance Analysis

In order to give an appropriate decision about employed group key management techniques, we construct a performance evaluation table for different group key management approaches. The key performance metrics of group key management techniques are bandwidth usage, processing and storage requirements [7]. Performance evaluation are detailed in Tables 5.1, 5.2, 5.3 and 5.4 and the notations used these tables are detailed in Table 5.5.

We consider three main key management scheme: $GKMP$, LKH, and $Flat$. In $GKMP$ [24] key management protocol, when the first member joins group, KDC creates a Group Key Packet (GKP) that contains a group traffic encryption key (GTEK) and a group key encryption key (GKEK). When a new member wants to join the group, the KDC sends it a copy of the GKP. When a rekey is needed, the group controller KDC generates a new GKP and encrypts it with the current GKEK. Since re-keying message is encrypted by using the current GKEK, as shown in Table 4.4 this key management scheme could not provide the forward secrecy. Forward secrecy in group communication is provided when a member who leaves a group, could not derive the group keys by eavesdropping). Since backward secrecy in group communication is provided when

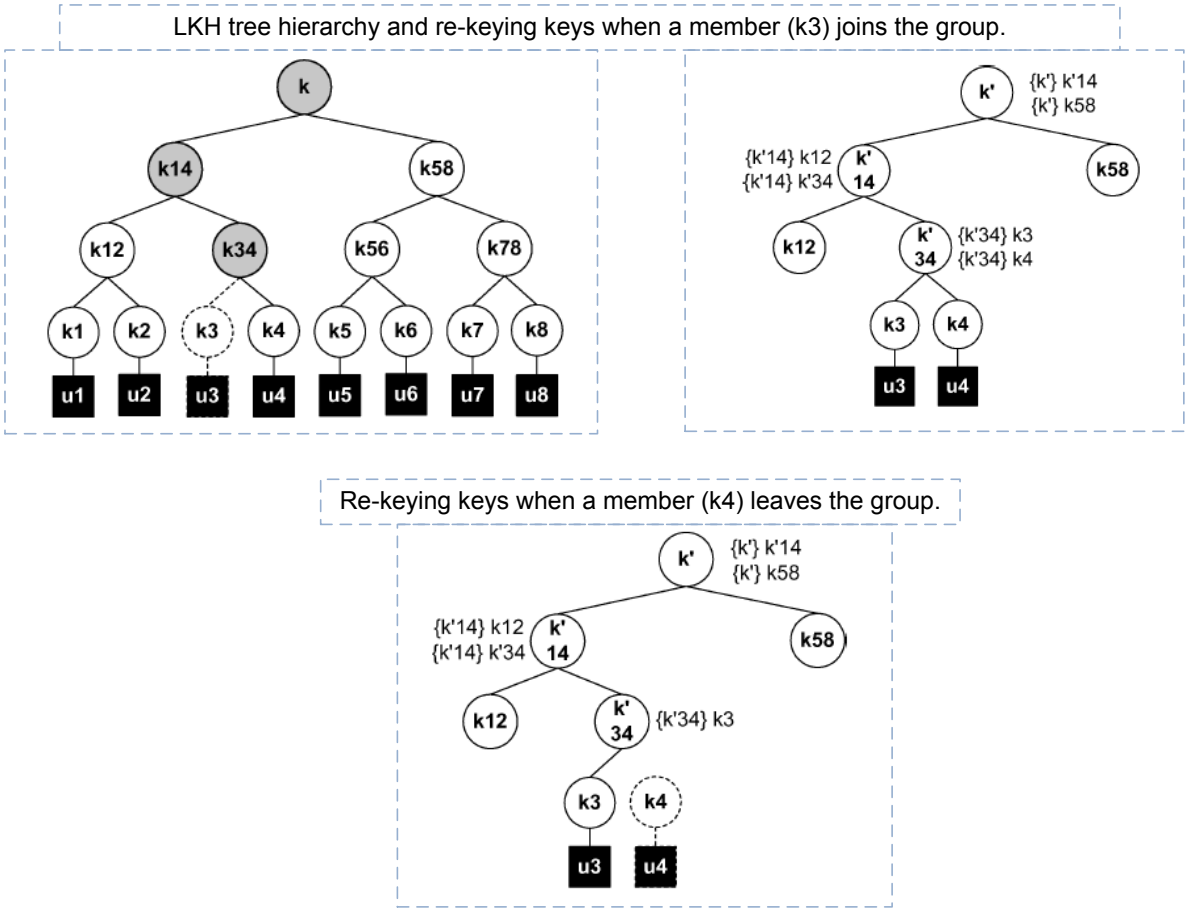


Figure 5.8. LKH Key Management Scheme - Re-keying

a member who joins the group, could not derive the previously used group keys, this key management scheme provide backward secrecy by easily re-keying the group keys after the new member joins the group.

In LKH a central server (key server) holds a key tree which is used for key distribution and key updates. Figure 5.8 shows a hierarchical key structure. The leaf nodes represent members whereas the root node represents the key server. In the initialization phase, each node is authenticated to the key server and ends up sharing a key with the server. These keys are cryptographically symmetric keys shared between the two parties and are in denoted as leaf keys in Figure 5.8. We assume that the leaf keys are constructed by a key establishment protocol run between the two entities. The cost of construction of the leaf keys are not explained in this subsection but in Subsection 5.3.2. In LKH, number of maximum number of members is calculated by k^d where k is the branching factor tree and d is the depth of the tree. This key management

Table 5.1. Bandwidth Cost of Key Management Schemes

Method/Metric	Bandwidth Cost		
	Initialization	Join	Leaving
Flat	NK	NK	$(N-1)K$
GKMP	$2NK$	$4K$	$-$
LKH	$(P_N-1)K$	$(kd_N)K$	$(kd_N-1)K$
LKH+LKH	$(P_L-1)K+L(P_S-1)K$	$(kd_L)K+(kd_S)K$	$(kd_L-1)K+(kd_S-1)K$
Flat+LKH	$LK+L(P_S-1)K$	$LK+(kd_S)K$	$(L-1)K+(kd_S-1)K$
GKMP+LKH	$L2K+L(P_S-1)K$	$4K+(kLd_S)K$	$L(kd_S-1)K$

Table 5.2. Storage Cost of Key Management Schemes

Method/Metric	Secrecy		Storage Cost	
	F	B	KDC	Members
Flat	yes	yes	$(N+1)K$	$2NK$
GKMP	no	yes	$2K$	$2NK$
LKH	yes	yes	P_NK	$N(d_N+1)K$
LKH+LKH	yes/yes	yes/yes	$P_LK+L(P_SK)$	$L(d_L+1)K+LS(d_S+1)K$
Flat+LKH	yes/yes	yes/yes	$(L+1)K+L(P_SK)$	$2KL+LS(d_S+1)K$
GKMP+LKH	no/yes	yes/yes	$2K+L(P_SK)$	$2KL+LS(d_S+1)K$

Table 5.3. Initialization - Processing Cost of Key Management Schemes

Method/Metric	Initialization - Processing Cost	
	KDC	Members
Flat	$R+N.E$	$N.D$
GKMP	$2R+N.E$	$N.D$
LKH	$(P_N-N)R+(P_N-1)E$	$DN.d_N$
LKH+LKH	$(P_L-L).R+(P_L-1)E+L((P_S-S).R+(P_S-1)E)$	$(Ld_L+L(S.d_S))D$
Flat+LKH	$R+L.E+L((P_S-S).R+(P_S-1)E)$	$L.D+L(S.d_S)D$
GKMP+LKH	$2R+L.E+L((P_S-S).R+(P_S-1)E)$	$L.D+L(S.d_S)D$

Table 5.4. Join/Leaving - Processing Cost of Key Management Schemes

Method/Metric	Processing Cost			
	Join		Leaving	
	KDC	Members	KDC	Members
Flat	$R + N.E$	$N.D$	$R + (N-1)E$	$(N-1)D$
GKMP	$2R + E$	$N.D$	$-$	$-$
LKH	$d_N R + kd_N E$	$(P_N - 1)D$	$d_N.R + (kd_N - 1)E$	$(P_N - d_N)D$
LKH+LKH	$d_L.R + kd_L E + d_S.R + kd_S E$	$((P_L - 1) + (P_S - 1))D$	$d_L.R + (kd_L - 1)E + (d_S.R + (kd_S - 1)E)$	$D((P_L - d_L) + (P_S - d_S))$
Flat+LKH	$R + L.E + d_S.R + kd_S E$	$(L + (P_S - 1))D$	$R + (L-1)E + d_S.R + (kd_S - 1)E$	$D((L - 1) + (P_S - d_S))$
GKMP+LKH	$2R + 2E + d_S R + kd_S E$	$(L + (P_S - 1))D$	$d_S.R + (kd_S - 1)E$	$(P_S - d_S)D$

Table 5.5. Notations in Tables 5.1, 5.2, 5.3

N	number of all members
M	number of mobile CR nodes
L	number of BSs
$M/L = S$	number of mobile nodes in each BSs
$(kN - 1/k - 1) = P_N$	number of nodes in the tree
d_N	depth of tree while number of member N
k	branching factor of tree
K	size of key
E	the cost of one encryption
D	the cost of one decryption
R	the cost of one random number generation
F	Forward secrecy
B	Backward secrecy

scheme provides forward and backward secrecy. In the *Flat* key management scheme, each node is authenticated to the key server and ends up sharing a key with the server. When re-keying is needed, key center sends the new group key in a private message to each member.

Communication Tier 1 consists of satellite and BSs. These entities are stationary and this property makes the entire network static. Therefore, re-keying, and backward and forward secrecy are not an issue which we need to consider during our security structure design. We assume that when a member join Tier 2 network, it stays in the network as long as the satellite is active. The proposed security structure in Tier 1 aims to minimize satellite resource usage, namely satellite channel bandwidth and internal satellite resources, e.g. satellite processing and storage. Since, providing forward secrecy is not necessary for this tier of communication, this tier employs $GKMP$ as a key management scheme.

Communication Tier 2 consists of BSs and CR nodes. Since CR nodes are mobile, this tier of network is highly dynamic and re-keying is needed to be handled in an efficient way while forward and backward secrecy are also provided. Therefore, we consider to use a tree based key management structure LKH, which could help to decrease the cost of re-keying.

The efficiency of proposed hybrid key management scheme ($GKMP + LKH$) compare with the other probable solutions. We could apply LKH, $GKMP$ or *Flat* key management scheme to whole network. In this solution satellite could be the key center and manage the group nodes and BSs. The other solution is to apply LKH for Communication Tier 1 and Tier 2 separately ($LKH + LKH$). In this option, satellite construct a LKH for Tier 1 while each BSs construct another LKH for Tier 2. The last option which we consider in this thesis is Flat key management for Tier 1 and LKH for Tier 2 ($Flat + LKH$). Since the re-keying cost is an important issue that is considered during the design of key management structure, we only consider the LKH scheme as a solution for the Tier 2 communication network.

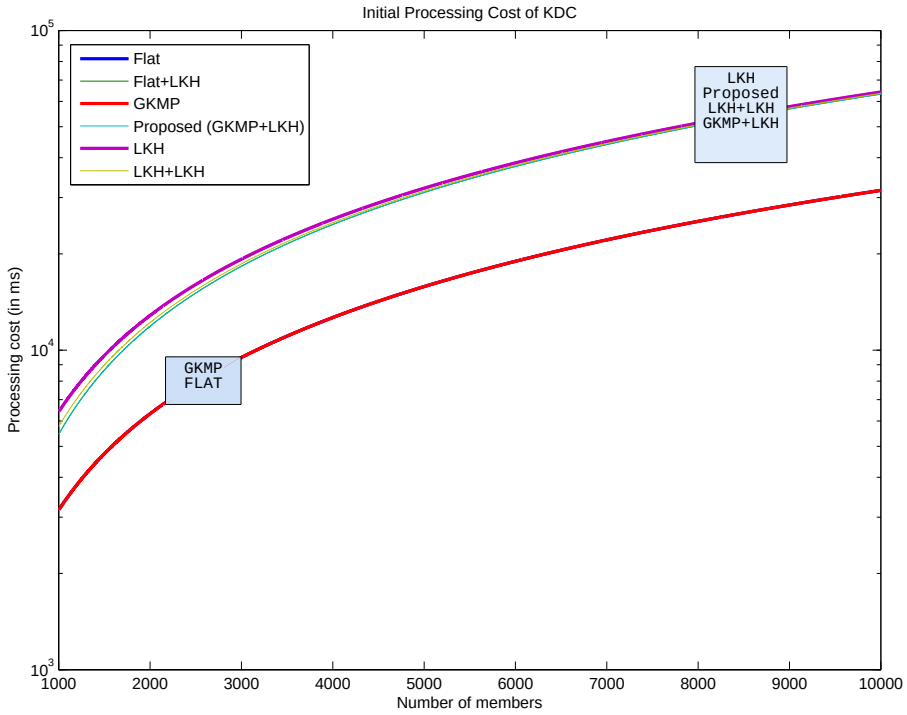


Figure 5.9. Initial processing costs for KDC

We denote the number of mobile CR nodes as M, the number of BSs L and the number of all member $(M + L)$, N. In our performance evaluations, we assume that there exists $S(M/L)$ CR nodes in each group of BSs. In proposed $GKMP + LKH$ solution, satellite construct a $GKMP$ key management scheme for L BSs while each BSs construct a LKH for S CR nodes. In the second option, Satellite construct a LKH, $GKMP$ or $Flat$ key management scheme for N members. In the $LKH + LKH$ solution, satellite applies LKH key management scheme for L BSs while each BSs construct a LKH for S CR nodes. In the $Flat + LKH$ solution, satellite applies Flat key management scheme for L BSs while each BSs construct a LKH for S CR nodes.

We make a series of simulations by using MatLab. We assume that there exist 1000 to 10000 members and 100 BSs in our network. We examine the bandwidth, storage and processing costs of different key management schemes by using the calculated formulas in the Table 5.1, 5.2, 5.3 and 5.4. We state the results of processing costs of initialization for KDC and members in Figures 5.9 and 5.10 respectively. By processing cost of initialization for KDC and members, $GKMP$ and $Flat$ key man-

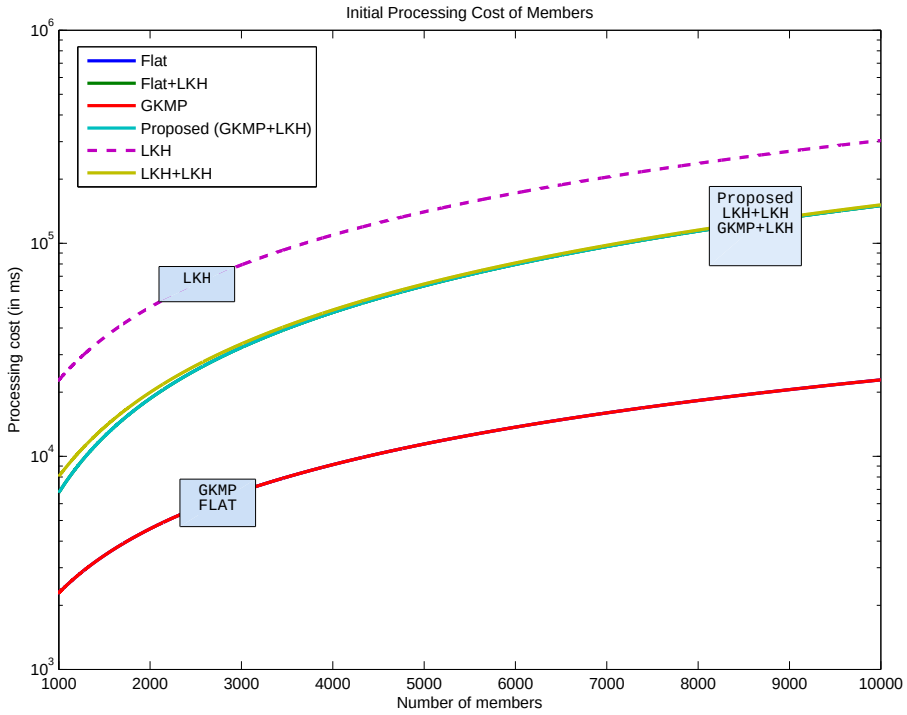


Figure 5.10. Initial processing costs for Members

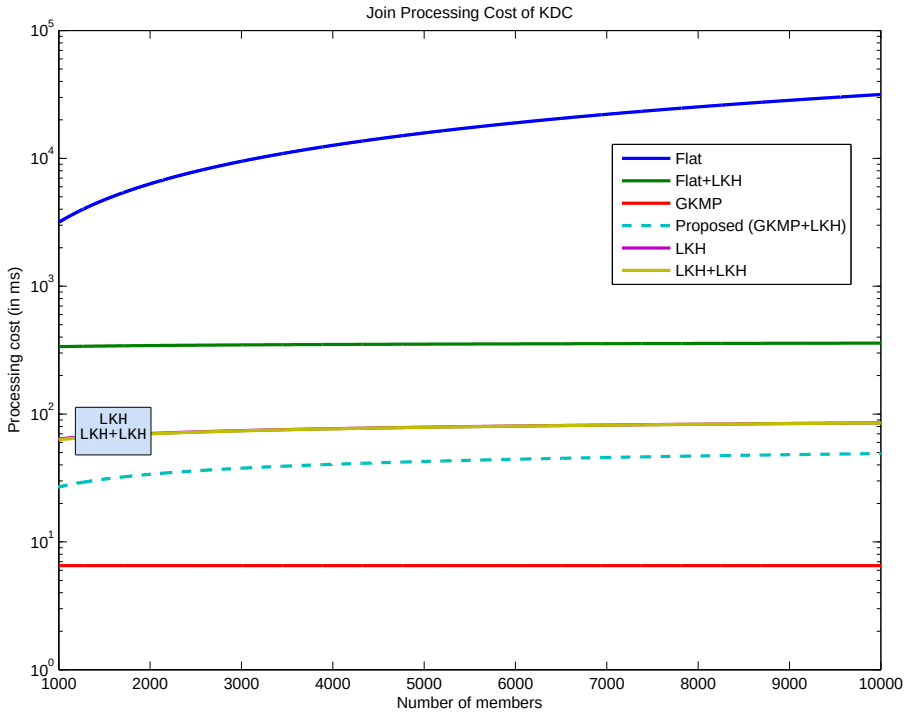


Figure 5.11. Join processing costs for KDC

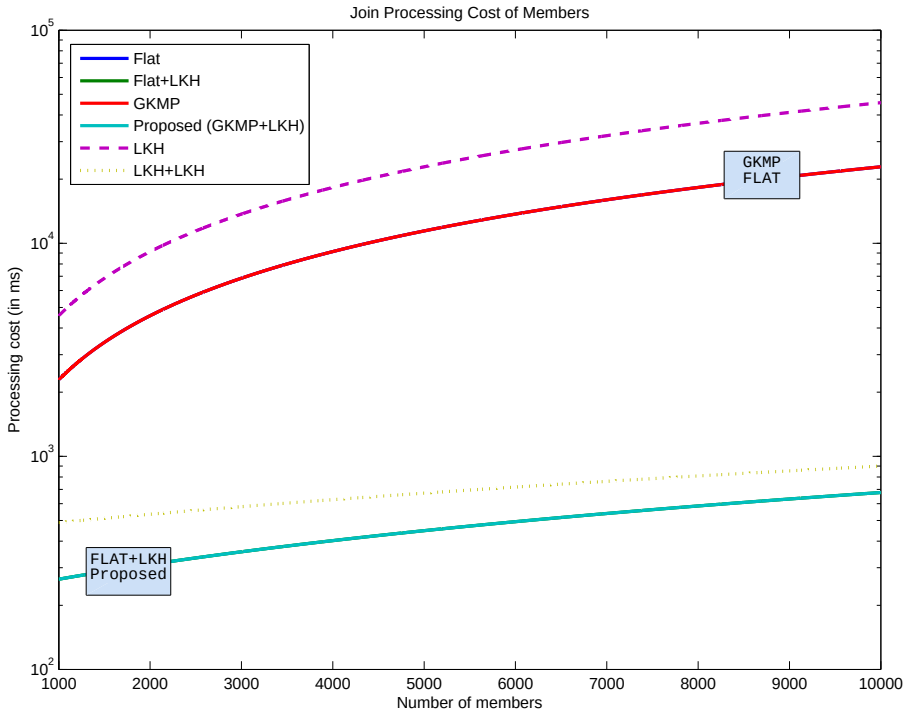


Figure 5.12. Join processing costs for Members

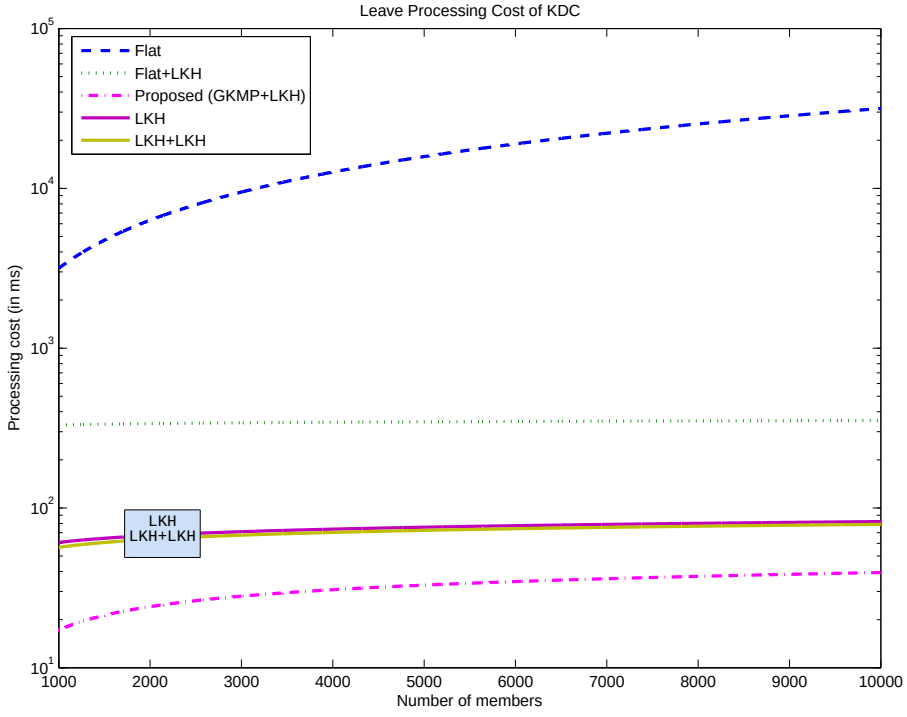


Figure 5.13. Leave processing costs for KDC

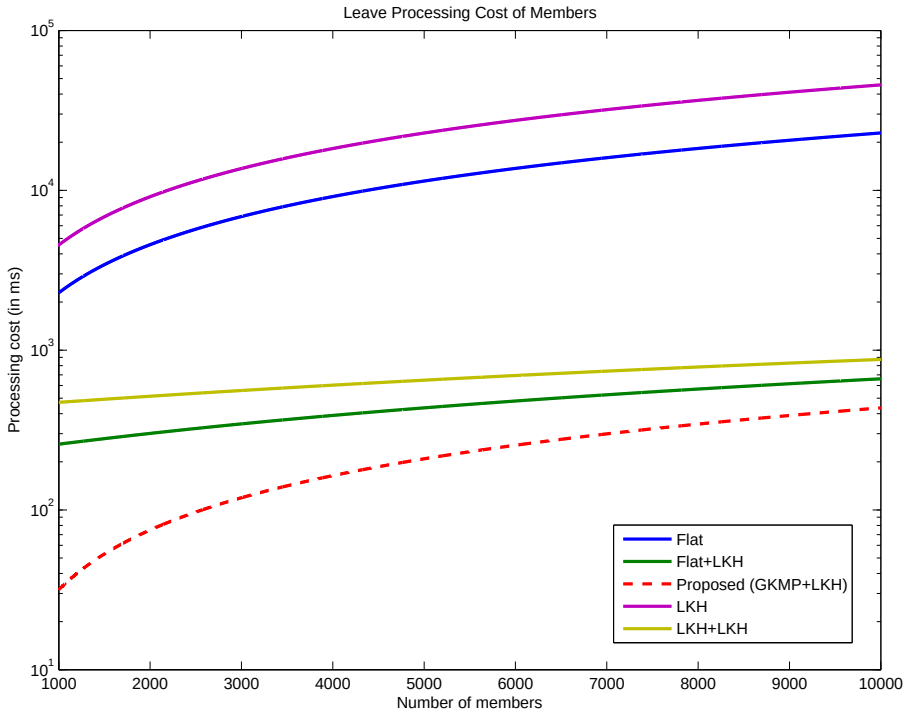


Figure 5.14. Leave processing costs for Members

agement schemes are the most efficient schemes among others. Since processing cost is calculated the total number of encryption, decryption and key generation made by all KDCs or members, and during initialization, the number of distributed encrypted keys in LKH greater that $GKMP$ and $Flat$, this is a result that we expect. We state the results of processing costs of join and leave for KDC and members in Figures 5.11, 5.12, 5.13 and 5.14 respectively. The simulation results of processing costs for join operations (for KDC and members separately) show that the most effective key management scheme is the $GKMP$ followed by our proposed scheme $GKMP+LKH$. Since $GKMP$ could not provide forward secrecy, this scheme is not a proper one for highly dynamic Communication Tier 2. Processing costs for leave operation points out that the most efficient scheme is or proposed scheme. Therefore, we take the join processing efficiency of $GKMP$ by applying it to the highly static Communication Tier 1. Since the $GKMP$ scheme does not take any action when a member leaves the group, this scheme is excluded from the leave processing calculation (since the cost is zero). The simulation result of processing cost of leave operation (for KDC and members separately) points out that the most efficient key management scheme is our

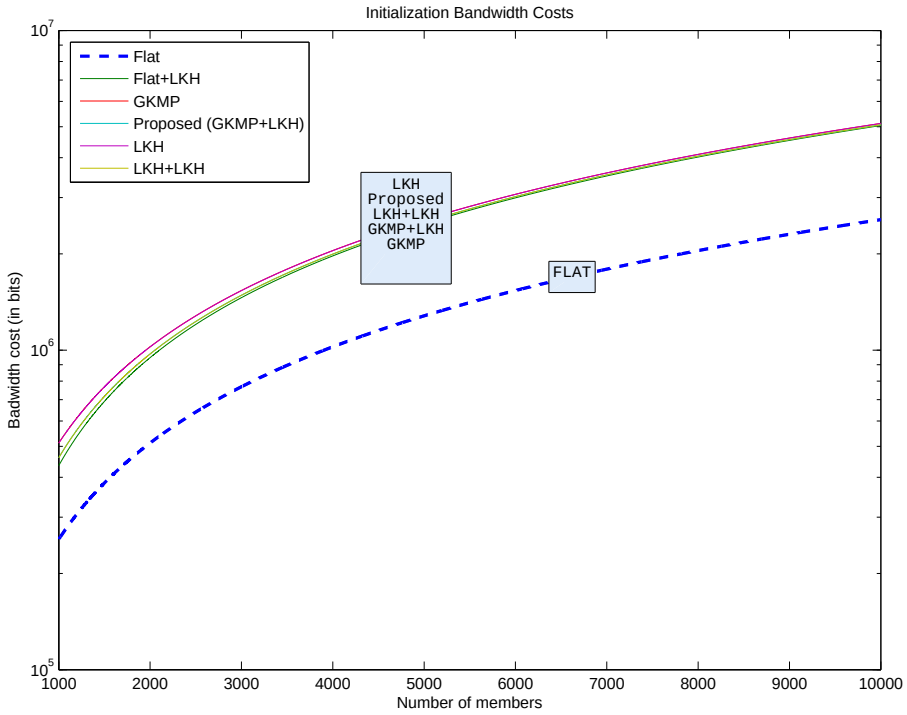


Figure 5.15. Initial bandwidth costs of key management schemes

proposed model $GKMP+LKH$. Since $GKMP$ can not provide forward secrecy, there is not any operation taken after a leaving occurs. Again, by applying this scheme to Communication Tier 1 in which leaving a member does not occur, we construct the most efficient scheme in terms of processing cost.

The results of bandwidth costs for initialization, join and leave operation are shown in Figures 5.15, 5.16 and 5.17 respectively. For initialization bandwidth cost the most efficient key management scheme is the $Flat$. Since for the $GKMP$ and LKH, the number of transferred keys for each member is greater that than transferred in $Flat$, the result of this simulation is not a surprising one. The bandwidth cost for join operation shows that the most effective scheme is $GKMP$ followed by our proposed scheme $GKMP+LKH$. Since $GKMP$ could not provide forward secrecy, this scheme is not a proper one for highly dynamic Communication Tier 2. Therefore, we take the join bandwidth efficiency of $GKMP$ by applying it to the highly static Communication Tier 1 and LKH to the highly dynamic Communication Tier 2.

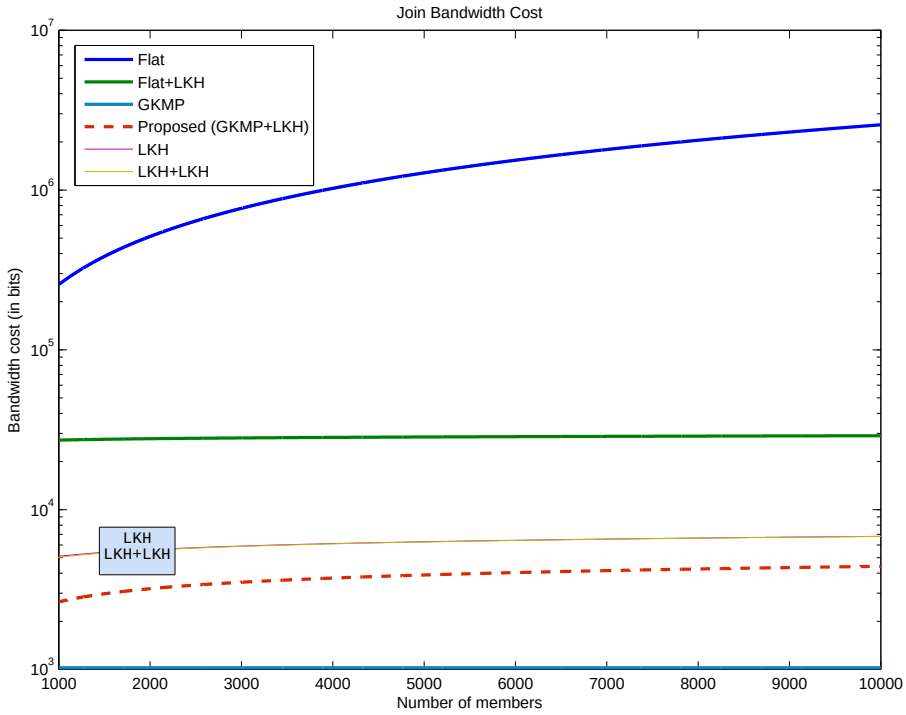


Figure 5.16. Join bandwidth costs of key management schemes

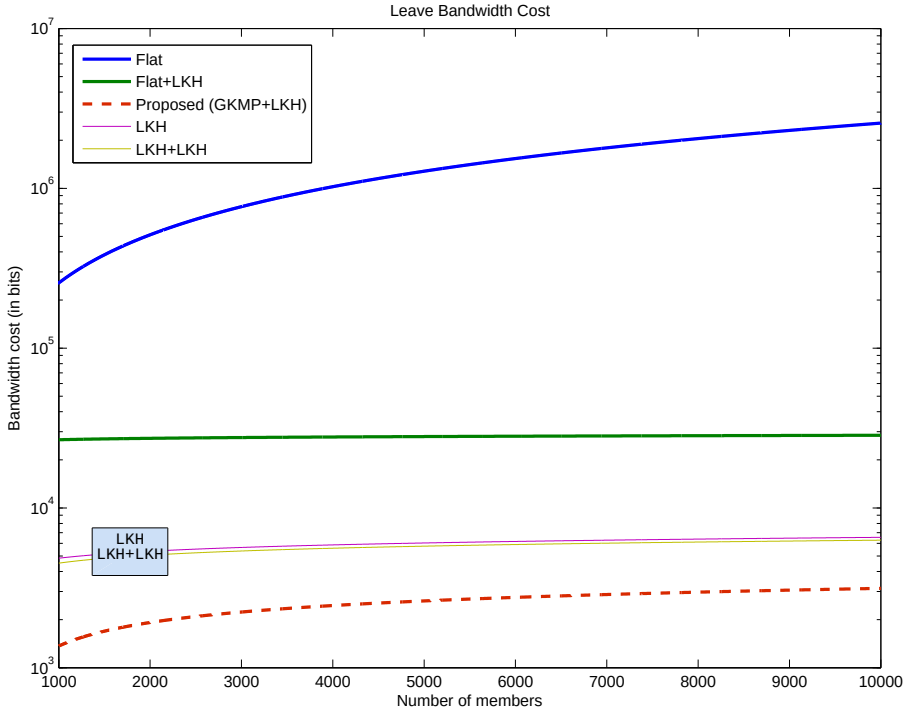


Figure 5.17. Leave bandwidth costs of key management schemes

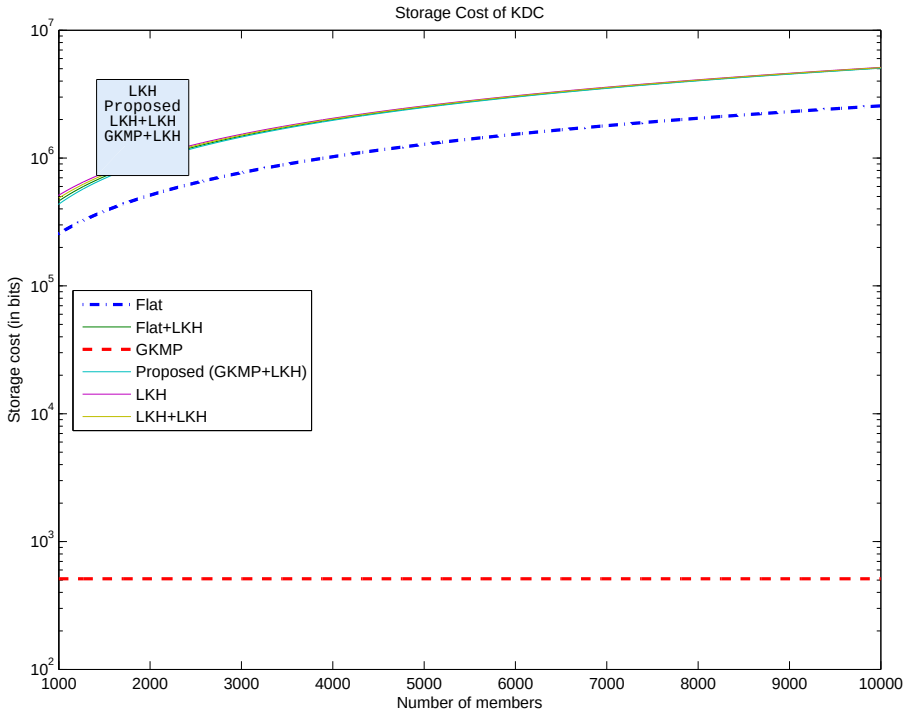


Figure 5.18. Storage costs for KDC

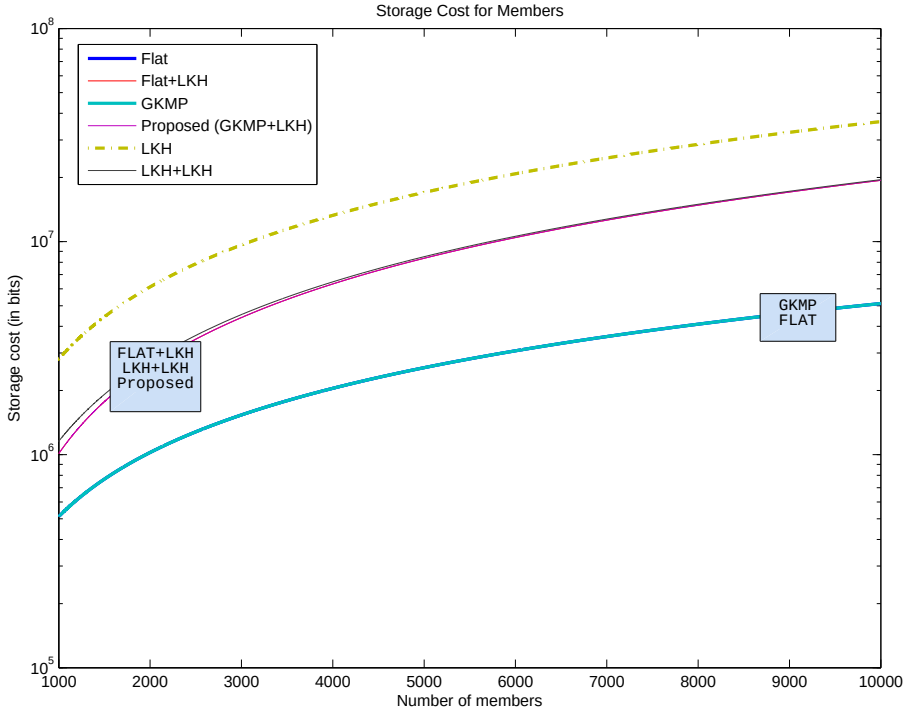


Figure 5.19. Storage costs for Members

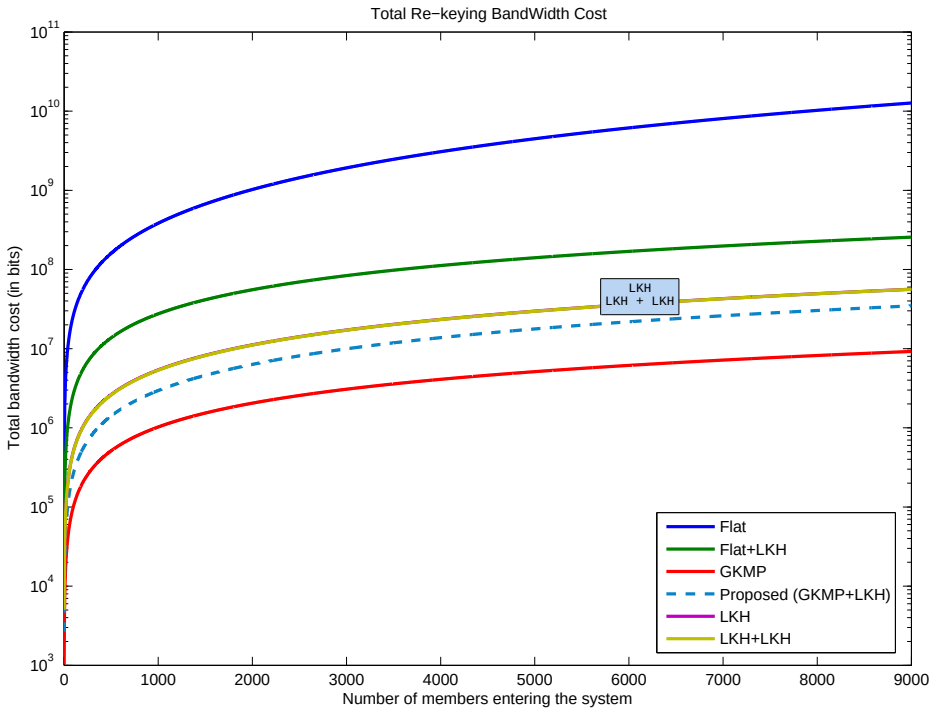


Figure 5.20. Total Re-Keying Bandwidth Cost

Since the $GKMP$ scheme does not take any action when a member leaves the group, this scheme is excluded from the leave processing calculation (since the cost is zero). The bandwidth cost for leave operation shows that the most effective scheme is the proposed $GKMP + LKH$. followed by LKH and $LKH + LKH$ where the worst scheme is $Flat$. Since $GKMP$ can not provide forward secrecy, there is not any operation taken after a leaving occurs. Therefore, bandwidth cost of $GKMP$ is zero. Again, by applying this scheme to Communication Tier 1 in which leaving a member does not occur, we construct the most efficient scheme in terms of bandwidth cost.

The results of storage costs for all KDCs and members, are shown in Figure 5.18 and 5.19 respectively. In terms of the storage cost for all KDCs, the most efficient scheme is $GKMP$ followed by $Flat$. The cost of other schemes are close to each other. Since $GKMP$ can not provide the forward secrecy which is a dramatic situation for highly dynamic Communication Tier 1, and the bandwidth and processing efficiency for join/leave operations of the $Flat$ scheme is the worst one among others, we decide the use the $GKMP + LKH$ scheme for our network model.

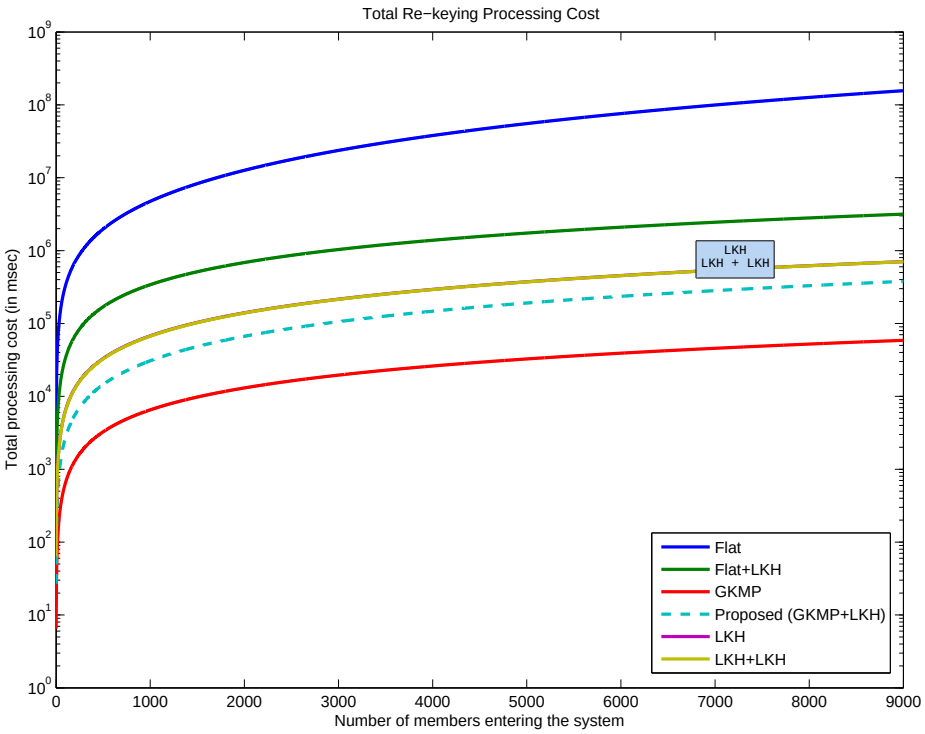


Figure 5.21. Total Rekeying Processing Cost

We also investigate the total bandwidth and processing costs for re-keying of the group keys under varying number of entering CRs the network. The bandwidth and processing results are shown in 5.20 and 5.21 respectively. The total bandwidth and processing cost points out that under varying number of CRs entering the network, the $GKMP$ scheme is the most effective followed by the proposed scheme ($GKMP + LKH$).

5.3.2. Cryptographic Algorithms - Performance Analysis

Design choices for securing a system affect performance, scalability and usability. There is usually a tradeoff between security vs. performance and usability. The more secure a system is, the more you have compromised in terms of performance and usability. Before designing a secure system for satellite assisted CRN, first we have determined all the possible (based on our knowledge) threats in Section, vulnerabilities 4.2, we try to choose the techniques to implement security based on threat mitigation first and performance second.

Table 5.6. Comparable key sizes for equivalent security levels

Security Level	Symmetric	ECC	DSA/RSA
80	80	160	1024
112	112	224	2048
128	128	256	3072
192	192	384	7680
256	256	512	15360

Spectrum sensing and decision threat analysis mentioned in Section 4.2, points out that confidentiality, entity and data origin authentication, cryptographic nonce and integrity services are needed to be employed in order to provide a robust security structure. We consider and apply all these cryptographic services in cryptographic structure design of each communication tier (Tier 1 and 2). By employing these cryptographic services, we try to overcome possible security threat which are mentioned in Section 4.2 and shown in Table 4.3 and Table 4.4.

This thesis follows NIST and ANSI in fixing five security levels: 80, 112, 128, 192, and 256 bits. The protection lifetimes of security levels have been extrapolated from similar NIST recommendations. The extrapolations are also based on a simple assumption similar to Moore's law: computing power will grow by a factor of about 216 every decade. Therefore, the minimum adequate security level must increase by 16 bits every 10 year. The comparable key sizes for equivalent key security levels shown in Table 5.6.

We begin with the comparison of the various symmetric data encryption algorithms. We use the performance evaluations results in [28]. This work provides evaluation of six of the most common encryption algorithms namely: AES, DES,3DES, RC2, Blowfish, and RC6. We only consider four data encryption standards: DES, 3DES, Blowfish and AES. DES was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES has 56 bits key size with 64 bits block size . Many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [29]. 3DES is an enhancement of DES. It has

Table 5.7. Execution times (in ms) of encryption with different packet size

Input size in (Kbytes)	AES	3DES	DES	Blowfish
49	56	54	29	36
59	38	48	33	36
100	90	81	49	37
247	112	111	47	45
321	164	167	82	45
694	210	226	144	46
899	258	299	240	64
963	208	283	250	66
5345.28	1237	1466	1296	122
7310.336	1366	1786	1695	107
Average Time	374	452	389	60.3
Throughput (Mb/sec)	4.174	3.45	4.01	25.892

64 bit block size with 168 bits key size. Blowfish is block cipher 64-bit block with variable length key, ranging from 32 bits to 448 bits and has variants of 14 rounds or less. AES has 128 bit block-size with variable key length of 128,192, or 256 bits. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

We only focus on the comparison based on the throughput of the encryption algorithm. The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm. As the throughput value is increased, the power consumption of this encryption technique is decreased. Since AES and Blowfish have variable key sizes, we need to note that in the throughput and power consumption simulation result achieved in [28], the key size for these algorithms are taken as 256 bits for AES and 128 bits for Blowfish.

Performance evaluations results in Table 5.7 and Table 5.8 which are cited from [28] show that the most efficient data encryption algorithm in terms of throughput and power consumption, is Blowfish and AES has an advantage over 3DES, DES. 3DES has low performance in terms of power consumption and throughput when compared with

Table 5.8. Execution times (in ms) of decryption with different packet size

Input size in (Kbytes)	AES	3DES	DES	Blowfish
49	63	53	50	38
59	58	51	42	26
100	60	57	57	52
247	76	77	72	66
321	149	87	74	92
694	142	147	120	89
899	171	171	152	102
963	164	177	157	80
5345.28	655	835	783	149
7310.336	882	1101	953	140
Average Time	242	275.6	246	83.4
Throughput (Mb/sec)	6.452	5.665	6.347	18.72

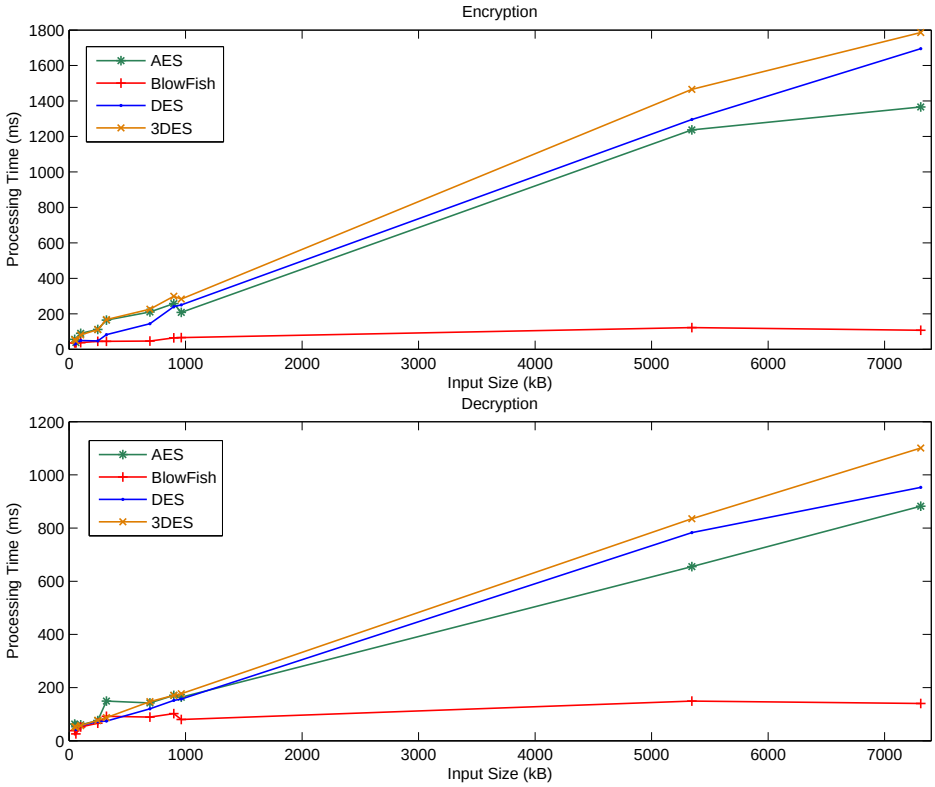


Figure 5.22. Execution times of encryption/decryption algorithms

DES. It requires always more time than DES because of its triple phase encryption characteristics.

We construct two performance evaluation graphics one for encryption and one for decryption (Figure 5.22). The graphics construct the calculated processing times for variable length of packet size which are shown in Table 5.7 and Table 5.8. The performance evaluation graphics show that the Blowfish data encryption algorithm has the best performance among DES,3DES and AES. Since there is no effective cryptanalysis on the full-round (16 round) version of Blowfish algorithm known publicly, we decide to use the Blowfish algorithm as the data encryption algorithm in or security structure.

The selection of the mode of operation for the selected block cipher is also a critical decision. NIST recommendation [25] defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). The simplest of the encryption modes is the electronic codebook (ECB) mode. The message is divided into blocks and each block is encrypted separately. The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all. In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block. CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential (can not be paralleled). A one-bit change in a plaintext affects all following ciphertext blocks.

The cipher feedback (CFB) mode makes a block cipher into a self-synchronizing stream cipher. Like CBC mode, changes in the plaintext propagate forever in the ciphertext, and encryption cannot be parallelized. The OFB mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then

XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. The CTR also turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a counter. The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time. In our security solution we decide to use CBC mode of operation. Since the transferred has not to have a high data rate, there is no need to be paralleled. In [26], there exist a one recommendation about CBC mode of operation about probability that at least one collision will occur depends mostly on the message span of the key(encrypted block of messages by using the same key) relative to the block size, b, of the underlying block cipher. For Blowfish, a collision is expected to exist among a set of $2^{b/2}$ arbitrary messages; in other words, 2^{64} messages for the Blowfish algorithm (32 GigaByte). Therefore, we assume that all keys are re-keyed regularly (before the message span reaches 16 GigaByte) to avoid a collision occurs.

We use public-key cryptography in Communication Tier 1 for providing message authentication in join operation and spectrum decision sensing. For the performance and security evaluation we examine RSA and ECDSA [30, 31] digital signature algorithms. Comparable key sizes for equivalent security levels of these algorithms are shown in Table 5.6 whic is cited from [31]. For the same level of resistance against the best known attacks, the system parameters for an elliptic-curve-based system can be chosen to be much smaller than the parameters for RSA. This comes with some advantages ECDSA over RSA like greater speed and less storage. The main drawback of ECDS underlies the selection of an appropriate ecliptic curve. This drawback by using the curves which are approved by NIST. Because of the processing and storage advantages of ECDSA over RSA, we decide use ECDSA in our security structure.

We decide use a hash function from the SHA-2 family. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 con-

sists of set of four hash functions with different digest sizes, with 224, 256, 384 or 512 bits respectively. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable [32]. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been extended to SHA-2 [33].

5.3.3. Cryptographic Protocols and Structural Design - Performance Analysis

We divide our network model into two communication tiers: (1) communication group of Satellite and BSs, and (2) communication group of BSs and CPEs. Separating communication into two different tiers improves system-wide performance and security by giving a chance to apply different security structure to networks with different kinds of constraints. Satellites have some storage, processing and bandwidth usage constraints, while CR nodes have some constraints because of their dynamic nature. By dividing the networks into two communication tier, we could apply symmetric cryptographic structure and an appropriate key management scheme which suits static nature of the Communication Tier 1, and an hybrid cryptographic structure and an appropriate key management scheme which suits dynamic nature of the Communication Tier 2. Two communication tier of our proposed network is shown in Figure 5.2.

First of all we consider if this two-tiered structural design is efficient that a single-tiered one or not. Since employing asymmetric techniques in cryptographic protocols of Communication Tier 2 is a necessity in order to simplify initial key distribution, and provide non-repudiation for some messages, we compare our actual design with the one in which the cryptographic protocols of Communication Level 2 is used for entire network. The common protocol that we used in Tier 1 and Tier 2 is Join Network. We compare Tier 1 and Tier 2 join operations by bandwidth and processing cost. In comparison, we use the bandwidth and processing cost calculations which are shown in Table 5.9. Figure 5.23 gives the comparison results for join operation cost of Tier 1 and Tier 2. The results state that Tier 1 structure much more efficient than the Tier 2. Therefore extending the cryptographic solution of Tier 2 to entire network is not an

Table 5.9. Bandwidth and Processing Costs of Tier 1 and Tier 2

Cost				
Tier 1		Tier 2		
Join	Sensing	Join	Sensing	Handover
$4R+I+5ID+4M+2K+1$	$2ID + 2t_s + 2M + s + d$	$2a^x + 2S + 2ID + 4R + (d_N+1)K+2H$	$2ID + 2t_s + M + S + s + d$	$2ID + 2t_s + Req + d_N + S$
Processing Cost				
Tier 1		Tier 2		
Join	Sensing	Join	Sensing	Handover
$2R+8M+3E+3D$	$2E+2D+2R+4M$	$2U+2R+4H+2S+2V_S+(3+d_N)E + (3 + d_N)D$	$2E+2D+M+V_M+2R+S+V_S$	$(1 + d_N)(E + D)+M+V_M+S+V_S$

efficient solution.

In Communication Tier 2 security structure, we modify the Station-to-Station protocol, which is used for establishing a session key by providing non-repudiation and entity authentication security services. We add two random numbers in this protocol in order to construct a KEK which is used in transferring the other keys which are used in this security structure. One option that once we establish a session key, we re-establish a key (KEK) by using symmetric key establishment technique. The symmetric key establishment technique mentioned here is a technique like the one using in Tier 1 join protocol. This option adds three additional messages in our protocol. In a highly dynamic network like we proposed, three additional message in join protocol cause severe bandwidth and processing costs. Therefore, we decide to use the modified version of Station-to-Station protocol.

As stated our network model is divided into cells which contain a BS and mobile CR nodes. Therefore these mobile nodes can easily switch between network cells. We assume that each BS sends information of new nodes including their encryption, key encryption and MAC keys to its neighbor BSs. Therefore nodes do not have to establish

Table 5.10. Notations in Table 5.9

R	random number generation cost and size of random number
I	Size of SAT-BS pre-shared key index
ID	Size of ID of all members
K	size of keys
t_s	Size of timestamps
M	MAC generation and size of MAC
s	Size of spectrum sensing data
d	Size of spectrum decision data
a^x	size of Diffie-Hellman parameter
S	Signature generation and size of signature
d_N	Depth of the LKH tree where N is the number of member
H	Hash generation and size of hash
E	Encryption cost
D	Decryption cost
U	Exponentiation cost
V_S	Verification of signature
V_M	Verification of MAC
Req	Size of handover request

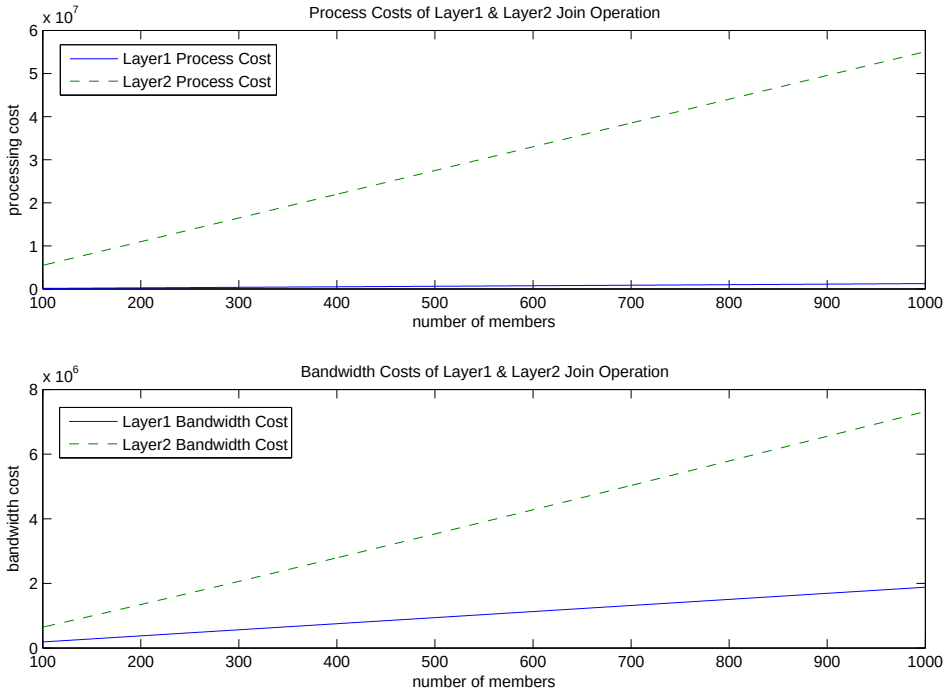


Figure 5.23. Processing and bandwidth costs of Tier 1 and Tier 2 join operations

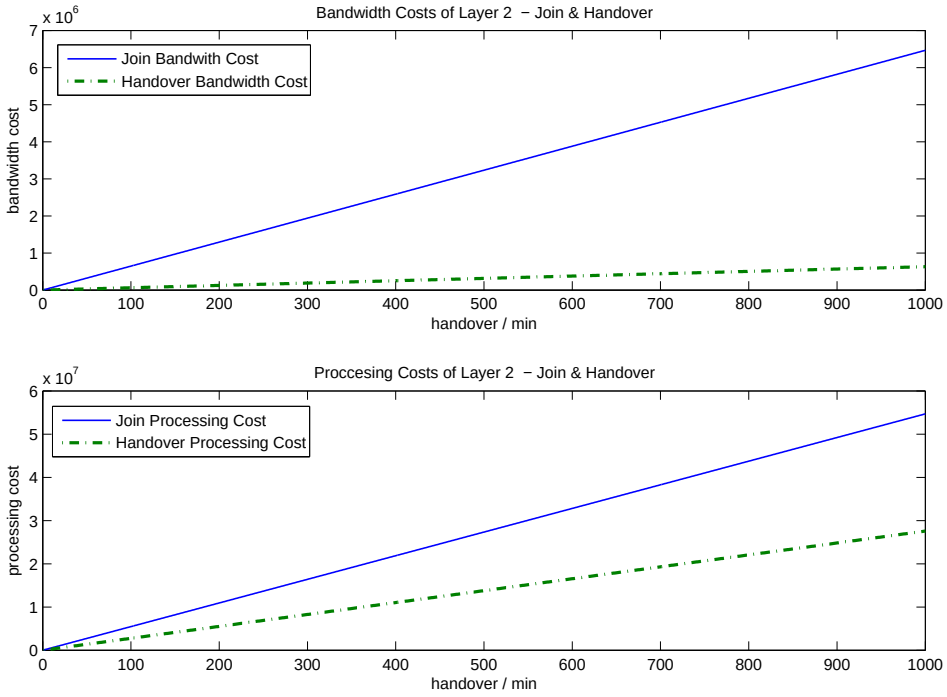


Figure 5.24. Join vs. Handover Bandwidth and Processing Cost

join protocol, each time they cross into a new cell. CR node, crosses into a new cell, sends a request to new BS in order to obtain group keys. The alternate solution is that whenever a CR node crosses into a new network cell, CR Node and BSs establish the join protocol.

In terms of bandwidth usage and processing costs our solution is more efficient than the alternate solution. The main drawback of our solution is the storage cost. Since each BS sends information of new nodes including their encryption, key encryption and MAC keys to its neighbor BSs, each BS has to store information of CR Nodes in neighbor cells besides information of its CR nodes. We assume that the storage capacity of BSs could be adapted to our solution. These adaptation is easy, because of the static nature and huge space capacity of BSs. Figure 5.24 shows the bandwidth and processing costs of cell handover where Tier 2 join or handover protocol applied. As the number of handover node in a minute is increase, the bandwidth and processing cost of handover which applying join protocol, is also dramatically increase. Therefore, instead of applying the join protocol shown in Figure 5.5, applying the handover

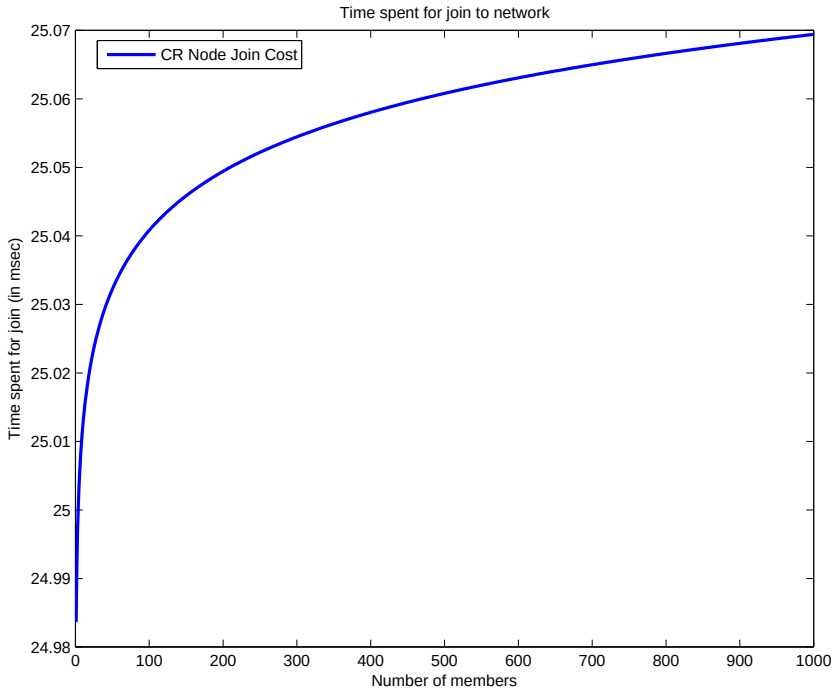


Figure 5.25. Total time spent during join protocol

protocol presented in Figure 5.7 is an efficient way.

We also investigate the total time spent(in msec) during the joining procedure of a CR node. We use the benchmark results of Crypto++ 5.6 Library [34] which includes different symmetric and asymmetric cryptographic algorithms and hash functions. The Crypto++ 5.6 Library benchmarks are computed by taking the geometric mean of the number of MB/second of each cipher, hash function, and MAC, and operations/second of each asymmetric. The join protocol of CR nodes includes symmetric encryption, DH key-pair generation, ECDSA signature generation, ECDSA signature verification and hash function. Total time spent for join protocol of CR nodes is analyzed under varying number of CR nodes in the network (1 to 1000). Results are shown in Figure 5.25.

6. CONCLUSION AND FUTURE DIRECTION

CRs are proposed as a solution to inefficient utilization of the overcrowding spectrum and opening space for the new wireless communication technologies. CRs have the ability to monitor the spectrum activities and decide on the best transmission channel depending on the measurements; thereby provide agility in spectrum access. While a traditional radio allows minimal user interaction and has unalterable receiver transmitter operations, the CRs have advanced functionalities of remote reconfigurability, spectrum sensing, spectrum decision and primary user detection. These new functionalities open new denial of service vulnerabilities. Therefore the security solutions given in the field of CRNs are mainly based on these new denial of service vulnerabilities.

In this thesis, we study on the security aspects of a satellite assisted CRN which is an infrastructured-based CRN that is controlled by a satellite. This architecture enables easy and efficient management of policy/software updates due to satellite's inherent coverage region. We focus on possible security threats of this architecture, and give their risk analysis and countermeasures. PUE, eavesdropping, traditional jamming, faulty data injection, intentional/non-intentional modifications and replay attack are the input of our threat analysis. Threat analysis points out that confidentiality, entity and data origin authentication, cryptographic nonce and integrity services are fundemental in order to provide a robust security structure. Therefore, we consider and apply all these cryptographic services in our security structure designed for spectrum sensing and decision procedure.

We divide our network model into two communication tier. Communication Tier 1 includes Satellite and BSs where Communication Tier 2 includes BSs and CPEs. Separating communication network into two different tiers improves system-wide performance and security by giving a chance to apply different security structures to networks with different kinds of constraints. Satellites have some storage, processing and bandwidth usage constraints, while CR nodes have some constraints because of their dynamic nature. By dividing the networks into two communication tier, we could

apply symmetric cryptographic structure and an appropriate key management scheme which suits static nature of the Communication Tier 1, and an hybrid cryptographic structure and an appropriate key management scheme which suits dynamic nature of the Communication Tier 2.

Finally, we give detailed performance analysis of structural design, key management techniques, cryptographic algorithms and protocols. In order to give an appropriate decision about employed group key management techniques, we evaluate performance analysis for different group key management approaches. The key performance metrics of group key management techniques are bandwidth usage, processing and storage requirements. This performance evolution points out that, GKMP key management scheme is a suitable scheme for Communication Tier 1 where LKH is suitable for Tier 2. Cryptographic algorithms used in our security structure are also examined by their processing costs and compared with the alternate algorithms. The efficiency of the proposed two-tiered structural design is examined by comparing with an alternate solution in terms of bandwidth and processing costs. The comparison results state that our structural design is more efficient that the alternate one. Bandwidth and processing costs of proposed protocol are calculated and compared with other possible solutions.

Further work includes examining possible counter-attacks against the proposed security structure, and giving their counter-measures in order to provide more robust security structure. Since satellite networks have some severe constraints, as a future work more efficient security structure solutions for spectrum sensing and decision protocol can be investigated. Beside spectrum sensing and decision procedure, an efficient security solution can be given for the other procedures of CRNs like spectrum mobility and coexistence.

REFERENCES

1. Bayhan, S., G. Gur, and F. Alagoz, "Satellite Assisted Spectrum Agility Concept", *Proc. MILCOM'07*, pp. 1–7, 2007.

2. "Cognitive Radio Definitions", http://www.sdrforum.org, 2007.

3. Hossain, E., D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*, Cambridge University Press, 2009.

4. "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1", Technical report, 2006, `http://dx.doi.org/10.1109/IEEESTD.2006.99107`.

5. Mahmoud, Q., *Cognitive Networks Towards Self-Aware Networks*, Wiley, 2007.

6. Menezes, A., P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography. 2001*, CRC Press, Florida.

7. Rafaeli, S. and D. Hutchison, "A survey of key management for secure group communication", *ACM Comput. Surv.*, Vol. 35, No. 3, pp. 309–329, 2003.

8. Brown, T. and A. Sethi, "Potential cognitive radio denial of service attacks and remedies", *Proceedings of the international symposium on advanced radio technologies*, pp. 26–28, 2007.

9. Clancy, T. and N. Goergen, "Security in cognitive radio networks: Threats and mitigation", *International Conference on Cognitive Radio Oriented Wireless Networks and Communications (Crowncom'08)*, 2008.

10. Burbank, J., "Security in cognitive radio networks: The required evolution in

approaches to wireless network security", *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008.*, pp. 1–7, 2008.

11. Bian, K. and J.-M. J. Park, "Security vulnerabilities in IEEE 802.22", *WICON'08: Proceedings of the 4th Annual International Conference on Wireless Internet*, pp. 1–9, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 2008.

12. Brown, T. and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment", *Mobile Networks and Applications*, Vol. 13, No. 5, pp. 516–532, 2008.

13. Anand, S., Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks", *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2008)*, pp. 1–6, October 2008.

14. Chen, R., J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks", *IEEE Journal on Selected Areas in Communications*, Vol. 26, No. 1, pp. 25–37, 2008.

15. Jin, Z., S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks", *IEEE Intl. Conf. on Commun.(ICC'2009)*, 2009.

16. Mathur, C. and K. Subbalakshmi, "Digital Signatures for Centralized DSA Networks", *4th IEEE Consumer Communications and Networking Conference, 2007. CCNC 2007*, pp. 1037–1041, 2007.

17. Schneier, B., *Applied cryptography: protocols, algorithms, and source code in C*, Wiley-India, 2007.

18. Jakimoski, G. and K. Subbalakshmi, "Towards secure spectrum decision", *IEEE*

International Conference on Communications, Symposium on Selected Areas of Communication, 2009.

19. Jakimoski, G. and K. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks", *CogNets Workshop, IEEE International Conference on Communications Workshops*, pp. 524–528, 2008.

20. "Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis. Technical Specification ", Technical Report ETSI TS 102 165-1 V4.1.1, ETSI, 2003.

21. Ersöz, S. D., S. Bayhan, and F. Alagöz, "Secure spectrum sensing and decision in cognitive radio networks", *Springer (LNCS) in Communications in Computer and Information Science (CCIS) Series*, 2010, accepted.

22. Rui-liang, C., J. Park, Y. Hou, *et al.*, "Toward secure distributed spectrum sensing in cognitive radio networks", *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 50–55, 2008.

23. Stanley, D., J. Walker, and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017 (Informational), March 2005, `http://www.ietf.org/rfc/rfc4017.txt`.

24. Harney, H. and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture", RFC 2094 (Informational), March 1997, `http://www.networksorcery.com/enp/rfc/rfc2094.txt`.

25. Dworkin, M., N. I. of Standards, and T. (U.S.), *Recommendation for block cipher modes of operation [electronic resource] : methods and techniques / Morris Dworkin*, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology : For sale by the Supt. of Docs., U.S. G.P.O., Gaithersburg, MD :, 2001 ed. edition, 2001.

26. Dworkin, M., N. I. of Standards, and T. (U.S.), *Recommendation for block cipher modes of operation [electronic resource] : the CMAC mode for authentication / Morris Dworkin*, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg, MD :, 2005.

27. Arslan, M. and F. Alagoz, "Security issues and performance study of key management techniques over satellite links", *11th Intenational Workshop on Computer-Aided Modeling, Analysis and Design of Communication Links and Networks*, pp. 122–128, 2006.

28. Elminaam, D. S. A., H. M. A. Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", *International Journal of Network Security*, Vol. 10, No. 3, pp. 213–219, 2010.

29. Coppersmith, D., "The Data Encryption Standard (DES) and Its Strength Against Attacks.", *IBM Journal of Research and Development*, pp. 243–250, 1994.

30. "SEC 1: Elliptic Curve Cryptography", Technical report, 2009.

31. Vanstone, S., "Next generation security for wireless: elliptic curve cryptography", *Elsevier*, pp. 412–415, 2003.

32. Schneier, B., "Cryptanalysis of SHA-1", February 2005, `http://www.schneier.com`.

33. Wikipedia, "SHA-2", April 2010, `http://en.wikipedia.org`.

34. Dai, W., "Crypto++", September 2009, `http://www.cryptopp.com/benchmarks.html`.