A Hierarchical Structure towards Securing Data Transmission in Cognitive Radio Networks

By

Mahmoud Khasawneh

A Thesis

In the Department

Of

Electrical and Computer Engineering

presented in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy (Electrical and Computer Engineering) at

Concordia University

Montreal, Quebec, Canada

August, 2017

CONCORDIA UNIVERSITY
SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: Mahmoud Khasawneh

Entitled: A Hierarchical Structure towards Securing Data Transmission
in Cognitive Radio Networks

and submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY (Electrical and Computer Engineering)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Chair
Dr. Luis Amador

External Examiner
Dr. Michel Kadoch

External to Program
Dr. Mourad Debbabi

Examiner
Dr. Yousef Shayan

Examiner
Dr. Dongyu Qiu

Thesis Supervisor
Dr. Anjali Agarwal

Approved by

Dr. Wei-Ping Zhu, Graduate Program Director
Chair of Department or Graduate Program Director

17/08/2017

Dr. Amir Asif, Dean, Faculty of Engineering and Computer Science
Dean of Faculty

Abstract

A Hierarchical Structure towards Securing Data Transmission in Cognitive Radio Networks

Mahmoud Khasawneh, Ph.D.

Concordia University, 2017

Cognitive Radio (CR) technology is considered as a promising technology to overcome spectrum scarcity problem in wireless networks, by sharing the spectrum between both unlicensed users (secondary users, (SUs)) and licensed users (primary users, (PUs)), provided that the SUs respect the PUs’ rights to use the spectrum exclusively.

An important technical area in cognitive radio networks (CRNs) is wireless security. A secure CRN must meet different security requirements, which are: confidentiality, integrity, availability and authentication. Data confidentiality is a mandatory requirement in cognitive radio networks, generally to maintain the privacy of the data owner (PU or SU). Integrity means that data is transmitted from the source to the destination without alteration. While availability is to release the channels assigned to one SU as soon as a PU wants to use its spectrum. Authentication in CRN means that each node has to authenticate itself before it can use the available spectrum channels.

New classes of security threats and challenges in CRNs have been introduced that target the different layers of OSI model and affect the security requirements. Providing strong security may prove to be the most difficult aspect of making CR a long-term commercially-viable concept. Protection of routes used for data transmission is a critical prerequisite to ensure the robustness of the routing process. Therefore, route discovery must be done in such a way that lets each node find the best secure path(s) for its data transmission.

In this work, network security of CRN is improved through proposing different models that are built to fulfil the security requirements mentioned above. Improving the network security enhances the network performance, taking into consideration the quality of service (QoS) desired by the different network nodes such as bandwidth and time delay. This work aims to combine the spectrum sensing phase and the spectrum management phase, as well as to detect all the adversary nodes that slow down the network performance by selectively holding and not forwarding packets to their next hop(s). We measure the network node's reliability for using network resources through a value called belief level (BL), which is considered as the main parameter for our entire work. BL is used to monitor the nodes' behavior during the spectrum sensing phase, and then it is used to form the best path(s) during the spectrum management phase. Particularly, this work follows a hierarchical structure that has three different layers. At the bottom layer, a novel authentication mechanism is developed to fulfil the authentication and the availability security requirements, which ends assigning a belief level (BL) to each node. At the middle layer, the nodes' behavior during the spectrum sensing phase is monitored to detect all the adversary node(s). Finally, at the top layer, a novel routing algorithm is proposed that uses the nodes' security (BL) as a routing metric. SUs collaborate with each other to monitor other nodes' behavior. Users' data confidentiality and integrity are satisfied through this hierarchical structure that uses the cluster-based, central authority, and nodes collaboration concepts. By doing so, the traffic carried in the CRN is secured and adversary nodes are detected and penalized.

Acknowledgement and/or Dedication

All praises be to “ALLAH” Almighty who enabled me to complete this task successfully and my utmost respect to His Last Prophet Mohammad (S.A.W.). This thesis would have never been completed without the will and blessing of Allah, the most gracious, the most merciful. AL HAMDU LELLAH. First of all, I thank my family for their constant moral support and their prayers. They are the people who are the closest to me and suffered most for my higher study abroad. Their support was invaluable in completing this thesis. Next, my gratitude to my supervisor Prof. Anjali Agarwal, whose constant encouragement and guidelines at each step made this thesis possible. I am very grateful for her motivation and support throughout this endeavor. Deepest thanks also to the committee members for their advices and suggestions regarding the thesis and beyond. Moreover, I would also like to express my appreciation to NSERC – Natural Sciences and Engineering Research Council of Canada to whom I am grateful for providing me the financial support. I dedicate this thesis to every one of my relatives who sadly passed away during my studies. They looked forward to seeing me finishing my Master’s and Ph.D. degrees and becoming a university professor. I would like to thank my wife Alaa, and my little princess Sham for standing beside me throughout my study. They have been my inspiration and motivation for continuing to improve my knowledge and finish my study. They always make me smile and understand on those weekend mornings when I was going to the university instead of hanging out with them.

Last but not least, I will not forget my soulmate friend, Saed Alrabaee, for motivating and encouraging me in my many moments of crisis. Your friendship makes my life a wonderful experience.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

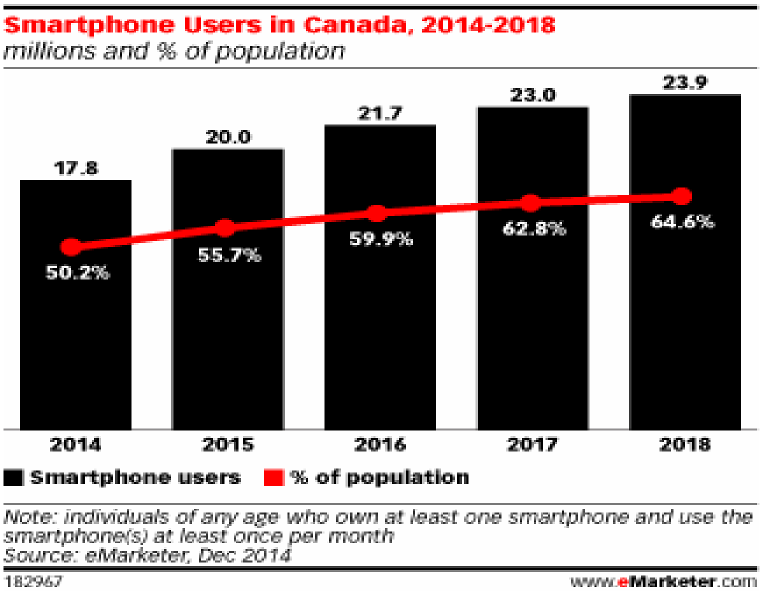
BL	Belief Level
CH	Cluster Head
CR	Cognitive Radio
CRNs	Cognitive Radio Networks
DoS	Denial of Service
FC	Fusion Center
PK	Primary Key
PU	Primary User
PUEA	Primary User Emulation Attack
QoS	Quality of Service
RD	Reported Node
RG	Reporting Node
SK	Symmetric Key
SR	Sensing Result
SSDFA	Spectrum Sensing Data Falsification Attack
SU	Secondary User
WSNs	Wireless Sensor Networks

Chapter 1: Introduction

Since 2000, the number of subscriptions for commercial mobile services in Canada has more than tripled, increasing by an average of 1.5 million per year over the last decade [1]. In fact, the increase in mobile subscriptions has been accompanied by the adoption of more sophisticated mobile devices, such as smart phones and tablets, which provide access to the Internet. Canadians are among the most ardent adopters of these types of devices. Figure 1.1 shows the number of smart phone users compared to the number of population in Canada for the period of 2014-2018 [2]. It is projected that by 2018, about two thirds of Canadians will be using smart phones. The number of mobile internet subscriptions in Canada has already increased from 3.8 million in 2011 to around 14 million in 2015. In fact, the Cisco Visual Networking Index [3] has shown that by the end of 2013, the number of mobile-connected devices has already exceeded the world's population, and that by 2017, video content will represent sixty-six percent of total mobile traffic.

Spectrum is a limited resource, and the "usable" spectrum range (given current technologies) is completely allocated to existing services. As a result, Canada must rely on a combination of demand-side and supply-side measures in order to meet the spectrum needs of new or growing services.

On the supply-side, the supply of spectrum has to be managed by reallocating limited spectrum resources between radio services. On the demand-side, licensees must use existing spectrum allocations more efficiently in order to provide improved service without requiring additional spectrum resources. Improved efficiency of spectrum use can be achieved by optimizing infrastructure deployment (for example, increasing network density in order to increase frequency reuse) or by adopting innovative technologies (such as 5G wireless mobile broadband technologies or Cognitive Radio (CR) technology). Figure 1.2 illustrates the rapid spectrum demand to support commercial use in Canada for the period of 2011-2017.


Smartphone Users in Canada, 2014-2018

millions and % of population

Note: individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month

Source: eMarketer, Dec 2014

Figure 11.1: Smartphone Users in Canada (2014-2018) [2]

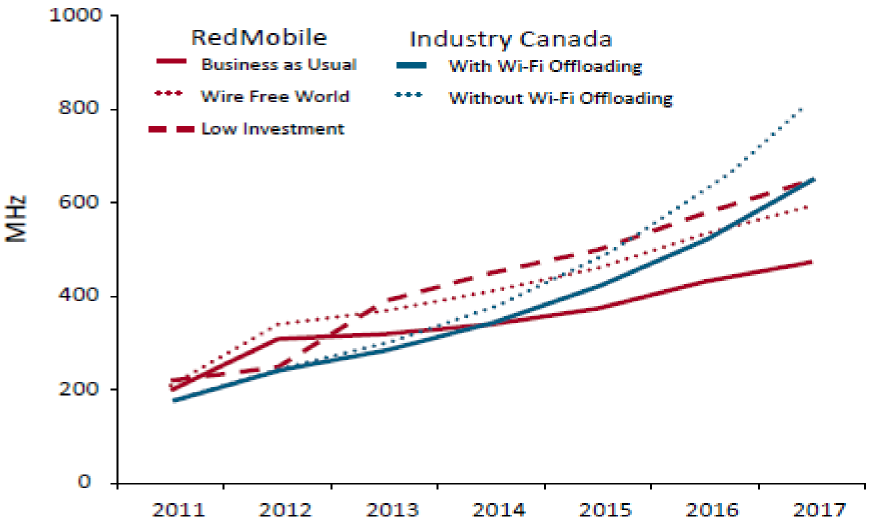


Figure 1.2: Spectrum Demand to Support Commercial Use for 2011-2017 in Canada [1]

In order to increase the spectrum utilization in an efficient way, new spectrum sharing models must be produced that allow sharing the spectrum among both types of users, the unlicensed users (secondary users, (SUs)) and the licensed users (primary users, (PUs)), while the SUs respect the rights of the PUs. Many solutions have been introduced to overcome the spectrum scarcity problem. Amongst the many, dynamic spectrum access (DSA) is one of them, wherein the spectrum is dynamically utilized. It enables users to adjust communication parameters (such as operating frequency, transmission power, modulation scheme) in response to the changes in the wireless environment [4-6]. DSA permits unlicensed users access the unused spectrum bands, which affects the security levels in the cognitive radio networks (CRNs).

As in any other type of wireless networks, CRNs are vulnerable to many security attacks (both passive and active) especially during the spectrum sensing phase. The radio technology itself is vulnerable to attacks as any radio frequency can be blocked or jammed when a transmitter sends a signal of adequate strength at the same frequency. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. The most important behaviors of attackers can be categorized into the following: (i) misbehaving, (ii) selfish (iii) cheating, or (iv) malicious [7]. An attacker can behave in one of these ways during spectrum sensing such as emulating PUs or sending false sensing results. The attacker aims to prevent other nodes from utilizing the spectrum efficiently, keep network resources for its own benefits, reduce the QoS of other nodes, and degrade the network security and performance.

Due to the importance of the security issue in the context of CRN, it has recently received interest from researchers [8]. Particularly during the spectrum sensing phase, new attacks have been introduced wherein malicious nodes exploit the vulnerability of the reliability issues, mentioned above, to attack the CRN. Any attack is the result of an attacker’s behavior. The attack is active when a network node is in an attacker's behavior category and when it is affecting the network security. In all other circumstances, the attack is passive and the adversary node is waiting for a chance to switch to an active attack.

The main focus of this research is to address the different attack behaviors that lead to multiple attacks other than addressing each attack separately. We develop a multi-layered model that improves the network performance measures, increases the network security, reduces the opportunity for malicious nodes to attack the CR network, and implicitly enhances the spectrum utilization and network throughput.

1.1 Cognitive Radio Networks (CRNs)

Networks that use the cognitive radio (CR) technology are referred to as cognitive radio networks (CRNs). The principle of Cognitive Radio (CR) was firstly mentioned and explained by J. Mitola [9]. Cognitive Radio is defined as an efficient technology that allows more users to use the available spectrum. It is a radio that can change its transmitter parameters based on interaction with the environment in which it operates. The two characteristics that are unique to CR are the cognitive capability and its re-configurability [9]. Cognitive capability represents the ability for the radio technology to capture or sense the information from its radio environment. Through this capability, the spectrum portions that are unused at specific locations or times can be identified. Re-configurability represents the ability of the CR to adapt any changes in its environment, which enables the radio to be dynamically programmed due to the radio environment.

As most of the spectrum is assigned to specific users (i.e. primary users (PUs)), the most important challenge is to share the licensed spectrum between the licensed users (PUs) and the unlicensed users (secondary users (SUs)).

Cognitive radio techniques provide the capability to use or share the spectrum in an opportunistic manner. The SUs have to detect the unused spectrum bands, which are known as spectrum holes, and this process is called spectrum sensing. Spectrum sensing is recognized as the basic functionality provided by CR. In the spectrum sensing process, the SUs continue to monitor the channel(s) that are owned by the PU(s). Once a channel is available, the SUs can start to use it. Despite the high-power levels consumed during the spectrum sensing process, the spectrum sensing results should be accurate, which helps the SUs in using the free frequency bands of PUs.

Although the major motivation of cognitive radio (CR) research is to manage the spectrum efficiently, CR is expected to be more than spectrum-agile. It is expected to convert the conventional radio into an intelligent agent that can learn from the radio environment and adapt the transmission parameters accordingly to optimize the communication performance. Spectrum agility is one dimension of its optimization parameters. Transmission parameters that may be adjusted to improve communication quality include operating frequency, modulation scheme, transmission power, and communication technology [8]. In [10], different Spectrum sensing methods and networking protocols for CRNs are summarized.

1.2 Security in CRNs

Unlicensed users can use the white bands of the spectrum in the absence of licensed users. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. A node can exploit the vulnerability of the CRN’s reliability and its lack of control in order to attack the different layers of the communication protocol.

There are many concepts that should be applied to satisfy a secure communication among cognitive radio network nodes, which are referred to as security requirements: confidentiality, integrity, availability and authentication [11].

Confidentiality means to protect information to prevent unauthorized revelations to systems or individuals. Data confidentiality is a mandatory requirement in CRNs generally to maintain the privacy of the data owner (PU or SU) as the data owner can include a bank storing credit and balance information about a customer [8]. Moreover, as radio is the communication medium in CRN which makes it open for access and easy to be attacked, confidentiality should be guaranteed for each connection.

Integrity is the property of ensuring that information will not be accidentally or maliciously altered or destroyed. It means that data is transmitted from the source to the destination without alteration [12]. The message can only be altered by the sender without detection by other nodes. Integrity protects against unauthorized creation, alteration or destruction of data. If it was possible for a corrupted message to be accepted, then this would show up as a violation of the integrity property [13].

Availability means to allow the network users to use the network for their own transmissions and to monitor the traffic in the network [8]. In CRN, when PUs are not using their spectrum channels, other users (SUs) can use these channels. However, once a PU wants to use its channels again all SUs have to leave immediately to make the channels available.

Authentication is the verification process of the claimed identity of a principal [14]. It is the primary security property; since, other properties often rely on accurate authentication. In CRN, each node has to authenticate itself before it can use the available spectrum channels. One access point manages the authentication process, wherein all SUs identify themselves to the access point.

The previous security requirements should be fulfilled through the different CR phases, such as spectrum sensing phase and spectrum management phase.

The first step in using the spectrum is the spectrum sensing phase, which is considered to be a cataleptic context for malicious nodes to arise and attack the CRN. The two security issues in PUs signals' detection are misdetection and false detection [8]. False detection is when an SU records the presence of a PU in its band, when in fact it is a malicious node posing as a PU that sends strong signals to SUs. Misdetection issue is the opposite of the false detection issue.

The second step in using the spectrum is the spectrum management phase, which includes finding the best paths between communicating nodes in the network. There are two different aspects of security that need to be considered in the design of routing algorithms or protocols in CRNs. The first aspect is to secure the routing algorithm or protocol itself (i.e. securing the route establishment, route maintenance, and data forwarding processes) by encrypting the control and data messages sent over the different paths. The second aspect is to consider security as a routing metric in order to find the best nodes to form the best path. To the best of our knowledge, the second aspect has not been applied in CRNs [15].

The issues previous mentioned are examples of security issues that can arise and make CRN a more challenging solution. Stronger security mechanisms should avoid the harmful effects of different attacks such as overhearing other users' information, interfering with other users' transmission signals and degrading the quality of service of licensed users. With these harmful effects, the spectrum scarcity problem will increase. CR technology is intended to prevent these effects and in turn, diminish the spectrum scarcity problem.

1.3 Motivation

In this section, we summarize the motivations that encouraged us to research in the area of CRNs mainly in monitoring nodes behavior during the spectrum sensing and the spectrum management phases in order to secure the communication among the different networks users and detect the misbehaving nodes. First, to the best of our knowledge, most of literature focuses on improving the spectrum sensing process to defend attacks that might occur during this process. Second, despite the significant importance of previous research, no studies have addressed the attacks that occur after the completion of spectrum sensing phase. Third, due to the effective conniving behavior of malicious nodes during the first two phases, nodes behavior after the completion of the spectrum sensing process should be considered. Fourth, none of the previous work penalizes the misbehaving nodes; the main focus is to identify the misbehaving nodes and disconnecting them from the network. The fifth factor is that other research work focuses on detecting one type of attack. In addition, there is no standard detection technique to identify and mitigate the attacker's behavior rather than the attack, itself. The sixth factor is that other routing protocols in CRNs do not consider the security level of nodes participating in data transmission as a routing metric. Their main focus is to minimize the cost and reduce the packets' transmission time between the source and destination. Although this is important, any path between the source and the destination nodes must be secured as much as possible in order to guarantee the data delivery with no alteration. Last but not the least, in order to build a general detection technique and a secure routing protocol among the network users, a node authentication process has to be completed as soon as a node joins the network. This authentication process has to prevent attacks from having the chance to occur later. If they do have the opportunity to occur after, the detection technique would detect them easily and faster. These factors inspired the idea to develop a hierarchal structure that contains three layers, which work together to secure the communication carried over CRNs, to improve the network reliability and efficiency, and to implicitly increase the network utilization.

1.4 Problem Statement and Research Goal

The radio technology itself is vulnerable to attacks as any radio frequency can be blocked or jammed when a transmitter sends a signal of adequate strength at the same frequency. As any other type of wireless networks, CRNs are vulnerable to many security attacks, such as denial of service attack, man-in-the-middle attack, and reflection attack. Unlicensed users can use the white bands of the spectrum in the absence of licensed users. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. A node can use the vulnerability of CRN reliability to attack the different layers of communication protocol.

Failing in spectrum sensing results, in terms of false detection or misdetection, might cause substantial interference for those who use the spectrum. On the other hand, wrong results of the spectrum sensing lead to inefficient spectrum utilization. More efficient and effective methods for detecting spectrum holes, when the CRN is highly dynamic, need to be developed. If the spectrum sensing is made by each secondary individually, the probability of collecting accurate sensing results is low. This probability is increased by applying the cooperation concept among the different secondary users. Cooperative spectrum sensing helps in achieving higher accurate and correct sensing results. Additionally, it prevents the negative impacts on performance caused by multipath fading and shadowing. Cooperative spectrum sensing allows the secondary users to share their initial decisions about the vacant spectrum bands and then proceed to make their final decisions. Therefore, any adversary nodes that participate in spectrum sensing can be identified and eliminated.

Moreover, adversary nodes may act normal during the spectrum sensing phase and then target the network during the data transmission phase. During the spectrum management phase, this detrimental behavior must be prevented. Routing is an important part of the spectrum management phase as all paths between any communicating network nodes are established. Routing in CRNs differs from traditional routing protocols in ad-hoc networks. There are many challenges related to CR technology itself or to the environment where the CR is applied, including the dynamic changes of spectrum availability, the instable behavior of PUs and SUs, resources heterogeneity, and the ability of synchronizing the different network nodes. Thus, traditional routing protocols in ad-hoc networks cannot be directly applied in CRNs as that will result in poor network performance in terms of end-to-end delay, packet delivery ratio and throughput.

With that being said, the research goal is to secure the data transmission in CRNs. In other words, it aims to prevent all adversary nodes from behaving abnormally either by eavesdropping on the messages sent over the different spectrum channels, altering, dropping, or falsely injecting them. Moreover, it aims to effectively share the spectrum among the different network nodes during the spectrum management phase relying on the nodes' behavior during the spectrum sensing phase.

1.5 General System Overview

This section presents the general form and assumptions of the system that are considered in this research. Figure 1.3 illustrates our system which is a network that has *M* SUs divided into *K* different clusters based on their geographical locations wherein each cluster has a unique identifier (Cluster ID) within the network. The fusion center (FC) controls the traffic over the network. In each cluster, one node is chosen by FC as a cluster head (CH). Any secondary user that wants to join the network has to be authenticated before it can use the network. Any SU can communicate with any node in the network (i.e. other SUs, CH, and the FC). Authentication is the process of validating the identity of the new or returning node(s) to the network. The joining node has to pass through the authentication process at the fusion center level and at the cluster head level. We assume that SUs can sense the PUs' spectrum accurately, and all of them are trusted nodes. We assume the CH cannot get compromised. If a CH gets offline, the FC will select another node in the cluster to be the new CH.

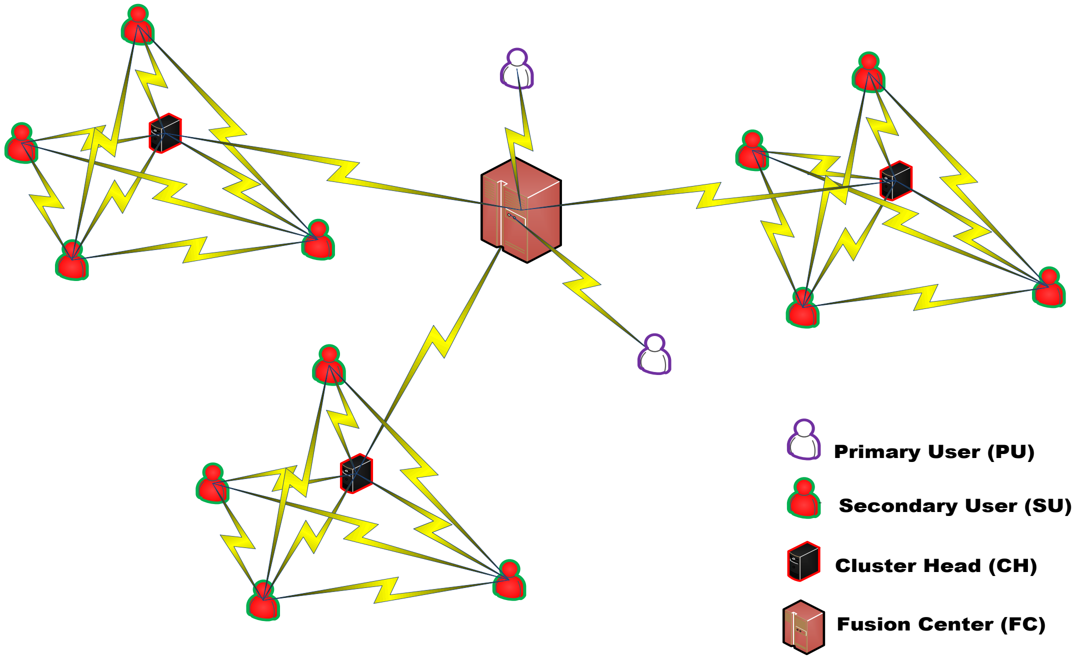


Figure 1.3: Network Overview.

The size for each channel is measured in hertz. The channel capacity, which represents the bandwidth or the data rate, is measured in bits/sec. In order to guarantee security in CRNs, we use two different methodologies: public key infrastructure-based and symmetric key cryptography. The common pre-defined control channel that is used as a communication channel was chosen for the following reasons:

- To send the spectrum sensing results between the different SUs in the spectrum sensing phase.
- To send the channel request and response messages between the SUs, FC and CHs in the authentication, sensing, and routing phases.

- To send the neighboring nodes information from FC to SUs in the sensing and routing phases.
- To send the routing requests and replies during the creation of the paths.

1.6 System Requirements and General Assumptions

The first step in cognitive radio networks is the spectrum sensing, wherein each SU explores the channels that are assigned for a specific PU and uses its own techniques in order to determine the absence or presence of the PU. The requirements of the system and its users are defined as well as the assumptions applied to our model.

1.6.1 System Requirements

Each secondary user (SU) would like to use any channel that is assigned to any PU in the network. The identity of all the nodes that use the spectrum has to be verified before any node granted a permission to access the spectrum. All messages exchanged during the spectrum sensing phase have to be encrypted, and only authorized nodes can decrypt them. Any node that wants to use the spectrum has to pass through two levels of identity verification. Specific nodes are selected to control the authentication process.

1.6.2 General Assumptions

In order to guarantee security in CRNs, we assume that the public key-infrastructure-based and symmetric-key cryptography are used for encrypting the messages exchanged in the authentication process. The symmetric key will be assigned to each node during the authentication process. Each node uses the same symmetric key for encoding and decoding the messages after it is shared among them. When a node sends a message to another node in the network, this message will be encrypted with the symmetric key. Meanwhile, the receiver decrypts this message by using the same symmetric key. Channels carrying the messages are error-free and all messages are received correctly by the recipient. A node's certificate is generated and validated through a certificate authority, server S, known to all the nodes similar as in TLS protocols [16]. The certificate authority, server S, grants a certificate to each node after it has been manufactured. The node's certificate includes its logic identifier, its MAC address and a pair of its public/private keys. As each node's certificate is signed by the key of the certificate authority, each node contacts the certificate authority, server S, to validate other nodes' certificate(s). During the certificate validation, each node gets all the node information from the certificate authority, server S, except the node's private key which is not shared with any other node in the network.

1.7 The Threat Model

In our system, an abnormal node might behave in one or more of the four different behavior categories (ways) to threaten the network in order to degrade the network security and performance. The threat model will be as following:

- A node behaves in a malicious, misbehaving, cheating, and/or selfish way to launch PUE attack by emulating one PU through sending signals over the spectrum channels.
- A node behaves in a malicious, misbehaving, cheating, and/or selfish way to launch SSDF attack by sending false sensing results to other nodes.
- Multiple collusive nodes behave in a malicious, misbehaving, cheating, and/or selfish way to launch collusion attack by sending false reputation reports about benign nodes aiming at degrading their QoS and gaining exclusive access to the spectrum for themselves.

- One or multiple nodes may behave in a malicious, misbehaving, cheating, and/or selfish way to launch DoS attack by sending any data over the spectrum channels in order to reduce the chance for other nodes from using the spectrum for their data transmission.
- One or multiple adversary nodes may behave in a malicious, misbehaving, cheating, and/or selfish way to launch objective function attack by trying to change the radio parameters such as center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size in order to reduce the network performance and security. There are three goals that the radio wants to achieve: low power, high data rate, and secure communication. Depending on the application, each of these goals has a different weight. Therefore, the adversary nodes 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.

1.8 Objectives and Contributions

This section includes the detailed objectives and contributions of this work.

1.8.1 Research Objectives

The principal goal of this work is to improve the communication performance of CRN as well as securing the data transmission in CRNs. To achieve this goal, we will develop a versatile system that is capable of interacting with changes in radio environment. Efforts will be geared towards the following objectives:

1. To improve the existing authentication mechanisms by developing an authentication approach that contributes the following:

- Thwarts all attackers and gives higher levels of security in the network.
- Improves the authentication successful rate and reduces the authentication time.
- Grants network access to authenticated nodes only, in order to reduce an opportunity for an attack to occur.

2. Following the authentication mechanism, to develop a novel monitoring mechanism of nodes' behavior during the spectrum sensing phase that contributes the following:

- Determines the adversary nodes and detects different types of attacks that might target the network (such as PUEA, DoS, Objective Function, etc.…).
- Improves the methods used in attacks detection and mitigation.
- Increases the efficiency of the spectrum sensing process.
- Improves the network security by penalizing adversary nodes.
- Improves the network reliability and efficiency by reducing false alarm probability.
- Increases the detection probability of free spectrum bands and the probability of detecting adversary nodes.
- Improves the transmission rates of different network nodes.

3. Based on the monitoring nodes' behavior technique that uses the authentication process, a novel routing algorithm is developed that contributes the following:

- Ensures a secure routing of packets among the communicating nodes.
- Enhances the spectrum utilization and efficiency.
- Increases the number of users that use the spectrum.
- Limits the number of messages being exchanged.
- Improves the network performance in terms of end-to-end delay, packet loss ratio, packet delivery ratio, and routing overhead.

1.8.2 Key Contributions

Although much research has been done in this area in different aspects, cognitive radio is considered to be a rich area for research. Despite the importance of the security issue in the context of CRN, it received less interest from researchers. Most of the research that has been done in the security of CRN was during the spectrum sensing process and it focused on identifying one or at most two attacks that simultaneously occur. To the best of our knowledge, this work is the first that considers the attacker's behavior rather than addressing the attacks, themselves. We address the misbehaving, cheating, selfish, and malicious behavior of nodes that might lead to different attacks such as PUEA, SSDF, DoS, and Collusion attacks. By mitigating the attacker's behavior, we reduce the prevalence of these multiple active or passive attacks. We merge the cooperative spectrum sensing and reputation systems in order to monitor the behavior of the node participating in the spectrum sensing process. We propose a collaborative approach for identifying and penalizing malicious and misbehaving node(s) during spectrum sensing phase. Moreover, we combine spectrum sensing phase and the routing in CRNs as it uses the nodes' behavior during the spectrum sensing as a routing metric. Our goal is to ensure secure communication among the different network nodes and to improve the network reliability and efficiency. With these goals in mind, this research contributes in the following aspects of CR networks:

1- Our first contribution is to develop an authentication mechanism that takes place when one node wants to join a CR network. To create this mechanism, a two-tier protocol was developed. The first tier is done at the fusion center (control authority) that controls all the traffic among all the network nodes. The second tier is at the cluster head (another control authority), which is responsible for fewer network nodes. This mechanism uses the existing encryption techniques to strengthen the authentication process, which is considered as the base of a secure communication in any type of network and especially in CRN. The proposed approach assigns each node a value called belief level (BL) that determines its security level for participating in the spectrum sensing process (i.e. in Contribution 2).

2- In the second contribution, a nodes' behavior monitoring approach is proposed. This technique applies the following concepts: clustering, collaboration, two-tier authentication (Contribution 1), reporting belief level value, rewarding and penalty. A center point called fusion center (FC) is responsible for managing resources among the different network users. Moreover, it has the authority to penalize misbehaving nodes by taking proper action(s) against the attacking nodes based on the attack severity. It is a collaborative approach during the spectrum sensing process that focuses on monitoring the nodes behavior rather than addressing the attacks themselves. By addressing the nodes behavior, multiple active and passive attacks can be detected and mitigated. In the proposed approach, all sensing nodes collaborate with each other to identify the behavior of other nodes. The node's belief level is updated and it will be used (in Contribution 3) as a routing metric.

3- The third contribution is to develop a routing algorithm that uses the belief level (in Contributions 1 and 2) as a routing metric to establish routes between any pair of nodes that would like to communicate. This algorithm provides a secure routing between the network nodes, which leads to improved network performance as it reduces the packet loss ratio that might occur because of different types of attacks that selectively drop/forward packets to next hop(s).

4- Last but not the least, the fourth contribution is to integrate the above contributions together in order to improve the network performance by establishing a complete spectrum management scheme that improves the spectrum utilization and detects all the misbehaving nodes.

1.9 Thesis Organization

The rest of the thesis is organized as follows. A literature review about CRN security and different kinds of attacks that target a CRN is described in Chapter 2. Our developed model for authentication mechanism (Contribution 1) and its performance evaluation are presented in detail in Chapter 3. The developed model for monitoring nodes’ behavior during spectrum sensing process (Contribution 2) and its performance evaluation are shown in Chapter 4. The routing algorithm (Contribution 3) and its performance evaluation are included in Chapter 5. Finally, the conclusion of the research and some suggestions for future work are summarized in Chapter 6.

1.10 Summary

In this chapter, an overview on the cognitive radio and security has been presented. The objectives and contributions of the thesis have been presented as well. These objectives and contributions can be summarized as follows:

- Proposing an authentication mechanism that can verify the identity of the nodes willing to use the network.
- Monitoring nodes’ behavior during the spectrum sensing phase in order to identify the adversary ones and eliminate them as well as reward normally behaving nodes.
- Using the nodes behavior during spectrum sensing as the foundation to build a secure routing algorithm.

Chapter 2: Literature Review

In this chapter, the security issues in cognitive radio networks (CRNs) are shown. The opportunities for security threats occurring in any mobile ad hoc network are much higher than a traditional wired network. Specifically, in CR networks, the threats are much more complex and the possibility of an attack is higher; since, the network nodes are much more intelligent by design. Unlicensed users can use the white bands of the spectrum in the absence of licensed users. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. A node can use the vulnerability of CRN reliability and the absence of control to attack the different layers of communication protocol.

The rest of this chapter is organized as follows: Section 2.1 describes the authentication process by showing different authentication approaches used in other wireless networks as well as in CRNs. Section 2.2 shows the spectrum sensing phase as well as the attacks that occur during the sensing phase. The spectrum management phase and the routing protocols used to share the spectrum are described in Section 2.3. Finally, we summarize the chapter in Section 2.4.

2.1 Authentication Process

The identity of any node that wants to join a CRN has to be verified before admitting the node to the network. This identity verification process is called authentication, which is known as one of the primary security requirements in wireless networks.

2.1.1 Authentication Mechanisms in CRNs and other Networks

Authentication process has been researched in many types of wireless networks with different solutions proposed. In [17], the authors proposed a dynamic user authentication scheme in Wireless Sensor Networks (WSN). It allows legitimate users to request the sensor data from any of the sensor nodes by imposing a smaller computational load. This scheme claimed that it is secure against replay and forgery attacks. However, the authors in [18] proved that the scheme proposed in [17] is vulnerable to replay and forgery attacks and proposed an authentication mechanism to overcome the drawbacks of [17]. The authors in [19] proposed a distributed node authentication model, wherein all the network nodes are involved in the authentication process as an authenticator. The main drawback of this scheme is the increased computational cost and communication overhead. Another authentication scheme is proposed by the authors in [20], where each node generates a one-way key chain and sends the commitment of it to their neighbors. If a node wants to send a message to its neighbors, it attaches the next authorization key from its key chain to the message. The receiving node can verify the validation of the key based on the commitment it has already received. The main drawback of this scheme is that it does not mitigate attacks from nodes, which are already part of the network as the adversary knows the node's authorization key. The authors in [21] have proposed an authentication scheme that uses one-way key chain to filter false messages sent between the access point and the sensor nodes. However, the main disadvantage of this scheme is that it uses signature-based authentication, which requires synchronization and periodic broadcasting between the access points and the sensor nodes. The authors in [22] claimed that authentication can only be completed on the physical layer as nodes might not deploy similar protocols at higher layers and then authentication messages cannot be understood. However, in CRN nodes are capable of understanding messages on different layers as they run similar software which can translate messages in a way that each node can understand it. The authors in [23] proposed an authentication scheme that uses the node's location information as a key factor to authenticate the cognitive nodes by a base station. However, it cannot be applied without the integration of the extensible authentication protocol (EAP). The authors in [24-26] have proposed a digital-signature based authentication scheme, which takes place on the physical and data link layers. This authentication scheme will find and permit the trusted users existing in CRN to access the spectrum. Despite the importance of this work to secure the communication in CRN, its performance evaluation shows that the message transfer with digital signature takes a long time compared to normal message transfer without digital signature. In [27], a mutual authentication protocol based on timestamp in Wireless Sensor Networks (WSN) that generates a new session-key for each session is proposed.

2.1.2 Analysis of Authentication Mechanisms

The approaches discussed previously have many limitations. Firstly, they take a long time to complete the authentication process as they rely on digital-signature cryptography, which means that more messages are transferred during the authentication process. Secondly, the other authentication schemes focused more on authenticating the spectrum usage and/or the joining node; however, the user of the joining node needs to also be authenticated in order to ensure whether it is a legitimate user. Lastly, these authentication schemes are completed on the physical and data link layers only. Authentication on different layers thwarts all attackers and gives higher levels of security in the network.

2.2 Security Analysis during Spectrum Sensing Phase

As in any other type of wireless networks, CRNs are vulnerable to many security attacks (both passive and active) especially during the spectrum sensing phase. The radio technology itself is vulnerable to attacks as any radio frequency can be blocked or jammed when a transmitter sends a signal of adequate strength at the same frequency. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. The most important behaviors of attackers can be categorized into the following: (i) misbehaving, (ii) selfish (iii) cheating or (iv) malicious [7]. If a node behaves in one of the previous categories, the node will be an adversary node and it might launch multiple attacks. An attacker that behaves in one of these ways during spectrum sensing can emulate PUs or send false sensing results in order to prevent other nodes from utilizing the spectrum efficiently, keep network resources for its own benefits, reduce the quality of service (QoS) of other nodes, and therefore, degrade the network security and performance.

2.2.1 Spectrum Sensing Process

As spectrum sensing is the main and first step for utilizing the CR technology in an efficient way, security is a main issue that has to be taken into consideration. After authenticating the nodes willing to use the spectrum, the nodes sense the spectrum looking for free channels in order to use them for their data transmission. The nodes behavior during the spectrum sensing process has to be monitored in order to prevent any authenticated nodes from acting a misbehaving way and threaten the spectrum sensing process as well as degrading the network performance. Failing to sense the spectrum correctly might cause substantial interference for those who use the spectrum and consequently, leads to inefficient spectrum utilization. When the conditions of CRNs are more dynamic, collaborative sensing helps to detect spectrum holes faster [5]. The detection probability to obtain correct sensing results is increased when the cooperation concept is applied among the different secondary users. Additionally, cooperative spectrum sensing alleviates the negative impacts on performance caused by multipath fading and shadowing [4] and [28]. Every participating user first detects the spectrum using any spectrum sensing method such as matched filter, energy detection, or cyclostationary feature detection [29], followed by exchanging their detection decisions, and finally making sensing decision based on all the nodes' sensing results. The authors in [30] study energy-efficient power allocation schemes for secondary users in sensing-based spectrum sharing cognitive radio systems. a cross-layer framework to jointly optimize spectrum sensing and access in agile wireless networks is presented in [31]. The different methods used for eliminating the interference in CRNs are summarized in [32]

2.2.2 Primary User Emulation and Spectrum Sensing Data Falsification Attacks

Due to the importance of the security issue in the context of CRNs, it has recently received interest from researchers [8]. New attacks have been introduced that are unique to CRNs, especially during the spectrum sensing process, wherein malicious nodes use vulnerability of the reliability issues to attack a CRN. Any attack is a result of an attacker's behavior. The attack is active when a network node is behaving in any of the attacker's behaviors and is affecting the network security. If this is not the case, the attack is passive and the network node is waiting for a chance to switch to an active attack. Primary User Emulation Attack (PUEA) in [6] and [33-35] and Spectrum Sensing Data Falsification Attack (SSDF) in [36-38] are two examples of attacks that are unique to CRN, which take place during the spectrum sensing phase. These two attacks are results of the different attackers' behaviors and both can be passive or active. PUEA is an active attack if a malicious node is emulating a PU and other nodes cannot detect it before making their own sensing decision. It is passive attack as long as other nodes can detect the malicious node before making their own sensing decision. SSDF is an active attack if a node sends false sensing results to other nodes or to a node that makes the final sensing decision and its false sensing results affect the final sensing decision. If its sensing results are not considered in making the final sensing decision, SSDF is a passive attack.

In PUEA, an attacker may modify their air interface as it emulates the primary-user's signal characteristics [39-40]. In this attack, other SUs will falsely determine that the frequency is in use by a legitimate PU. If the SUs vacate the frequency right away, then PUEA is an active attack. The following research addresses the active PUEA. In [41], the authors introduce a robust technique based on the principal component analysis for spectrum sensing process to prevent any attack from targeting the network. A defense method against the PUEA is proposed in [42]. All secondary users in the network follow a sequence of steps until the suspect nodes are detected and excluded from the spectrum sensing process. In [43], a fusion center receives the sensing information from the different SUs in the network that uses estimation algorithms to detect the PU signals in the presence of the attacker. A multiple criteria scheme known as INCA for a decentralized and cooperative analysis of the PUEA presence in cognitive radio ad hoc networks is proposed in [44]. Each SU cooperates with its neighbors to detect the PUEA by broadcasting the probability of PU's presence to its neighbors based on predetermined criteria such as received signal strength, transmission power, distance, noise, and transmission rate. This approach showed some improvements of the detection probability; however, the maximum value of the detection probability is 0.5. This is not a sufficient detection probability in order to be considered a reliable authentication approach.

In SSDF, the attackers share false sensing information into the decision stream as a legitimate member of the network. By doing this, the attackers aim to selfishly acquire increased spectrum availability for themselves, or the attackers may have a goal of disrupting the throughput of the network for other heinous reasons. The authors in [45] propose a mitigation method for SSDF attack. During the sensing period, all the malicious nodes and the other SUs make their own decisions about the presence/absence of PUs in their bands and forward these decisions to a fusion center. The fusion center manages the number of accurate decisions each node needs about the PU; this number of times is called measure. The higher the value of the measure the less reliable the node's observation is considered. The nodes with higher value of measure will be excluded from the following sensing results collection iteration. In [46], the authors develop a malicious user detection algorithm that calculates the suspicious level of SUs and then use the suspicious level to eliminate the malicious users' influence on the PU detection results. An attack-tolerant distributed sensing protocol that selectively filters out abnormal sensor reports and maintains the accuracy of incumbent detection is developed in [47]. The key idea behind this mechanism is that the measured primary signal strength at nearby sensors should be correlated due to shadow fading. The authors in [48] focus on a challenging attack scenario, wherein multiple cooperative attackers can overhear the honest SU sensing reports. However, the honest SUs are unaware of the existence of attackers. In [49], the authors propose a model for detecting the SSDF attack based on D-S theory for cooperative spectrum sensing method. They use the similarity degree to measure the evidence reliability of different users, where a low reliability means it is a malicious user and it will be excluded from the FC's final decision about the spectrum. The authors in [50] use a bioinformatics algorithm to propose a cooperative spectrum sensing approach. The sensing nodes that sensed spectrum multiple times in one allocated sensing time slot forwarded their sensing results to a fusion center that compares them using the bioinformatics algorithm. Based on the comparison, a similarity index is computed for each CR user. CR users with similarity indices below a threshold are declared malicious and their reports are excluded from decision combination process. While in [51], a principal-agent-based joint spectrum sensing and access framework to thwart the malicious behaviors of malicious users in CR networks is proposed.

2.2.3 Analysis of PUEA and SSDF Attacks Detection Techniques

In the research mentioned above, there are many limitations. Firstly, the PUEA and SSDF attacks are addressed individually (i.e. no previous work has considered both the attacks happening at the same time). Their effects to the network performance are higher if they happen simultaneously; therefore, addressing them together has a high impact on improving the network performance.

Secondly, researchers focused on addressing active PUEA and SSDF (i.e. current research has not addressed these two attacks while they are passive). Addressing active PUEA and SSDF attacks is a reactive solution to attacks; since, the attacks have already occurred and degraded the network performance. While addressing the passive attacks works as a proactive solution because it contributes to the elimination of such attacks before they occur and affect the network performance. Thirdly, the messages carrying the sensing results are exchanged between the different sensing nodes in an unencrypted way, which makes it easier for adversary nodes to overhear, capture the sensing results and launch multiple active attacks.

The work in [39-40] is the first work that addresses the two different attacks (PUEA and SSDF) while they are both active. The authors in [39-40] propose a model, which is a lightweight cryptographic algorithm that provides authentication and integrity to SUs' reports. Each node sends its sensing results to a fusion center (FC) encrypted with a variable number of security bits, which depends on how certain the node is about its sensing result. Despite the importance of this work, it has its disadvantages. It focuses more on encrypting the sent sensing result. It does not consider the case when sensing nodes send a wrong sensing result through a correct encrypted message, in which case its sensing result will be considered correct. Moreover, it does not provide a solution for the cases when collusive nodes agree on sending false sensing results.

2.2.4 Analysis of Other Attacks

There are other attacks addressed in other types of wireless networks such as denial of service (DoS), collusion, and objective function attacks [8] that can also be launched in CRNs as a result of PUEA and/or SSDF attacks. In active DoS attack, the adversary node acts normally in the network to gain the trust of other nodes and then targets the network by behaving in one of the attacker behavior categories. Another form of DoS attack is when the adversary node emulates PU signal (i.e. launches PUEA) luring other nodes to vacate the spectrum. DoS attack [52] results in degrading other nodes quality of service (QoS). In collusion attack, multiple adversary nodes agree on targeting benign node(s), which results in eliminating normal behaving nodes while adversary nodes keep network resources for their own use. In objective function attack, one or multiple adversary nodes try changing the radio parameters such as center frequency, bandwidth, or modulation. Addressing such attacks is important in CRNs especially during the spectrum sensing phase as it results in improving network performance, security, and spectrum utilization.

2.3 Security Analysis during Spectrum Management Phase

After the spectrum has been sensed and the free channels have been identified, the spectrum access has to be managed. Spectrum management is the process of regulating the use of radio frequencies among the different users to promote efficient use and gain a net social benefit. The research on cognitive radio has mostly focused on physical and data link layer issues, mainly on spectrum sensing and interference avoidance to PUs [53]. The authors in [54] propose an approach that formulate a stochastic optimization problem to integrate the power control, link scheduling, and routing, which minimizes the expected power consumption while guaranteeing the system stability.

2.3.1 Routing Protocols and Algorithms in CRNs

A number of challenges make the routing in CRNs differ from the traditional routing protocols in the ad-hoc networks. These challenges are related to two factors: the CR technology itself and the environment where the CR is applied. The former challenges are the dynamic changes of the spectrum availability and the instable behavior of the PUs and the SUs, while the latter challenges are the resources' heterogeneity and the ability of synchronizing the different network nodes. Thus, the traditional routing protocols used in the ad-hoc networks cannot be directly applied in the

CRNs, as that will result in a poor network performance in terms of higher end-to-end delay, less packet delivery ratio, more packet loss ratio and low throughput.

The two different routing infrastructures used in conventional networks are single-hop infrastructure and multi-hop infrastructure [55]. In the single-hop infrastructure, there is only one single path between any two nodes in the network that is used to transmit packets between the communicating nodes. The main advantages of single-hop infrastructure are that the routing tables are simpler and the packets flow smoothly. However, this infrastructure is not fault-tolerant (i.e. in case of any failure in the network the nodes after the failure will become unreachable and packets sent to them will be dropped and will not be transmitted successfully). In the multi-hop infrastructure, multi paths are available between any two communicating nodes, which make it fault-tolerant. Any failure that occurs in the network will not prevent packets from being sent successfully; since, there are be back-up paths that can be used for packets transmission. The main drawback of multi-hop infrastructure is that they are more complex to implement and that makes the routing tables larger.

Multiple routing metrics can be used in both the infrastructures such as classical routing metrics (e.g. delay, hop count, distance, power consumption, etc.) [56] or new routing metrics that have been introduced based on the CRN characteristics (e.g. spectrum availability, SU interference, route stability, etc.) [57].

The end-to-end delay is considered as a routing metric in classical networks. Many factors affect the end-to-end delay such as queuing delay, transmission delay, and channel switching time. A new routing metric called the Effective Transmission Time (ETT) is proposed in [58]. It measures the transmission delays on a link taking into account the expected number of retransmissions, which effectively captures the transmission time. Another routing metric is proposed in [59] and

[60], which combines two concepts of delay: the time required to change the channel and the back-off delay caused by the contention between the different nodes. The time required to change the channel is proportional to the difference between the initial and final channels. Another concept of delay, the queuing delays, has been added to the previous concepts of delay to propose another routing algorithm in [61-62]. Another routing algorithm that uses the delay as a routing metric is proposed in [63], which is referred as SEARCH. It takes the end-to-end delay as a routing metric, which includes the cost of switching channels and the delay over each channel. The authors in [64] proposes spectrum aware opportunistic routing (SAOR), another routing protocol. It uses a routing metric called the opportunistic link transmission (OLT) that combines three delay concepts, which are the link transmission delay, packet queuing delay, and link access delay. The authors in [65] proposed a routing based on location information and channel usage statistics. It uses a routing metric called cognitive transport throughput (CTT), which represents the potential relay gain over next hop.

Hop count is another routing metric that is used in different routing algorithms. CAODV [66] and SAMER [67] are two examples of routing algorithms that use the hop count as a metric. In CAODV, which is an adapted version of AODV for CRNs, the regions that have active PUs are eliminated during the routes establishment and data forwarding phases. Therefore, the best path does not have active PUs. In SAMER, multiple routes are established based on the hop count; however, one of them is used as a best path based on spectrum availability. In [68], an on-demand routing scheme called split multi-path routing (SMR) is proposed. It establishes multi-routes between source and destination nodes wherein one of these routes has the shortest delay route. In [69], an on-demand node-disjoint routing algorithm (NDMR) is proposed. It builds multiple node-disjoint paths with a low routing overhead. The authors in [70] use differential queue backlog as the routing metric to achieve throughput efficiency by proposing a distributed medium access control algorithm.

Many routing algorithms have used the power consumption as a routing metric, where all of them try to minimize the power consumed in order to find the best path for data transmission. MP-JSRA in [71] is an example of a routing protocol that uses the lowest data transmission cost (DTC) as a routing metric to find the best next node. DTC represents the weighted sum of two factors, the mobility cost and the interference cost to other network nodes including PUs and SUs. The authors in [72] propose a routing protocol called MWRP that uses the total transmission power used to send packets from the source to the destination as a routing metric based on the “lower-is-better” principle. LAUNCH in [73] is another routing protocol that uses PU activity, switching delay, and location information as a routing metric to find the best path between any two communicating nodes.

2.3.2 Analysis of Routing Algorithms

The main limitation of the previous research is that they do not consider security as a routing metric; therefore, the proposed work is the first to combine the spectrum sensing phase and the routing in CRNs as it uses the nodes’ behavior during the spectrum sensing as a routing metric. All routing protocols differ from each other in three factors: the routing metric, the environment where the protocol is applied, and the performance measures such as end-to-end-delay, packet delivery ratio, packet loss ratio, throughput, etc.

2.4 Summary

Any attack is a result of an attacker’s behavior. Therefore, mitigating the attackers’ behavior leads to detect and mitigate multiple attacks simultaneously, without addressing the attacks themselves.

In Table 2.1, we show the different attacks that might be launched as a result of one or multiple adversary nodes behaviors.

The routing in CRNs differs from the traditional routing protocols in the ad-hoc networks due to multiple factors including CR dynamicity and resource heterogeneity. Therefore, if the traditional routing protocols used in other networks are directly applied in the CRNs, a poor network performance will result. Moreover, the routing protocols used in CRNs do not consider security as a routing metric, which threatens the security properties of the network. The spectrum can be shared effectively between the SUs and the PUs taking into consideration that the spectrum sensing phase is done correctly. Therefore, monitoring the nodes' behavior during the spectrum sensing phase leads into better spectrum management.

Table 2.1 THE RELATIONSHIP BETWEEN ATTACKS AND ADVERSARY NODES' BEHAVIOR

Attack Name	**Adversary Node Behavior**
PUEA	Misbehaving, Malicious, and Cheating
SSDF	Misbehaving, Cheating, and Selfish
DoS	Misbehaving, Malicious, and Selfish, Cheating
Collusion	Misbehaving, Selfish, Malicious, and Cheating
Objective Function	Misbehaving and Malicious

Chapter 3: A Secure and Efficient Authentication Mechanism

In this chapter, a two-level authentication scheme for communication in CRN is proposed. Authentication is a primary security property in wireless networks wherein the identity of a cognitive node is verified before providing access to available resources. Before joining the network, a CR node is validated by obtaining security credentials from an authorized point.

Our proposed authentication scheme differs from other authentication schemes proposed in the literature in the following aspects:

- It is a two-level authentication, wherein the authentication process is done by two different entities (fusion center (FC) and cluster head (CH) defined earlier in Section 1.5) consecutively, and the joining node can gain access to the network resources only after it has been verified by both the entities.
- It utilizes the advantages of public and symmetric key cryptography approaches to encrypt messages sent between the joining node and the authenticating entities (both FC and CH), while other schemes apply the digital signature-based approach, which requires synchronization and periodic broadcasting that takes a longer execution time.
- It authenticates the spectrum usage and the joining node in addition to the user. Other authentication schemes focused more on authenticating the spectrum usage and/or the joining node; however, the user of the joining node needs also to be authenticated to ensure whether it is a legitimate user.
- The authentication process in our proposed scheme is carried over different layers (physical, data link, network, and application), while other authentication schemes are done on the physical and data link layers only. Authentication on different layers strengthens the

authentication process.

- It mitigates different attacks that target the different layers such as the reflection attack, the denial of service attack, and the man-in-the-middle attack, which can occur after the spectrum sensing phase is done. While other authentication schemes focus more on mitigating the Primary User Emulation (PUE) attack only that takes place during the spectrum sensing phase.
- It is specific to CRNs, as an attacker (adversary SU) may emulate a primary user's signal to lure other secondary users. Therefore, a secure authentication algorithm is needed that can determine if a signal sent over the network is a primary user's signal or an attacker's signal. A unique challenge in addressing this problem is that the Federal Communications Commission (FCC) prohibits authentication or any modification to primary users after they buy the spectrum license. Consequently, existing cryptographic techniques cannot be used directly.

The importance of having a two-level authentication scheme in CRNs stems from the need to reduce the opportunity for any adversary node to target the network and its nodes. In two-level authentication mechanism, the identity of the joining node is validated at two phases. In the first phase (at the FC level), the joining node is authenticated based on information that it already has, while in the second phase (at the CH level), it is authenticated based on information that is assigned to the joining node during the first phase. The information used in the first-level of authentication is stored on the device of the joining node and can be stolen and copied by the attacker, and therefore the attacker can successfully impersonate the joining node without actually stealing any physical device. On the other hand, the information needed in the second-level of authentication, which is sent to the node in the first-level of authentication, cannot be copied by the attacker unless it actually steals the node's physical device.

The two-level authentication mechanism uses multiple biometric factors, which therefore gives higher levels of security in the network as people with malicious intents have to pull off two different types of theft to obtain all information before attempting to spoof the network.

This chapter is organized as follows: in Section 3.1, the authentication process is described by developing a model that is implemented on two different levels. In Section 3.2, the performance of the proposed approach is measured and compared with other approaches in the literature. Next, the mechanism is validated through two different formal validation techniques in Section 3.3. After that in Section 3.4, the proposed approach is analyzed informally from different security perspectives. The chapter is concluded with a summary in Section 3.5.

3.1 The Mechanism

3.1.1 Mechanism Description

In this section, our two-level secure authentication scheme is explained. It is based on public and symmetric key cryptography, which reduces the number of cryptographic operations and the authentication time needed to complete the authentication process.

The proposed authentication scheme aims to authenticate the node (device) and its user as well as the spectrum usage. It works at two different levels which are FC's level and CH's level. The joining node has to correctly pass over the proposed two levels of authentication in order to be admitted as a part of the CRN. The message sequence of the proposed authentication scheme is illustrated in Figure 3.1.

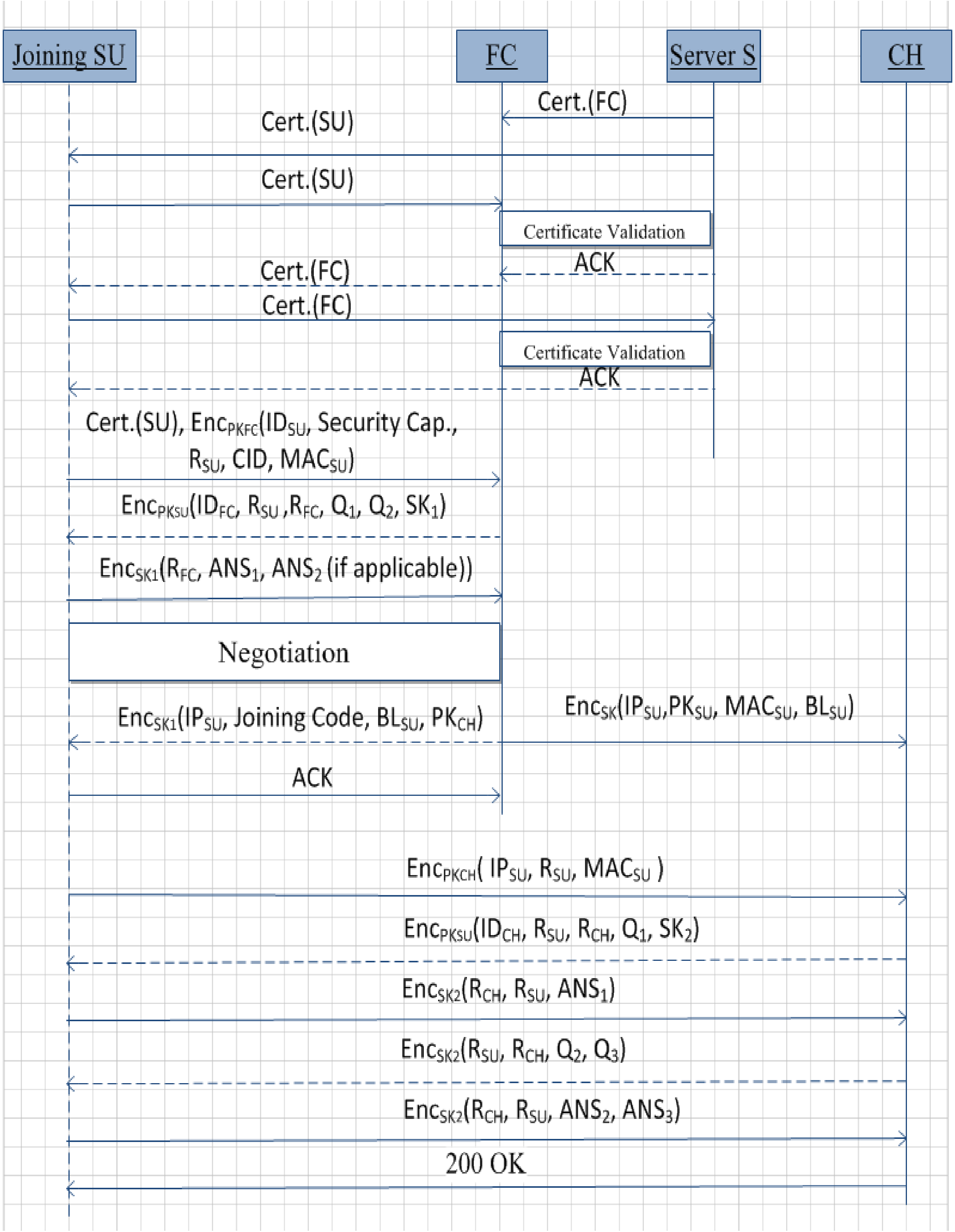

Joining SU
FC
Server S
CH
Cert.(FC)
Cert.(SU)
Cert.(SU)
Certificate Validation
ACK
Cert.(FC)
Cert.(FC)
Certificate Validation
ACK
Cert.(SU), $Enc_{PKFC}(ID_{SU}$, Security Cap., R_{SU}, CID, $MAC_{SU})$
$Enc_{PKSU}(ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SK_1)$
$Enc_{SK1}(R_{FC}, ANS_1, ANS_2$ (if applicable))
Negotiation
$Enc_{SK1}(IP_{SU}$, Joining Code, $BL_{SU}, PK_{CH})$
$Enc_{SK}(IP_{SU}, PK_{SU}, MAC_{SU}, BL_{SU})$
ACK
$Enc_{PKCH}(IP_{SU}, R_{SU}, MAC_{SU})$
$Enc_{PKSU}(ID_{CH}, R_{SU}, R_{CH}, Q_1, SK_2)$
$Enc_{SK2}(R_{CH}, R_{SU}, ANS_1)$
$Enc_{SK2}(R_{SU}, R_{CH}, Q_2, Q_3)$
$Enc_{SK2}(R_{CH}, R_{SU}, ANS_2, ANS_3)$
200 OK

Figure 3.1: The Sequence Diagram of the Proposed Scheme.

We define the terms that will be used in our proposed authentication model as follows:

- X: represents one of the system entities which are FC, CH, or SU.
- $Server\ S$: a certificate authority that generate and validate certificates of nodes.
- PK_X: the public key of entity X.
- ID_X: the logical identifier of entity X.
- MAC_{SU}: the hardware address of SU.
- $Cert.(SU)$: the manufacturing certificate of entity SU, which contains ID_X, MAC_{SU}, and PK_{SU}. It is generated and validated by the certificate authority, Server S.
- $Cert.(FC)$: the manufacturing certificate of entity FC, which contains ID_{FC}, MAC_{FC}, and PK_{FC}. It is generated and validated by the certificate authority, Server S.
- $ENC(Info.)$: all information is encrypted before sending it.
- R: a random number (nonce) generated by the sender and sent with each message to track the messages and to correlate with their response messages.
- C_{ID}: the connection ID.
- Symmetric Key (SK): a key used for encryption and decryption by the communicating nodes (FC, SU, and CH), SK_1 between FC and SU, SK_2 between SU and CH.
- Joining Code: generated by the FC. The joining code is unique within the cluster and is known by the nodes of the cluster. This joining code will be used to determine if this joining node is known to other cluster nodes.
- Security Capabilities: features or the properties that a node supports to make a secure communication with other nodes such as encryption/decryption protocol, message integrity code and key management cryptography algorithm.

- Belief Level (BL): describes the level of reliability of a node to participate in spectrum sensing and data transmission over the network.

After users' certificates have been validated through the certificate authority, server S, all messages exchanged between the FC/CH and the joining node cannot be accessed by a listening adversary as the receiving node can easily determine if the received message was sent from an intruder or not, based on the node's ID and its public key.

During the authentication process, the authenticating node (i.e. FC or CH) asks the joining node up to three different questions as shown in Table 3.1. Answering these questions correctly by the joining node leads to successful authentication of this joining node. During the first level of authentication, the FC asks the joining node Question 1 (Q_1) and Question 2 (Q_2) to check its ID and what information this node has about the joining cluster. If the joining node is a returning node to the same cluster, it has to answer the two questions correctly.

TABLE 3.1 QUESTIONS TO THE JOINING NODE

Question		**Joining Node Status**	**Asked by**
Q_1	What is your ID? and What is(are) the cluster(s) ID that you want to join?	New or Returning	FC & CH
Q_2	What is the joining code of the cluster(s) that you want to join?	Returning	FC & CH
Q_3	What is your IP? and What is your BL?	New or Returning	CH

However, if the node is a returning node, but to a different cluster or the node is completely a new node, it answers Q_1 only. The FC keeps track of all joined nodes by storing their MAC address in a database that is used to determine if a joining node is a new node or a returning node. During the second level of authentication, the CH asks the joining node all the three questions as it should have the answers to all these questions as long as it has correctly passed the FC's level of authentication.

3.1.2 Authentication at FC level

The FC's authentication level starts by validating the nodes' certificates, which are generated and assigned by Server S. In this process, the certificates of the joining node and the authenticating node are validated through the certificate authority, Server S. During the certificate validation, the joining node (SU) sends its certificate ($Cert.(SU)$ to the FC, which contacts the Server S to validate SU's certificate. Once the SU's certificate is validated, FC replies to SU by sending its own certificate ($Cert.(FC)$). Then, SU contacts the Server S to validate the certificate of FC. If it is validated, SU sends a message ($ENC_{PK_{FC}}(()$, encrypted with PK_{FC}, that contains its ID (ID_{SU}), its security capabilities, a random number (nonce) $RSU,$ a connection ID (CID), and its MAC address. MAC address is used because it is unique for each node at the authentication layer. The FC sends a message ($ENC_{PK_{SU}}$ ()), encrypted with PK_{SU}, to the joining SU, which contains its ID (ID_{FC}), symmetric key SK_1 used to encrypt/decrypt the messages exchanged from now on, a random nonce (R_{FC}) connected with the received R_{SU}, and questions (Q_1 and Q_2). The purpose of these questions is to ensure that this joining node has enough information about the cluster(s) that it wants to join.

If the joining node is a new node or a returning node to a different cluster, Q_1 will be answered only by sending ANS_1, which includes its ID (ID_{SU}) and all cluster(s) ID(s) that SU receives from nodes which are within its range. However, if the joining node is a returning node to the same cluster that it was part of during the last connection time, it answers both Q_1 and Q_2 by sending ANS_1 and ANS_2. If a returning node to the same cluster fails to provide the FC with the joining code, it will not be admitted. The joining SU replies to Q_1 and Q_2 by sending ANS_1 and ANS_2 encrypted with the symmetric key SK_1. Upon the success of answering Q_1 and Q_2 (if applicable), the resource negotiation phase starts in which the joining SU sends its QoS requirements to the FC. The FC takes the responsibility to determine if the desired cluster can provide them or not.

The negotiation phase ends with either an agreement or a disagreement between the joining SU and the FC. If both do not agree on resources, SU will not be joined. If both of them agree on resources, the FC assigns an IP address to this node, provides it with the cluster joining code, calculates a value called belief level, and prepares the public key of CH. The belief level describes the level of reliability of this node to participate in data transmission over the network. The public key of CH, PK_{CH}, is used in the second level of authentication. The node's IP address, the node's belief level, the cluster head's public key, and the cluster's joining code are encrypted in one message and sent to the joining node. Meanwhile, the FC sends the node's MAC address, the node's belief level, and the node's public key PK_{SU} to the CH. These parameters are sent in an encrypted message as FC and CH communicate over a secure control channel. Figure 3.2 illustrates the flow chart of the FC level authentication.

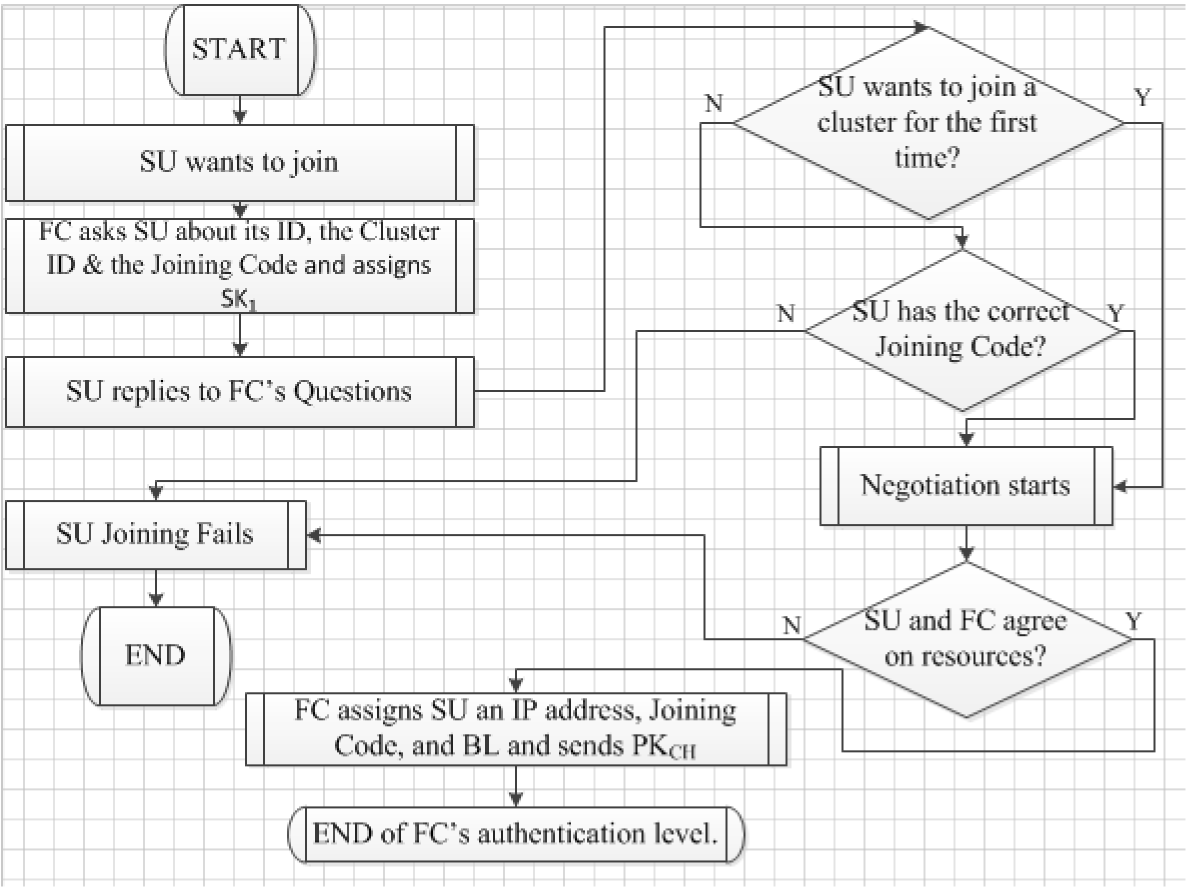

START
SU wants to join
FC asks SU about its ID, the Cluster ID & the Joining Code and assigns SK1
SU replies to FC's Questions
SU wants to join a cluster for the first time?
N
Y
SU has the correct Joining Code?
N
Y
Negotiation starts
SU Joining Fails
END
SU and FC agree on resources?
N
Y
FC assigns SU an IP address, Joining Code, and BL and sends PKCH
END of FC's authentication level.

Figure 3.2: Flow Chart for Authentication at FC Level.

3.1.3 Authentication at CH level

The joining SU starts the second level of authentication by sending a message ($ENC_{PK_{CH}}(\,)$), encrypted with the already known CH's public key, to the cluster head. This encrypted message contains the joining node's public key PK_{SU}, its MAC address, and a random number R_{SU}. The CH now wants to authenticate the user of this joining node by asking three questions. First, the CH sends ($ENC_{PK_{SU}}(\,)$), an encrypted message with the joining node's public key. In this message, the CH asks the joining SU about its IP and about the cluster ID, and sends the symmetric key, SK_2, that will be used to encrypt/decrypt the messages from now on. The joining SU replies by sending its answer encrypted with SK_2.

If the joining SU answers correctly, the CH sends an encrypted message with the SK_2 asking the joining SU Q_2 about the cluster's joining code and Q_3 about its BL. The joining SU replies by sending its answers (ANS_1 and ANS_2) encrypted with SK_2. If the joining SU answers correctly, the CH admits the joining SU to be part of the cluster. The SU can now join the cluster and can start transmitting data with the other cluster nodes. If the joining node fails to answer any of these three questions, it will not be admitted and the CH sends a report to the FC. Figure 3.3 illustrates the flow chart of the CH level authentication. Each message sent between the joining node and the authenticating node contains their random (nonce) numbers, which are used to synchronize messages and to prevent any intruder from eavesdropping on the messages exchanged between the communicating nodes. On the other hand, each node's IP is sent encrypted once the node sends its first message to the other communicating party. The message receiver validates the sender's IP by extracting the sender's IP from the message sent earlier by FC to CH, and compares it with the received one. This validation prevents the messages exchanged between the communicating nodes from being accessed by an intruder; and therefore, improves the network security.

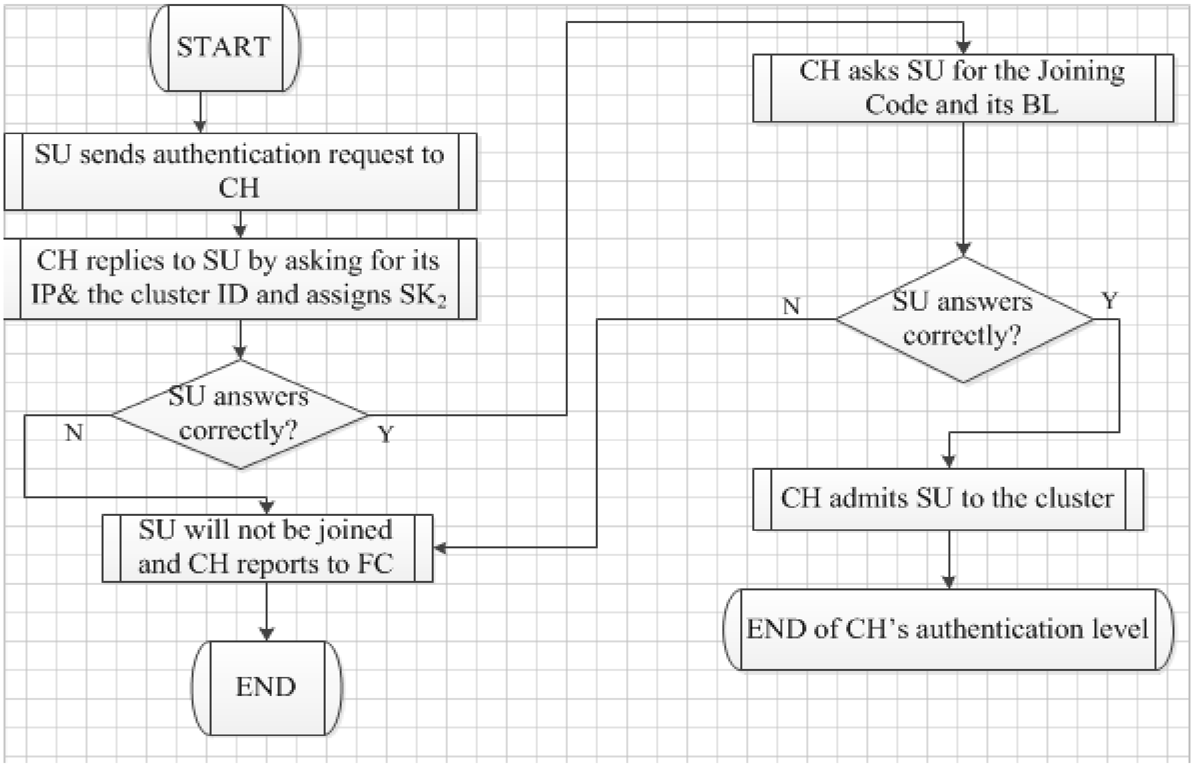

START
SU sends authentication request to CH
CH replies to SU by asking for its IP& the cluster ID and assigns SK₂
SU answers correctly?
N
Y
SU will not be joined and CH reports to FC
END
CH asks SU for the Joining Code and its BL
N
SU answers correctly?
Y
CH admits SU to the cluster
END of CH's authentication level

Figure 3.3: Flow Chart for Authentication at CH Level.

3.2 Performance Evaluation

3.2.1 Complexity Analysis

We analyze the performance overhead of our proposed authentication algorithm. Our algorithm has two stages (at the FC or CH levels), five steps/each. In each stage, the joining node and the authenticating party exchange their first message using the other node's public key (two messages), and the other messages are sent encrypted using the symmetric key. By analyzing those messages, we find that the authenticating party (FC or CH) sends two messages, and the joining node sends three messages. As each joining node SU_i encodes three messages and decodes two messages, each joining node performs $5 * O(1)$ messages' encoding and decoding. Thus, the computation overhead for each node is $\approx O(1)$. On the other hand, the authenticating party encodes $2 * |M|$ and decodes $3 * |M|$ messages, where

M represents the total number of SUs. Therefore, the computation overhead at the authenticating party is $(2 * |M| + 3 * |M|)$. If we replace M by N for complexity calculation standards, the computation overhead for the authenticating party is $\approx O(N)$.

The communication overhead is calculated based on the number of messages exchanged between the joining node and the authenticating party. The number of messages is equal to that used in the computation overhead; therefore, the communication overhead at the joining SU is $\approx O(1)$ and at the authenticating party is $\approx O(N)$.

3.2.2 Numerical Results

In this section, we compare our proposed authentication scheme with the approaches described in [26-27]. The comparison is in terms of the number of cryptographic operations needed by each technique and the total authentication time. We use the benchmarks available in [74] where C++ is used to implement the cryptographic algorithms, and Microsoft Visual C++ 2005 SP1 is the compiler and the system specifications are an Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode. We select a cryptographic algorithm for each cryptographic operation as in Table 3.2.

By analyzing the authentication techniques proposed in [26], and in [27] and our proposed scheme using the benchmarks in [74], we can determine how many times each cryptographic operation is executed in total, as shown in Table 3.3. Moreover, we use the values in Table 3.2 and Table 3.3 to compute the time needed to complete the authentication process in each approach.

TABLE 3.2 CRYPTOGRAPHIC ALGORITHMS

Cryptographic Operation	Cryptographic Algorithm	Execution Time
Digital Signature Generation	RSA 1024	1.48ms
Digital Signature Verification	RSA 1024	0.07ms
Certificate Validation	RSA 1024	0.07ms
Message Encryption with Public Key	RSA 1024	0.08ms
Message Encryption with Symmetric Key	AES/EAX	1.8µs
Message Decryption with Public Key	RSA 1024	1.46ms
Message Decryption with Symmetric Key	AES/EAX	1.8µs
Hash Function	HMAC(SHA-1)	0.509µs

TABLE 3.3 CRYPTOGRAPHIC OPERATION COUNT

Cryptographic Operation	Scheme					
	[26]		[27]		Ours	
	Number of operations	Execution time	Number of operations	Execution time	Number of operations	Execution time
Certificate Validation	5	0.35m	4	0.28m	2	0.14m
Hash Function	2	1.02µ	13	6.62µ	2	1.02µ
Message Encryption with Public Key	7	0.56m	4	0.32m	4	0.32m
Message Encryption with Symmetric Key	0	0	6	10.8µ	6	10.8µ

Message Decryption with Public key	7	10.22m	4	5.84m	4	5.84m
Message Decryption with Symmetric Key	0	0	6	10.8µ	6	10.8µ
Digital Signature Generation	4	5.92m	1	1.48m	0	0
Digital Signature Verification	4	0.28m	1	0.28m	0	0
Total	**29**	**17.3m**	**39**	**8.2m**	**24**	**6.3m**

To complete the authentication scheme proposed in [26] and in [27], twenty-nine and thirty-nine cryptographic operations have to be executed, respectively. However, in our proposed scheme only twenty-four operations are required, which means more than 10% less computation and calculation cost.

We next analyze the time needed to complete the authentication process, which is referred to as the authentication delay. It consists of two parts, the processing time and the transmission time. The processing time is the major part, which represents the time needed to execute the cryptographic operations. The transmission time is the time needed to transmit each message between the authenticating node and the joining node. It was assumed that the transmission time has the same value in all the schemes, therefore we neglect the transmission time in the calculation of authentication delay.

According to [74], the signature generation time is 1.48ms, the verification time using RSA 1024 is 0.07ms, the time for the message encryption with public key is 0.08ms, the time for the message decryption with public key is 1.46ms, the time for the message encryption with symmetric key is 1.8µs, the time for the message decryption with symmetric key is 1.8µs, and the hashing time using HMAC (SHA-1) is 0.509µs. The authentication time in [26] was 17.3ms and in [27] is equal to 8.2ms. It is approximately 6.32ms in our authentication scheme, which is about 63% and 23% faster in comparison to that in [26] and [27], respectively. It is evident that our proposed scheme reduces the authentication time. Moreover, our proposed approach is less complex in comparison to that of [26] and [27]'s; since, the symmetric key cryptography is used for encrypting and decrypting most of the messages exchanged. The symmetric key cryptography has less memory occupation, less memory use, and less power utilization.

3.3 Mechanism Validation

We verify the correctness of our proposed authentication scheme by using two different formal verification methods which are BAN logic [75] and Scyther verification tool [76].

3.3.1 Verification through BAN logic

In BAN logic, all messages sent between two communicating nodes are formulated according to the BAN logic format and then BAN logic axioms and messages' analysis are applied to these messages to conclude if the protocol meets its desired objectives or not.

We define the terms used through the verification process of our proposed authentication algorithm as follows:

- SU, FC, and CH: are the network agents.
- S: is a certificate authority known to all network nodes.
- (Info.): is the message encrypted.
- PK_{FC}: is the public key of entity FC.
- PK_{SU}: is the public key of entity SU.
- PK_{CH}: is the public key of entity CH.
- PK_{S}: is the public key of the server S and known to SU and FC, which grants certificates to

each node.

- $\mathrm{ID_{FC}}$: is the logical identifier of entity FC.
- $\mathrm{ID_{SU}}$: is the logical identifier of entity SU.
- $\mathrm{ID_{CH}}$: is the logical identifier of entity CH.
- $\mathrm{R_{FC}}$: is a random number (nonce) generated by FC.
- $\mathrm{R_{SU}}$: is a random number (nonce) generated by SU.
- $\mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}$: is the symmetric key that SU and FC agree during the FC level authentication.
- $\mathrm{SU} \overset{\mathrm{SK_2}}{\Longleftrightarrow} \mathrm{CH}$: is the symmetric key that SU and CH agree during the CH level authentication.

In BAN logic, there are two network agents (P and Q), a message (X) is exchanged between the network agents. Message (X) is encrypted by an encryption key (K). The axioms definitions and their implications are below:

- $P\ believes\ X$: P acts as if X is true, and may assert X in other messages.
- P said X: At one time, P transmitted and believed message X, although P might no longer believe X.
- P sees X : P receives message X, and can read and repeat of X.
- $fresh(X)$: X has not previously been sent in any message.

Authentication at FC Level

We start with defining the assumptions:

$$SU \text{ believes } \xrightarrow{PK_{SU}} SU,$$

$$FC \text{ believes } \xrightarrow{PK_{FC}} FC,$$

$$SU \text{ believes} \xrightarrow{PK_{S}} S,$$

FC believes $\xrightarrow{PK_S} S$,

SU believes fresh $(\mathrm{R_{SU}})$,

FC believes fresh $(\mathrm{R_{FC}})$,

SU believes FC controls $\left(SU \overset{SK_1}{\Longleftrightarrow} FC\right)$,

FC believes FC controls $(SU \overset{SK_1}{\Longleftrightarrow} FC)$.

We can represent the goals of the FC level authentication (what we want to prove) according to BAN logic as following:

SU believes $SU \overset{SK1}{\Longleftrightarrow} FC$,

FC believes $FC \overset{SK1}{\Longleftrightarrow} SU$.

Here are the idealized messages of the FC's level authentication, note that we omit the messages and the parts of messages which do not affect the sender and receiver identities.

MSG1: FC → SU: $\mathrm{ENC_{PK_S}(MAC_{FC}, \xrightarrow{PK_{FC}} FC)}$.

MSG2: SU → FC: $\mathrm{ENC_{PK_S}\left(MAC_{SU}, \xrightarrow{PK_{SU}} SU\right)}$,

$\mathrm{ENC_{PK_{FC}}(ID_{SU}, R_{SU}, MAC_{SU})}$.

MSG3: FC → SU: $\mathrm{ENC_{PK_{SU}}\left(ID_{FC}, R_{SU}, R_{FC}, Q_1, Q_2, SU \overset{SK_1}{\Longleftrightarrow} FC\right)}$.

MSG4: SU → FC: $\mathrm{ENC_{SK_1}(R_{FC}, ANS_1, ANS_2)}$.

We apply the axioms of BAN logic on each message.

<u>On message 1:</u>

SU sees $(\mathrm{MAC_{FC}}, \xrightarrow{PK_{FC}} FC)$ **<u>and</u>** SU believes $\xrightarrow{PK_S} S$, **<u>therefore</u>** SU believes S said$(\mathrm{MAC_{FC}}, \xrightarrow{PK_{FC}} FC)$.

<u>So,</u> SU believes S believes ($\mathrm{MAC_{FC}},\xrightarrow{PK_{FC}} FC$), **<u>which means</u>** SU believes S controls ($\mathrm{MAC_{FC}}$, $\xrightarrow{PK_{FC}} FC$), **<u>which results in</u>** SU believes ($\mathrm{MAC_{FC}},\xrightarrow{PK_{FC}} FC$).

For simplicity, we consider the part that is related to the public key cryptography, hence SU believes $\xrightarrow{PK_{FC}} FC$.

<u>On message 2:</u>

We start by considering the first part of message 2, which is $\mathrm{ENC}_{PK_S}\left(\mathrm{MAC_{SU}},\xrightarrow{\mathrm{PK_{SU}}} \mathrm{SU}\right)$.

FC sees ($\mathrm{MAC_{SU}},\xrightarrow{PK_{SU}} SU$) **<u>and</u>** FC believes $\xrightarrow{PK_S} S$, **<u>therefore</u>** FC believes S said ($\mathrm{MAC_{SU}}$, $\xrightarrow{PK_{SU}} SU$).

<u>So,</u> FC believes S believes ($\mathrm{MAC_{SU}},\xrightarrow{PK_{SU}} SU$), **<u>which means</u>** FC believes S controls ($\mathrm{MAC_{SU}}$, $\xrightarrow{PK_{SU}} SU$), **<u>which results in</u>** FC believes ($\mathrm{MAC_{SU}},\xrightarrow{PK_{SU}} SU$).

For simplicity, we consider the part that is related to the public key cryptography, hence FC believes $\xrightarrow{PK_{SU}} SU$.

We next consider the second part of message 2, which is $\mathrm{ENC_{PK_{FC}}}(\mathrm{ID_{SU}}, \mathrm{R_{SU}}, \mathrm{MAC_{SU}})$. The only deduction that we obtain is FC sees ($\mathrm{ID_{SU}}, \mathrm{R_{SU}}, \mathrm{MAC_{SU}}$).

<u>On message 3:</u>

SU sees $\left(\mathrm{ID_{FC}}, \mathrm{R_{SU}}, \mathrm{R_{FC}}, \mathrm{Q_1}, \mathrm{Q_2}, \mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}\right)$, but SU believes fresh ($\mathrm{R_{SU}}$),

<u>therefore</u> SU believes fresh $\left(\mathrm{ID_{FC}}, \mathrm{R_{SU}}, \mathrm{R_{FC}}, \mathrm{Q_1}, \mathrm{Q_2}, \mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}\right)$. SU believes $\xrightarrow{PK_{FC}} FC$,

<u>and</u> SU sees $\left(\mathrm{ID_{FC}}, \mathrm{R_{SU}}, \mathrm{R_{FC}}, \mathrm{Q_1}, \mathrm{Q_2}, \mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}\right)$,

<u>therefore</u>SU believes FC said $\left(\mathrm{ID_{FC}}, \mathrm{R_{SU}}, \mathrm{R_{FC}}, \mathrm{Q_1}, \mathrm{Q_2}, \mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}\right)$. With the previous derivation **<u>we conclude that</u>** SU believes FC believes $\left(\mathrm{ID_{FC}}, \mathrm{R_{SU}}, \mathrm{R_{FC}}, \mathrm{Q_1}, \mathrm{Q_2}, \mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}\right)$, and **<u>with the assumption</u>** SU believes FC controls $\left(SU \overset{SK_1}{\Leftrightarrow} FC\right)$, **<u>we find that</u>**

SU believes $\left(\mathrm{ID_{FC}}, \mathrm{R_{SU}}, \mathrm{R_{FC}}, \mathrm{Q_1}, \mathrm{Q_2}, \mathrm{SU} \overset{\mathrm{SK_1}}{\Longleftrightarrow} \mathrm{FC}\right)$,

<u>which means</u> SU believes $(SU \overset{SK_1}{\Leftrightarrow} FC)$. (a)

<u>On message 4:</u>

FC sees $(\mathrm{R_{FC}}, \mathrm{ANS_1}, \mathrm{ANS_2})$ and then compares the received $\mathrm{R_{FC}}$ with the sent $\mathrm{R_{FC}}$. If both are equal, it means FC ensures that SU has received SK_1.

<u>Therefore,</u> FC believes SU believes $\left(SU \overset{SK_1}{\Leftrightarrow} FC\right)$, and **<u>with the assumption</u>** FC believes FC controls $\left(SU \overset{SK_1}{\Leftrightarrow} FC\right)$, **<u>we find that</u>** FC believes $(SU \overset{SK_1}{\Leftrightarrow} FC)$. (b)

Derivations (a) and (b) are the objectives of our proposed authentication scheme on the FC's level.

Authentication at CH Level

The authentication on the CH's level aims to validate the identity of the SU, i.e. the CH ensures that the user of the CR node is a legitimate user already authenticated by the FC and has received the information needed. This authentication level follows the question and answer method wherein the CH asks the SU for some information and the SU replies with the answers. Failing in answering any of these questions results in not accepting the node in the network and a report will be sent to FC.

We start with the assumptions:

$$SU\ believes\ \xrightarrow{PK_{SU}} SU,$$

$$CH\ believes\ \xrightarrow{PK_{CH}} CH,$$

$$SU\ believes\ \xrightarrow{PK_{CH}} CH,$$

$$SU\ believes\ fresh\ (R_{SU}),$$

$$CH\ believes\ fresh\ (R_{CH}),$$

$$SU\ believes\ CH\ controls\left(SU\ \overset{SK_2}{\Leftrightarrow}\ CH\right),$$

$$CH\ believes\ CH\ controls\ \ (SU\ \overset{SK_2}{\Leftrightarrow}\ CH).$$

According to BAN logic the goals of the CH authentication level (what we want to prove) are:

SU believes $SU \overset{SK_2}{\Leftrightarrow} CH,$

CH believes $CH \overset{SK_2}{\Leftrightarrow} SU.$

The messages exchanged between the CH and the SU are:

$\mathrm{MSG1: SU \rightarrow CH: ENC_{PK_{CH}}(IP_{SU}, R_{SU}, MAC_{SU})}.$

$\mathrm{MSG2: CH \rightarrow SU: ENC_{PK_{SU}}\left(ID_{CH}, R_{SU}, R_{CH}, Q_1\ , SU \overset{SK_2}{\Leftrightarrow}\ CH\right)}.$

$\mathrm{MSG3: SU \rightarrow CH: ENC_{SK_2}(R_{CH}, R_{SU}, ANS_1)}.$

$\mathrm{MSG4: CH \rightarrow SU: ENC_{SK_2}(R_{SU}, R_{CH}, Q_2, Q_3)}.$

$\mathrm{MSG5: SU \rightarrow CH: ENC_{SK_2}(R_{CH}, R_{SU}, ANS_2, ANS_3)}.$

Note that CH encrypts question 1 in message 2 by the public key of SU while question 2 and question 3 in messages 4 and 6 are encrypted with the symmetric key $\mathrm{SK_2}$ upon the key agreement between the CH and SU that occurs in message 3. Therefore, to verify the correctness of this authentication level, we need to apply BAN logic to the first three messages only.

On message 1:

CH compares $\xrightarrow{\mathrm{PK_{SU}}}$ SU with the one received from the FC, and if they are same, CH **concludes that** CH believes $\xrightarrow{PK_{SU}} SU.$

On message 2:

SU sees $\left(\mathrm{ID_{CH}, R_{SU}, R_{CH}, Q_1, SU \overset{SK_2}{\Leftrightarrow}\ CH}\right),$

but SU believes fresh $(\mathrm{R_{SU}})$, **therefore** SU believes fresh $\left(\mathrm{ID_{CH}}, \mathrm{R_{SU}}, \mathrm{R_{CH}}, \mathrm{Q_1}, \mathrm{SU} \overset{\mathrm{SK_2}}{\Leftrightarrow} \mathrm{CH}\right)$.
SU believes $\xrightarrow{PK_{CH}} CH$ **and** SU sees $\left(\mathrm{ID_{CH}}, \mathrm{R_{SU}}, \mathrm{R_{CH}}, \mathrm{Q_1}\ , \mathrm{SU} \overset{\mathrm{SK_2}}{\Leftrightarrow} \mathrm{CH}\right)$,
therefore SU believes CH said $\left(\mathrm{ID_{CH}}, \mathrm{R_{SU}}, \mathrm{R_{CH}}, \mathrm{Q_1}, \mathrm{SU} \overset{\mathrm{SK_2}}{\Leftrightarrow} \mathrm{CH}\right)$.

With the previous derivation we conclude that
SU believes CH believes $\left(\mathrm{ID_{CH}}, \mathrm{R_{SU}}, \mathrm{R_{CH}}, \mathrm{Q_1}, \mathrm{SU} \overset{\mathrm{SK_2}}{\Leftrightarrow} \mathrm{CH}\right)$, and **with the assumption**
SU believes CH controls $\left(SU \overset{SK_2}{\Leftrightarrow} CH\right)$,

we find that SU believes $\left(\mathrm{ID_{CH}}, \mathrm{R_{SU}}, \mathrm{R_{CH}}, \mathrm{Q_1}, \mathrm{SU} \overset{\mathrm{SK_2}}{\Leftrightarrow} \mathrm{CH}\right)$,

which means SU believes $(SU \overset{SK_2}{\Leftrightarrow} CH)$. (c)

On message 3:

CH sees $(\mathrm{R_{CH}}, \mathrm{R_{SU}}, \mathrm{ANS_1})$ and compares the received $\mathrm{R_{CH}}$ with the sent $\mathrm{R_{CH}}$. If both are equal, CH ensures that SU has received SK_2.

Therefore, CH believes SU believes$(SU \overset{SK_2}{\Leftrightarrow} CH)$, and **with the assumption**
CH believes CH controls $\left(SU \overset{SK_2}{\Leftrightarrow} CH\right)$, **we find that** CH believes $(SU \overset{SK_2}{\Leftrightarrow} CH)$. (d)

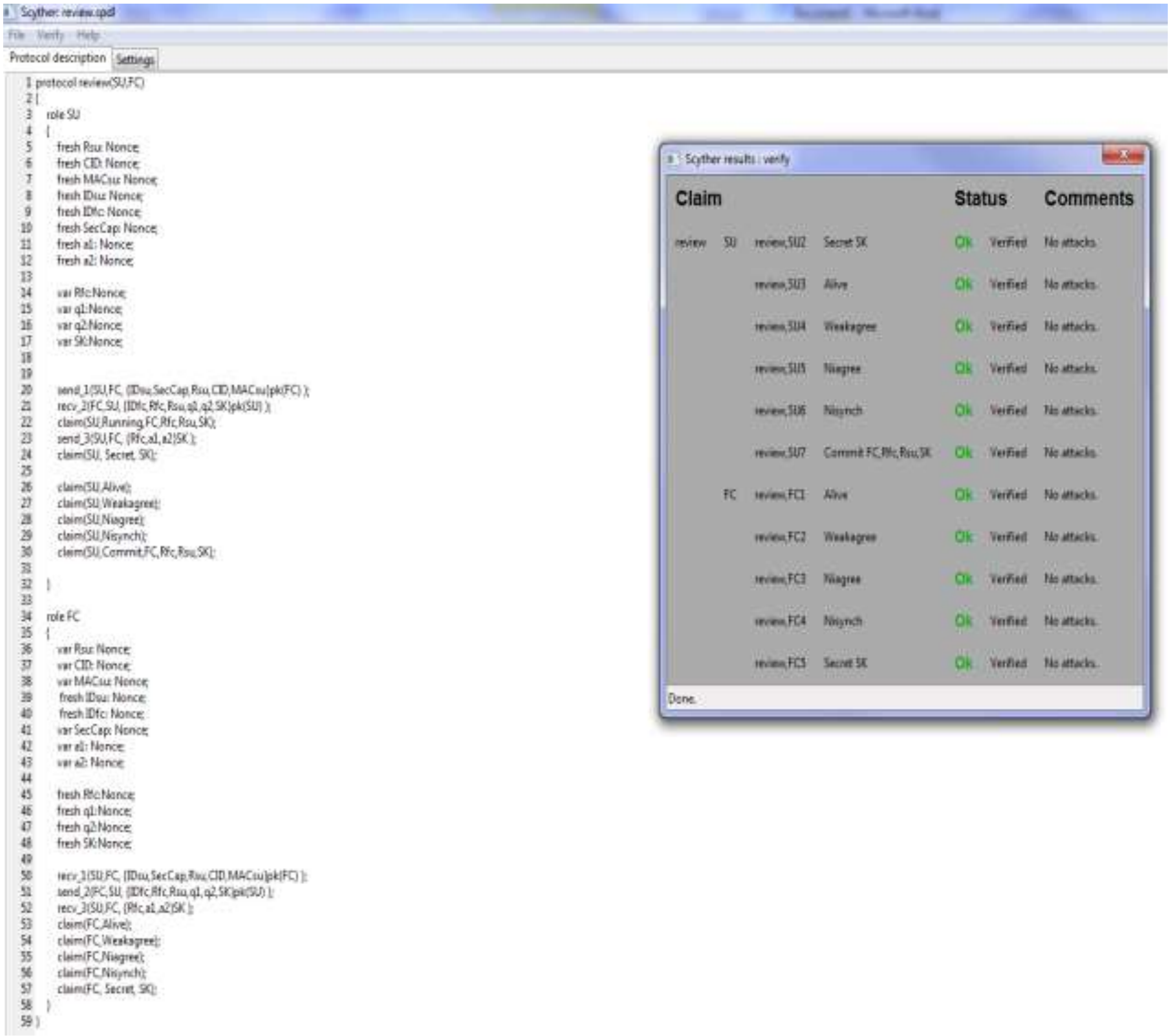
Derivations (c) and (d) are the objectives of our proposed authentication scheme on the CH's level.

3.3.2 Verification through Scyther

We verified the vulnerability of the proposed authentication mechanism to potential well-known attacks such as reflection attack, man-in-the-middle attack and denial of service (DoS) attack, by using the Scyther verification tool [76]. We set up the verification environment by using the following settings parameters shown in Table 3.4. We then, described the algorithm messages sent between the two entities, the joining node and the authenticating party (FC and CH). After the verification run has completed, a "no attacks" messaged popped up as show in Figures 3.4 and 3.5. It shows that our protocol is safe against the multiple attacks mentioned earlier, as "no attacks" break the verification process. Moreover, the “status of each message is “OK, verified”, which means that each message has been received correctly by the destination with no alteration (i.e. same at it has been sent by the source). These attacks are analyzed in the following section and we show how they are eliminated through our authentication mechanism.

TABLE 3.4 VERIFICATION ENVIRONMENT PARAMETERS

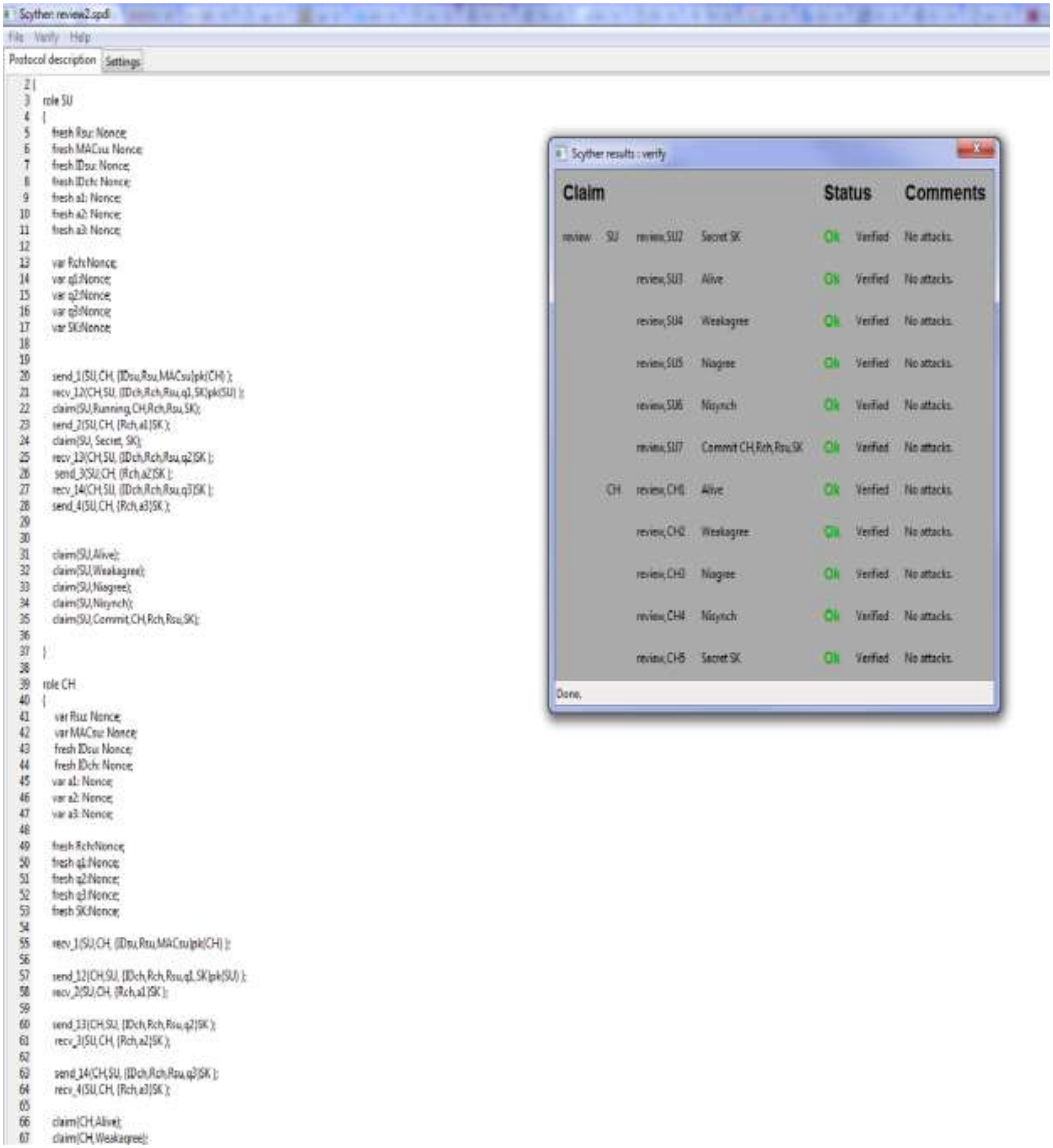
Parameter	**Value**
Maximum Number of Runs	1000
Matching Type	Find all type flaws
Search Running	Find all attacks
Maximum Number of Patterns per Claim	100



```
protocol review(SU,FC)
{
  role SU
  {
    fresh Rsu: Nonce;
    fresh CID: Nonce;
    fresh MACsu: Nonce;
    fresh IDsu: Nonce;
    fresh IDfc: Nonce;
    fresh SecCap: Nonce;
    fresh a1: Nonce;
    fresh a2: Nonce;

    var Rfc:Nonce;
    var q1:Nonce;
    var q2:Nonce;
    var SK:Nonce;


    send_1(SU,FC, {IDsu,SecCap,Rsu,CID,MACsu}pk(FC) );
    recv_2(FC,SU, {IDfc,Rfc,Rsu,q1,q2,SK}pk(SU) );
    claim(SU,Running,FC,Rfc,Rsu,SK);
    send_3(SU,FC, {Rfc,a1,a2}SK );
    claim(SU, Secret, SK);

    claim(SU,Alive);
    claim(SU,Weakagree);
    claim(SU,Niagree);
    claim(SU,Nisynch);
    claim(SU,Commit,FC,Rfc,Rsu,SK);

  }

  role FC
  {
    var Rsu: Nonce;
    var CID: Nonce;
    var MACsu: Nonce;
     fresh IDsu: Nonce;
     fresh IDfc: Nonce;
    var SecCap: Nonce;
    var a1: Nonce;
    var a2: Nonce;

    fresh Rfc:Nonce;
    fresh q1:Nonce;
    fresh q2:Nonce;
    fresh SK:Nonce;

    recv_1(SU,FC, {IDsu,SecCap,Rsu,CID,MACsu}pk(FC) );
    send_2(FC,SU, {IDfc,Rfc,Rsu,q1,q2,SK}pk(SU) );
    recv_3(SU,FC, {Rfc,a1,a2}SK );
    claim(FC,Alive);
    claim(FC,Weakagree);
    claim(FC,Niagree);
    claim(FC,Nisynch);
    claim(FC, Secret, SK);
  }
}
```

```
Claim                                                  Status          Comments

review   SU   review,SU2   Secret SK                   Ok   Verified   No attacks.
              review,SU3   Alive                       Ok   Verified   No attacks.
              review,SU4   Weakagree                   Ok   Verified   No attacks.
              review,SU5   Niagree                     Ok   Verified   No attacks.
              review,SU6   Nisynch                     Ok   Verified   No attacks.
              review,SU7   Commit FC,Rfc,Rsu,SK        Ok   Verified   No attacks.
         FC   review,FC1   Alive                       Ok   Verified   No attacks.
              review,FC2   Weakagree                   Ok   Verified   No attacks.
              review,FC3   Niagree                     Ok   Verified   No attacks.
              review,FC4   Nisynch                     Ok   Verified   No attacks.
              review,FC5   Secret SK                   Ok   Verified   No attacks.
Done.
```

Figure 3.4: The Results of Executing the Proposed Authentication Mechanism at FC Level in Scyther Environment.



```
{
role SU
{
   fresh Rsu: Nonce;
   fresh MACsu: Nonce;
   fresh IDsu: Nonce;
   fresh IDch: Nonce;
   fresh a1: Nonce;
   fresh a2: Nonce;
   fresh a3: Nonce;

   var Rch:Nonce;
   var q1:Nonce;
   var q2:Nonce;
   var q3:Nonce;
   var SK:Nonce;


   send_1(SU,CH, {IDsu,Rsu,MACsu}pk(CH) );
   recv_12(CH,SU, {IDch,Rch,Rsu,q1, SK}pk(SU) );
   claim(SU,Running,CH,Rch,Rsu,SK);
   send_2(SU,CH, {Rch,a1}SK );
   claim(SU, Secret, SK);
   recv_13(CH,SU, {IDch,Rch,Rsu,q2}SK );
    send_3(SU,CH, {Rch,a2}SK );
   recv_14(CH,SU, {IDch,Rch,Rsu,q3}SK );
   send_4(SU,CH, {Rch,a3}SK );


   claim(SU,Alive);
   claim(SU,Weakagree);
   claim(SU,Niagree);
   claim(SU,Nisynch);
   claim(SU,Commit,CH,Rch,Rsu,SK);

}

role CH
{
    var Rsu: Nonce;
    var MACsu: Nonce;
    fresh IDsu: Nonce;
    fresh IDch: Nonce;
   var a1: Nonce;
   var a2: Nonce;
   var a3: Nonce;

   fresh Rch:Nonce;
   fresh q1:Nonce;
   fresh q2:Nonce;
   fresh q3:Nonce;
   fresh SK:Nonce;

   recv_1(SU,CH, {IDsu,Rsu,MACsu}pk(CH) );

   send_12(CH,SU, {IDch,Rch,Rsu,q1, SK}pk(SU) );
   recv_2(SU,CH, {Rch,a1}SK );

   send_13(CH,SU, {IDch,Rch,Rsu,q2}SK );
    recv_3(SU,CH, {Rch,a2}SK );

    send_14(CH,SU, {IDch,Rch,Rsu,q3}SK );
    recv_4(SU,CH, {Rch,a3}SK );

   claim(CH,Alive);
   claim(CH,Weakagree);
```

```
Claim                                                  Status          Comments

review   SU   review,SU2   Secret SK                   Ok   Verified   No attacks.
              review,SU3   Alive                       Ok   Verified   No attacks.
              review,SU4   Weakagree                   Ok   Verified   No attacks.
              review,SU5   Niagree                     Ok   Verified   No attacks.
              review,SU6   Nisynch                     Ok   Verified   No attacks.
              review,SU7   Commit CH,Rch,Rsu,SK        Ok   Verified   No attacks.
         CH   review,CH1   Alive                       Ok   Verified   No attacks.
              review,CH2   Weakagree                   Ok   Verified   No attacks.
              review,CH3   Niagree                     Ok   Verified   No attacks.
              review,CH4   Nisynch                     Ok   Verified   No attacks.
              review,CH5   Secret SK                   Ok   Verified   No attacks.
Done.
```

Figure 3.5: The Results of Executing the Proposed Authentication Mechanism at CH Level in Scyther Environment.

3.4 Security Analysis

We formally validated the authentication mechanism through two different formal verification techniques. We now discuss the proposed authentication scheme informally, in terms of its ability to fulfil security requirements and prevent multiple attacks. The proposed scheme is a secure scheme as long as it disallows any adversary node from accessing the network. In this section, we show the security properties (requirements) that our two-level authentication scheme fulfills. Moreover, we show the attacks that are prevented by our authentication scheme.

3.4.1 Authentication

As mentioned above, authentication is one of the security requirements that a secure network has to fulfill. Our proposed authentication scheme ensures that a node cannot get access to network resources until it gets authenticated. Moreover, applying a two level of authentication strengthens the authentication process and reduces or even cancels the opportunity for a malicious node to cheat the FC or the CH.

3.4.2 Resource Availability and Accessibility

In the proposed scheme, network resources are only allocated to authenticated nodes. Nodes that are not authenticated are not allowed to access the resources; therefore, the resources are available for authenticated nodes only. This enhances the network security and network performance.

3.4.3 Reflection Attack

It is an attack that targets any challenge-response authentication scheme wherein the attacker contacts a third party to get a response to the authenticating node’s challenge. By our proposed authentication scheme, random numbers (nonce) are generated as a challenge to the joining node that has to send its identifier with the received nonce, as well as its own random number encrypted by its private key. The FC or the CH, whichever is the authenticator, decrypts this message and checks the random nonce number of the joining node. If they do not match, the reflection attack is detected and prevented. Therefore, the reflection attack cannot be launched with our authentication scheme.

3.4.4 Man-in-the-Middle Attack

In this attack, a malicious node accesses or invades communication between two parties. It impersonates both parties and gains access to information that the two parties were trying to send to each other. It allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until the action is complete. By our proposed authentication scheme, all messages exchanged between the joining node and the authenticator (FC or CH) are encrypted by the receiver's public key or the symmetric key, which ensures that the only one that can decrypt and understand the entire message is the one that has the corresponding private key or the symmetric key. Therefore, this attack can be easily detected and mitigated by our proposed authentication scheme.

3.4.5 Denial of Service Attack

A malicious node may eavesdrop on the communication between two nodes and drop the messages exchanged between the communicating nodes in order to reduce the network performance. Another example of DoS attack is that a malicious node may inject the network with meaningless messages, which influence other nodes' performance. By our proposed authentication, the FC accepts authentication requests from nodes that are already predefined in a manufacture. If a node that belongs to this list launches the DoS attack, the FC will receive multiple requests from this node in order to flood the network. Therefore, the FC quickly and effectively identifies incoming traffic as malicious. Once the flood of traffic is identified as a DoS attack, an effective response is taken to absorb the attack, until the source is identified and blocked. This response contains releasing the assigned channels, setting its belief level value to zero and notifying the cluster heads about this node in order to prevent any node from communicating with this malicious node.

3.5 Summary

Cognitive radio is considered as a promising technology to solve the spectrum scarcity problem. The CR nodes are more exposed to security vulnerabilities and threats because of their wireless nature. Secure communication is one of the challenging tasks in CRNs. A CR node cannot access the spectrum unless it has been authenticated by a reliable node. In this chapter, we propose a two-level secure authentication scheme in CRN wherein the authenticating node and the joining node accept a key agreement. We use the advantages of the public-key and the symmetric-key cryptography to secure the messages exchanged between the communicating nodes. During the authentication process and after a symmetric key is shared between the communicating nodes, any communication would be carried out using the symmetric key cryptography.

The proposed authentication scheme, in comparison to the existing approaches, reduces the number of cryptographic operations and the authentication time needed to complete the authentication process. Moreover, the correctness of the proposed approach has been verified using the BAN logic and through the Scyther verification tool. We showed that our authentication scheme is safe against multiple attacks.

Chapter 4: Monitoring Nodes Behavior during Spectrum Sensing Mechanism

In this chapter, we propose a novel collaborative approach during spectrum sensing process that monitors the behavior of sensing nodes and identifies the malicious and misbehaving sensing nodes. To the best of our knowledge, this work is the first effort that focuses on addressing the attacker behavior rather than the attack itself. By monitoring the sensing nodes behavior, multiple passive and active attacks can be mitigated. The proposed approach measures the node's sensing reliability through a value called belief level, which is assigned to each communicating node during the authentication process (Chapter 3).

The main contributions in this chapter can be summarized as following:

- To the best of our knowledge, it is the first work in CRNs security that focuses on addressing the adversary nodes' behaviors more than addressing the attacks themselves. By doing so:
    - It mitigates multiple attacks other than just PUEA and SSDF attacks, such as DoS, collusion, and objective function attacks.
    - It works as a reactive approach to active attacks and as a proactive approach to passive attacks.
    - In increases the probability of detecting adversary nodes, which therefore improves the spectrum utilization.
- It increases the probability of detecting vacant spectrum channels and it also decreases the false alarm probability.
- It secures the sensing-reputation reports exchanged between the different sensing nodes by encrypting the messages carrying them through the public and symmetric key cryptography.

This chapter is organized as follows: firstly, the system requirements and the general assumptions are shown in Section 4.1. Then, the description of the threat model that we are addressing is described in Section 4.2. Next in Section 4.3, the proposed approach for monitoring nodes' behavior is described. After that in Section 4.4, the performance of the proposed approach is measured and compared with other approaches in the literature. Next in Section 4.5, the proposed approach is validated informally from different security perspectives. The chapter is concluded with a summary in Section 4.6.

4.1 System Requirements and General Assumptions

The system used in the proposed approach is the same one shown in Figure 1.3 of Chapter 1. Each sensing node is assigned a value called belief level (BL), which describes the accuracy and reliability of the sensing nodes that participate in making the final sensing decision. The belief level of each node is the key element of the proposed approach as it will be used to correctly monitor the sensing nodes' behavior and detect the adversary nodes during the spectrum sensing phase. We assume four categories of trust and the BL has a range of [0-4] based on these categories of trust as following:

$$0 \leq \mathrm{BL} \leq 1 \text{: Very\_Untrusted}$$

$$1 < \mathrm{BL} < 2 \text{: Untrusted}$$

$$2 \leq \mathrm{BL} < 3 \text{: Trusted}$$

$$3 \leq \mathrm{BL} \leq 4 \text{: Very\_Trusted}$$

Each node is assigned an initial moderate belief level (BL) of value equal to two i.e. it is in the "Trusted" category.

In each cluster, one node is chosen by the FC as a cluster head (CH) that has the highest BL. At the time of cluster formation any node is randomly chosen as a CH as all the nodes have the same initial BL value. The cluster heads are not fixed all the time; whenever, a new node is added to a cluster and it has a higher BL than the current CH's BL, the new node will be selected as a CH. The energy detection method is used by all SUs to detect the presence or absence of the PU in its spectrum band. The cooperative spectrum sensing is done as in [76], wherein all the cluster nodes sense the spectrum, make a decision about the PU presence/absence and forward their decision to other nodes.

4.2 The Mechanism

4.2.1 Preface

The sequence diagram of the proposed approach is shown in Figure 4.1 that starts with exchanging nodes' certificates. Each node's certificate is validated by Server S. Upon the success of certificates' validation, the joining node sends its ID and its security capabilities to the CH. The CH keeps track of the nodes IDs that participate in the sensing process. The CH then assigns symmetric keys to the sensing nodes. These symmetric keys will be used later for encrypting/decrypting the sensing-reputation reports. Next, the sensing nodes perform the sensing, monitor other nodes' behavior, prepare the sensing-reputation reports and forward them to the CH (Section 4.3.2). These sensing-reputation reports are analyzed in each cluster by its CH to make the final decision about the spectrum availability and the sensing nodes behavior. The CH then forwards the final sensing decisions to its cluster nodes (Section 4.3.3). All cluster nodes are rewarded or penalized based on their behavior in the cluster during the sensing process (Section 4.3.4).

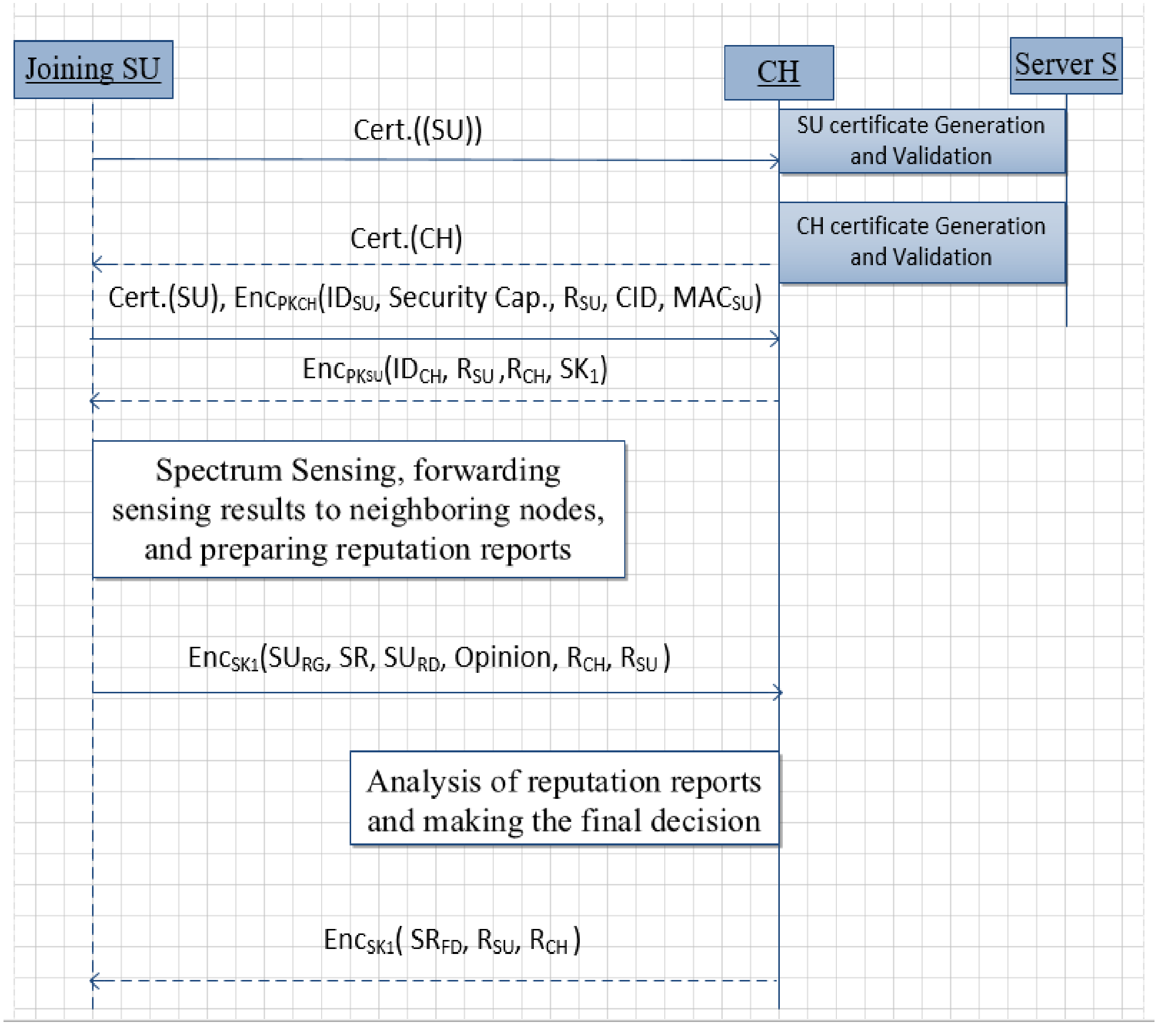

Joining SU
CH
Server S
Cert.((SU))
SU certificate Generation and Validation
Cert.(CH)
CH certificate Generation and Validation
Cert.(SU), $Enc_{PKCH}(ID_{SU}$, Security Cap., R_{SU}, CID, $MAC_{SU})$
$Enc_{PKsu}(ID_{CH}, R_{SU}, R_{CH}, SK_1)$
Spectrum Sensing, forwarding sensing results to neighboring nodes, and preparing reputation reports
$Enc_{SK1}(SU_{RG}$, SR, SU_{RD}, Opinion, $R_{CH}, R_{SU})$
Analysis of reputation reports and making the final decision
$Enc_{SK1}(SR_{FD}, R_{SU}, R_{CH})$

Figure 4.1: System Sequence Diagram.

4.2.2 Monitoring Nodes Behavior

All the clusters nodes perform the spectrum sensing process to find the vacant spectrum channels by using the energy detection technique wherein each sensing node measures the signal strengths in all PU's channels, and by using the energy detection method SUs make the initial binary decision about the presence/absence of PU in its reserved channel(s). Each sensing SU uses the pre-known information about PUs signal (such as signal power threshold and modulation type) and compares it with the sensing signal in order to avoid PUEA. If the received signal does not match the expected signal (i.e. a malicious node emulates PU), the sensing SU broadcasts a message to all cluster nodes notifying them and therefore PUEA is mitigated. However, if they match, it means a PU is present in its spectrum channels. If an SU does not receive any signal over the sensing channel, it decides that the spectrum is free and can be used. Each sensing node forwards its sensing decision(s) to its neighbors, compares their sensing results with its sensing results, prepares sensing-reputation reports about their neighboring node(s), and forwards these reports to the CH.

In case PUEA is avoided as mentioned earlier, each sensing SU senses the spectrum and saves its sensing results in a parameter called the *sensing result* (*SR*). It has two values, either 0 for a free spectrum or 1 for an occupied spectrum by a real PU. The sensing SU forwards its *SR* to its neighboring nodes, which have their own *SR*s. Each sensing node compares its own *SR* with the received *SR* from its neighboring node and if they match with the received *SR*, the sensing node decides that its neighboring node is a "GOOD" node G; otherwise it is a "BAD" node B. The sensing node does the same for all its neighboring nodes.

4.2.3 Analyzing Nodes Behavior

Each node will keep monitoring the behavior of its neighboring nodes and keep sending periodic sensing-reputation reports to its CH about their sensing results and their neighboring nodes' behavior. Sensing-reputation reports sent by each cluster node to its CH have the following format (*Reporting Node ID (RG)* || SR_{RG} || *Reported Node ID (RD)* || *Opinion*) where SR_{RG} is the sensing result of the reporting node and it is either 0 (i.e. "*Free*" spectrum) or 1 (i.e. "*Occupied*" spectrum) and Opinion is about the reported node (*RD*) and it is either 0 (i.e. "*BAD*" node) or 1 (i.e. "*GOOD*" node). Note that a reporting node is a reported node in its neighboring nodes' sensing-reputation reports and a reported node is a reporting node in its own sensing-reputation report. CH is a trustworthy node since its BL is the highest in the trusted range and it is the only node that can check the correctness of the periodic sensing-reputation reports. Upon the reception of the different sensing-reputation reports from the different cluster nodes, CH analyzes these reports by extracting the sensing result of the reporting nodes and their opinion about the reliability of the reported nodes to make the final decision about the spectrum availability and about the nodes behavior.

The sensing-reputation reports analysis of making the final sensing decision, SR_{FD}, is described in Algorithm 4.1. CH forms two groups of nodes, occupied group (OG) and free group (FG), where all the nodes in the same group have the same sensing decision "occupied" or "free", respectively. CH analyzes the sensing-reputation reports received from the trusted nodes in each group only. A trusted node is a node that has its BL greater than or equal to a value called $BL_{threshold}$, which describes the lower limit of a BL for a node to be considered trusted.

CH makes the final decision about the spectrum availability based on the reports sent by different nodes and their BL values and then forwards the final decision to its cluster nodes. A specific rule is applied to process these reports in order to make the final decision about the reported node. The general rule of *K-out-of-N* rule is where *K* users out of *N* users must have the same opinion in order to consider their opinion. In case 50% *K*-rule is used, *K* is equal to N/2.

We propose a new *K*-rule, where *K* represents the number of votes and where we assign each user a different voting weight based on its BL value. We apply the following criteria in order to find the value of *K*:

- A node's decision with a BL value of $3 \leq BL \leq 4$ counts as three votes.
- A node's decision with a BL value of $2.5 \leq BL < 3$ counts as two votes.
- A node's decision with a BL value of $2 \leq BL < 2.5$ counts as one vote.
- A node's decision with a BL value less than 2 does not count.

The total votes' number of the nodes, which have the same sensing decision, has to fulfill the 50% K-rule (i.e. it has to be greater than or equal to a value called $M_{threshold}$), which is equal to half the number of the cluster nodes.

CH analyzes the sensing-reputation reports to determine the malicious and misbehaving reporting and reported nodes as following:

<u>If the reporting node reports "*GOOD*" about the reported node:</u>

- If $(SR_{FD} == SR_{RG} \,\&\&\, SR_{FD} == SR_{RD})$, then it is a true "*GOOD*" opinion→ both the reporting and the reported node are trusted nodes.
- If $(SR_{FD} \,!= SR_{RG} \,\&\&\, SR_{FD} == SR_{RD})$, then it is a true "*GOOD*" opinion → the reporting node is an adversary node that wants to falsify the sensing result (i.e. → the reporting node launches SSDF attack).
- If $(SR_{FD} == SR_{RG} \,\&\&\, SR_{FD} \,!= SR_{RD})$, then it is a false "*GOOD*" opinion → both the reporting and the reported node are adversary nodes. The reported node wants to falsify the sensing result (i.e. the reported node launches the SSDF); while the reporting node wants to send false report about the reported node (i.e. the reporting node launches Collusion attacks).
- If $(SR_{FD} \,!= SR_{RG} \,\&\&\, SR_{FD} \,!= SR_{RD})$, then it is a false "*GOOD*" opinion → both the reporting and the reported node are adversary nodes (both the nodes launch the SSDF and the Collusion attacks).

<u>If the reporting node reports "*BAD*" about the reported node:</u>

- If $(SR_{FD} == SR_{RG} \,\&\&\, SR_{FD} == SR_{RD})$, then it is a false "*BAD*" opinion → the reporting node is an adversary node. The reporting node wants to send false report about the reported node (i.e. the reporting node launches Collusion attack).

- If $(SR_{FD}\ != SR_{RG}$ && $SR_{FD} == SR_{RD})$, then it is a false "*BAD*" opinion → the reporting node is an adversary node that wants to falsify the sensing result and wants to send false report about the reported node (i.e. the reporting node launches SSDF and Collusion attacks).
- If $(SR_{FD} == SR_{RG}$ && $SR_{FD}\ != SR_{RD})$, then it is a true "*BAD*" opinion → the reported node is an adversary node that wants to falsify the sensing result (i.e. the reported node launches the SSDF attack).
- If $(SR_{FD}\ != SR_{RG}$ && $SR_{FD}\ != SR_{RD})$, then it is a false "*BAD*" opinion → both the reporting and the reported node are adversary nodes (both the nodes launch SSDF and Collusion attacks).

In summary, each node is given a variable weight of votes based on its BL, and this variable votes' weight affects the final sensing results decision. The nodes behavior is analyzed based on the final sensing results decision. Note that we assume the channels carrying the sensing-reputation reports are error-free and each sensing-reputation report has a timestamp associated to it. If CH does not receive a sensing-reputation report from a node within its timestamp, CH considers the node as an adversary node.

ALGORITHM 4.1: FINAL DECISION OF SPECTRUM SENSING

```
Initialization
$OG$: All reporting nodes including CH that have SR $= 1$
$FG$: All reporting nodes including CH that have SR $= 0$
$C$: Number of SUs in a cluster
$BL_{threshold}$: Threshold value of the reporting node's belief level
$M_{threshold}$: Threshold value of the number of nodes that should have the same sensing decision and is equal to $\lceil C/2 \rceil$
$OccupiedCount$: Votes count of reporting nodes that have SR $= 1$ and initialized to zero
$FreeCount$: Votes count of reporting nodes that have SR $= 0$ and initialized to zero
$SR_{FD}$: Final sensing decision
$SR_{CH}$: The sensing decision of the CH
$RG$: The reporting node
$KRule(BL_{RG_m})$: Function to calculate the votes count for each node
$K$: Total votes for all nodes and initialized to zero
…………………………………………………………………………....
 $\forall RG_i \in OG$
    $IF\ (BL_{RG_i} \geq BL_{threshold})$
          $OccupiedCount += KRule(BL_{RG_i})$
                                                         =====================
$\forall RG_j \in FG$
    $IF\ (BL_{RG_j} \geq BL_{threshold})$
          $FreeCount += KRule\ (BL_{RG_j})$
                                                         =====================
$IF\ (OccupiedCount \geq M_{threshold}\ \&\&\ OccupiedCount > FreeCount)$
        $SR_{FD} = 1$

$else\ IF(FreeCount \geq M_{threshold}\ \&\&\ FreeCount > OccupiedCount)$
        $SR_{FD} = 0$
$else$
        $SR_{FD} = SR_{CH}$

$K = OccupiedCount +\ FreeCount$
…………………………………………………………………………...

$KRule(BL_{RG_m})$
{
  $count = 0;$
    $IF\ 3 \leq BL_{RG_m} \leq 4$
              $count = count + 3;$

    $else\ IF\ 2.5 \leq BL_{RG_m} < 3$
              $count = count + 2;$

    $else\ IF\ 2 \leq BL_{RG_m} < 2.5$
              $count = count + 1;$

    $else\ IF\ BL_{RG_m} < 2$
              $count = count + 0;$
 $return\ count;$
}
```

4.2.4 Reward/Penalty Mechanism

CH adjusts the belief level of each node based on whether a node is to be rewarded or penalized. Each “GOOD” behaving node will be rewarded by increasing its BL. Each “BAD” behaving node will be penalized by decreasing its BL and applying a proper penalty action according to a value called Adjustment Factor (AF) that is calculated by CH as in equation (4.1). It is then added to the latest value of BL as in equation (4.2). AF is calculated according to the number of “GOOD” and “BAD” reports sent by the reporting nodes about the reported node.

$$at\ t = t_{update}$$

$$AF_{SU_i} = \left(\sum_{g=1,\neq i}^{G} \propto *\ \mathbb{N}(BL_{SU_g})\right) - \left(\sum_{b=1,\neq i}^{B} \beta\ *\ \mathbb{N}(BL_{SU_b})\right) \tag{4.1}$$

$$s.t. -4 \leq AF \leq 4$$

where G and B represent the number of nodes, which decide that SU_i is a good or bad node, respectively. $\propto$ is the rewarding factor, and β is the penalizing factor, $\mathbb{N}(BL_{SU_b})$ is the normalized belief level of the node which reports that SU_i is a bad node, and $\mathbb{N}(BL_{SU_g})$ is the normalized belief level of the node which reports that SU_i is a good node. The rewarding factor and the penalizing factor are chosen as in real life where penalty has more weight than rewarding.

$$\left(BL_{SU_i}\right)_{t_{update}} = \left(AF_{SU_i}\right) + \left(BL_{SU_i}\right)_{t_{update-1}} \tag{4.2}$$

Equation (4.2) finds the updated value of belief level of each cluster node at every reporting round, where $\left(\mathrm{BL}_{\mathrm{SU_i}}\right)_{t_{update-1}}$ is the belief level in the previous updating round.

The maximum and minimum values of AF is 4 and -4 respectively, i.e. if AF value is more than 4, it will be set to 4 and if it is less than -4 it will be set to -4. The BL of each reporting cluster node is important in the process of finding the AF; the higher the BL of a reporting cluster node is, the higher the effect on the AF value is.

Normal behaving sensing nodes will be rewarded for their normal behavior, which allows them to gain higher belief level in the cluster. Consequently, the normal behaving node benefits from that as it can have enough resources to fulfill its QoS requirements. On the other hand, an adversary node (attacker) is penalized by decrementing its BL and applying penalty action(s) for its abnormal activity in the network. The penalty mechanism affects the attacker throughput as that decreases its belief level and reduces the resources assigned to it, which therefore results in a low throughput. Consequently, the desire of other cluster nodes to communicate with the misbehaving node during data transmission phase is low; hence, no node will want to behave in an abnormal way. CH penalizes the adversary node by applying the proper penalty actions according to the AF value. These penalty actions are:

- *P1:* give a time out for three sensing rounds.
- P2: de-allocate 50% of the assigned resources to the adversary node, where resources are the channels allocated to the user SU_i at the end of the negotiation phase during the authentication process.
- *P3*: de-allocate all resources and disconnect this adversary node.
- *P4*: mark the adversary node as an undesirable node.

Table 4.1 shows the proposed penalty scheme which depends on other cluster nodes' decision about each other.

TABLE 4.1 PENALTY SCHEME

Adjustment Factor (AF)	**Penalty Action(s)**
$-1 < \mathrm{AF} \leq 0$	No extra penalty

$-2 < \mathrm{AF} \leq -1$	P1
$-3 < \mathrm{AF} \leq -2$	P1 and P2
$-4 < \mathrm{AF} \leq -3$	P3
-4	P3 and P4

4.2.5 Analysis of Detection and False Alarm Probability

We use the value of K (calculated as in Algorithm 4.1 in Section 4.3.3) to formulate the detection probability P_D^{BL} which is the probability of identifying a malicious reported node as malicious or the probability of identifying a used spectrum as used, as shown in equation (4.3).

$$P_D^{BL} = \begin{cases} \sum_{i=K}^{C} \binom{C}{i} {P_d}^{i} (1 - P_d)^{C-i}, & K < C \\ 1 & K \geq C \end{cases} \tag{4.3}$$

where P_d denotes the individual detection probability of the reporting node, and C is the number of SUs in each cluster.

A malicious reporting node is a node that sends false sensing-reputation reports to CH. A false sensing-reputation report is a report that has a false opinion about a reported node or a false sensing result. When CH receives the sensing-reputation reports from the reporting nodes, it analyzes these reports to find if the reporting/reported node is an adversary node or not. The probability for CH to make a wrong decision about the reporting/reported node or about the spectrum availability is denoted as probability of false alarm, $P_F(C, K)$, as in equation (4.4) where P_f denotes the individual false alarm probability of the reporting node, (i.e. it is the probability that the reporting node erroneously transmit a false sensing-reputation to the CH).

$$P_F(C,K) = \begin{cases} \sum_{i=K}^{C} \binom{C}{i} {P_f}^i \left(1 - P_f\right)^{C-i}, & K < C \\ 1 & K \geq C \end{cases} \tag{4.4}$$

A malicious reporting node (SU_z) will try to send false sensing-reputation reports to CH with a probability of success $P_s^{SU_z}$ as in equation (4.5).

$$P_s^{SU_z} = \frac{BL_{SU_z}}{BL_{max}} * \frac{1}{2^{BV}} \tag{4.5}$$

where BL_{SU_z} is the belief level of the malicious reporting node (SU_z) and BV is the number of bad votes about SU_z.

The probability of false alarm using our mechanism can be expressed as in equation (4.6) where $P_F(C,K)$ is obtained from equation (4.4).

$$P_F^{BL} = \sum_{i=1}^{Y} \prod_{z\in(1,i)} [P_s^{SU_z}] \prod_{z\in(1,i)} [1 - P_s^{SU_z})] \, P_F(C,K) \tag{4.6}$$

where Y is the number of malicious reporting nodes, and K represents the total number of votes of the malicious reporting node(s) about the same reported node. K is calculated in the same way as in the *K*-rule used for the spectrum sensing decision, however this time the $BL_{threshold}$ is equal to 2.5 (i.e. the node(s) should have a BL value higher than or equal to 2.5 in order for its sensing-reputation report to be analyzed by the CH). The reason behind that is to consider the reputation part of the sensing-reputation reports sent only by trusted nodes with high BLs.

Collusive cluster nodes or compromised node(s) can send false sensing results or report a benign node as misbehaving node. In the case of targeting a benign node, the collusion attack occurs if multiple nodes report to CH about a benign node that this benign node is a "*BAD*" node while in real it is not. Our approach prevents any node from acting as a collusive node or compromised node by analyzing and comparing the different reports sent by different cluster nodes about the benign node. In other words, CH applies one of five different actions to the reported and the reporting nodes. These actions are A1 (Do nothing), A2 (Increment its BL), A3 (Decrement its BL), A4 (Decrement its BL after five nonconsecutive or three consecutive "*BAD*" reports about its neighboring reported node), and A5 (Penalize the adversary node by one of the penalty actions).

4.3 Performance Evaluation

4.3.1 Complexity Analysis

In this section, we discuss the complexity of the monitoring nodes behavior algorithm proposed, including the sensing phase, in terms of computation overhead and communication overhead. In our proposed algorithm, all SUs are divided into different clusters and the cluster nodes communicate with their CHs instead of communicating with a centralized point (i.e. FC). This reduces the amount of computation and resource management; therefore, improves the security level of the network.

Firstly, we analyze the computation overhead in the proposed approach and in the centralized model with no clusters. In the centralized model with no clusters, a bidirectional way of messaging between all SUs and the FC is used. Therefore, the FC needs to manipulate $2 * |\mathrm{M}|$ messages, where M represents the total number of SUs. In the proposed model using clusters, the FC manipulates $2 * |\mathrm{K}|$, where K represents the number of cluster heads. The computation overhead at the FC in both approaches is $\approx O(M)$ and $\approx O(K)$, respectively. However, $|\mathrm{K}| < |M|$; therefore, our approach reduces the computation overhead at the FC.

In our proposed approach, the number of messages that the CH has to manipulate is $|\mathrm{N}|$ messages, where N represents the number of SUs in the cluster. Therefore, the computation overhead at the CH is $\approx O(N)$.

Secondly, we use the number of messages exchanged to also calculate the communication overhead. The number of messages is equal to that used in the computation overhead calculation; therefore, the communication overhead at the FC with no clustering is $\approx \mathrm{O(M)}$, at the FC with clustering is $\approx O(K)$, and at the CH is $\approx O(N)$ where $|K| < |N| < |M|$.

4.3.2 Simulation Environment Setup

We simulate the proposed approach using MATLAB to identify the adversary sensing nodes during the spectrum sensing phase. Table 4.2 shows the network simulated with values used for the parameters required in our approach. We use two different values of $BL_{threshold}$. It is equal to 2 when the algorithm is applied to find the available spectrum channels, while it is 2.5 when the algorithm is used to detect the adversary nodes. The reason behind that is sending a reputation decision about other nodes is more important than sensing a sensing decision about the spectrum. In other words, a node should have a higher BL in order to analyze its reputation decision of its sensing-reputation report by the CH. The simulation results are analyzed from two perspectives. First, the importance and the effects of the concepts used in the proposed approach such as (monitoring nodes behavior, BL, K-rule, and detection and false alarm probability) are analyzed as shown in Figures 4.2-4.5. Second, a comparison is made between the proposed approach and the other approaches in the literature in terms of detection probability and false alarm probability as shown in Figures 4.6-4.8. The detection probability found in equation (4.3) of our approach is compared with that of INCA [44] and with two other approaches as we refer them as Model A and Model B proposed in [39] and [40] respectively. Moreover, we compare the false alarm probability found in equation (4.6) in our approach with that in Model A and Model B [39-40].

TABLE 4.2 SIMULATION PARAMETERS

Parameter	Value
Number of SUs	[0-125]
Number of Clusters	[0-15]
Number of malicious nodes	5% of SUs
α	0.3
β	0.7
$BL_{threshold}$	2 (for the spectrum sensing final decision) 2.5 (for the adversary node detection)
BL_{CH}	[2-4]
P_d	0.8
P_f	0.2

4.3.3 Numerical Results

The normal behavior of any cluster node in our proposed model is illustrated in Fig. 4.2 as each node starts with a moderate belief level and keeps gaining more belief through the spectrum sensing phase until it reaches the maximum belief level of four. All nodes aim at increasing their BL in the network. On the other hand, the adversary node (even with a maximum belief level value of four) can have its belief level decreased to the minimum value of zero due to its abnormal behavior in the cluster.

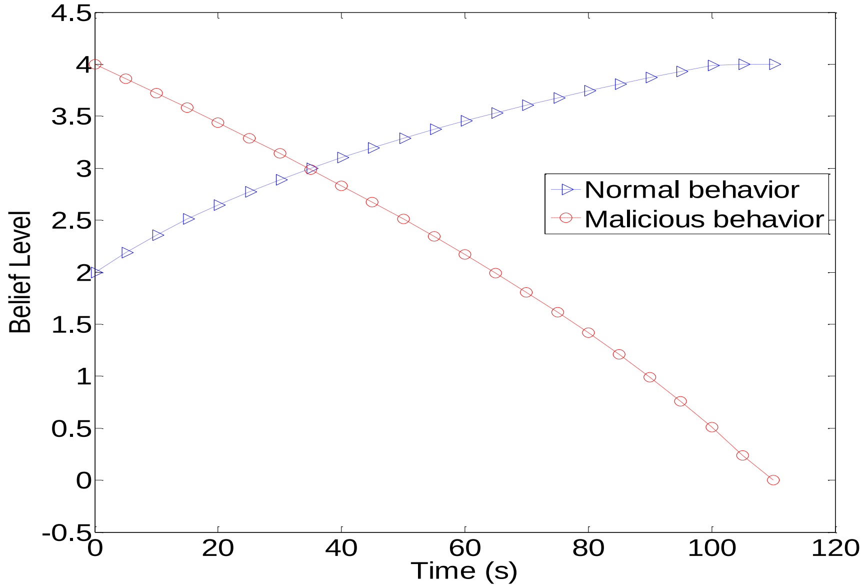


Figure 4.2: Belief Level over Time.

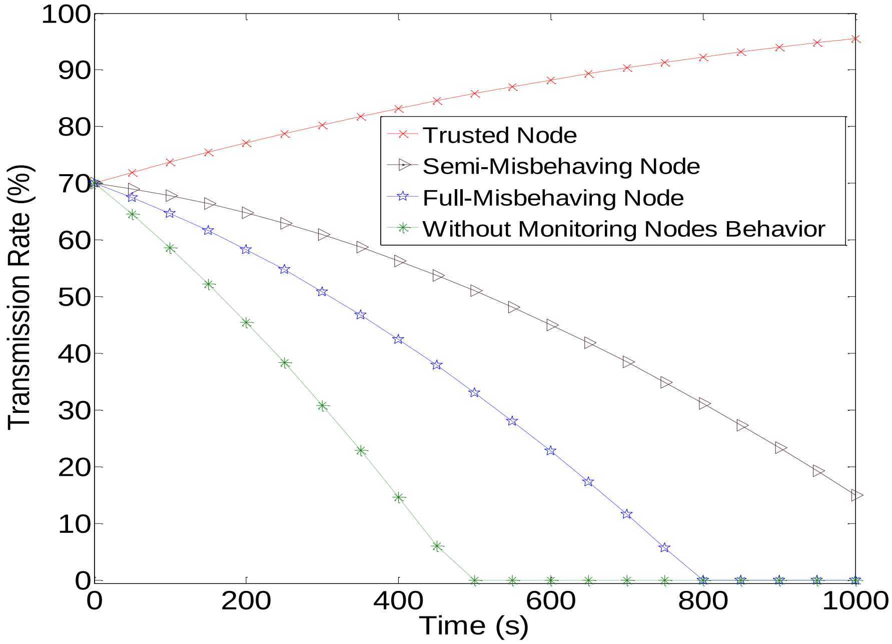


Figure 4.3: Transmission Rate over Time.

The transmission rate in our proposed model is compared with and without monitoring nodes behavior as shown in Fig. 4.3. We assume all nodes initially achieve 70 percent of their desired transmission rate. The behavior of the trusted nodes, the semi-misbehaving nodes and the full-misbehaving node is monitored. The normal behavior of the trusted node makes its BL increase and therefore, its transmission rate increases gradually. The semi-misbehaving node lures some nodes in the cluster; therefore, those nodes vote “BAD” while other nodes vote “GOOD” about its behavior. Overall, its BL relatively decreases (i.e. |AF| is less than 3) and therefore its transmission rate decreases. The transmission rate of the full-misbehaving node that lures all nodes in the cluster decreases rapidly and its BL reaches zero in a shorter time; since, all the cluster nodes vote “BAD” about its behavior (i.e. |AF| is greater than 3). The transmission rate of an adversary node without monitoring its behavior (i.e. no BL associated to the node’s behavior) is also measured. It is found that its transmission rate decreases and reaches zero faster due to its malicious behavior.

Figure 4.4 illustrates the effects of the different number of nodes in a cluster with their BL on the detection probability. It is depicted that with a higher BL, the detection probability increases and (i.e. reaches the maximum value of one) due to the increase in the number of the cooperating SUs. Therefore, when more SUs that have high BL participate in the sensing phase, the detection is completed faster.

Figure 4.5 shows the effects of applying two different K rules on the detection probability in our proposed approach. We assume that the number of SUs in a cluster is 12. In the first K-rule (50%), the detection probability reaches the maximum value of one, when 50% of the users (i.e. six out of twelve SUs) successfully have the same decision. While in our proposed K-rule, the detection probability reaches the maximum value of one when fewer users (i.e. four out of twelve SUs), which have higher BL, make the same decision. In comparison with the 50% K-rule, the detection is completed faster by applying our proposed K-rule.

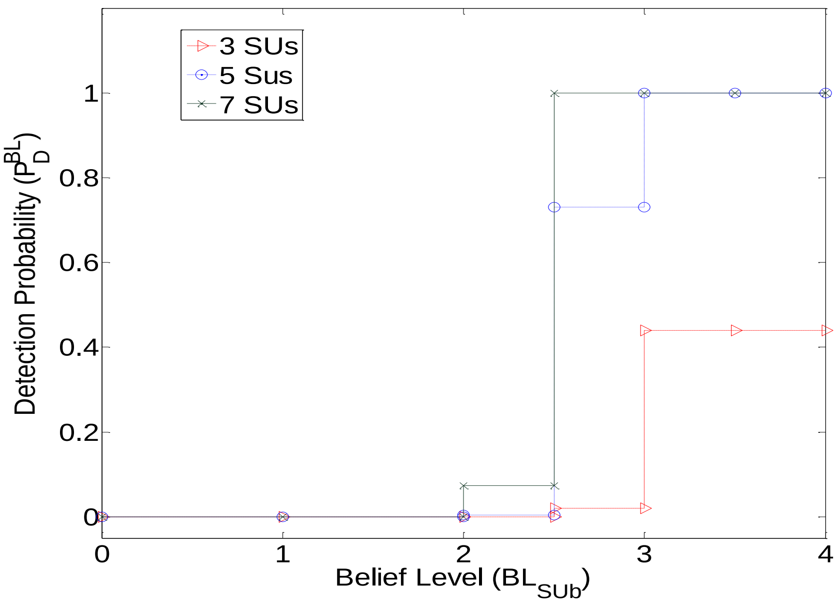


Figure 4.4: Effects of BL on Detection Probability in Proposed Approach.

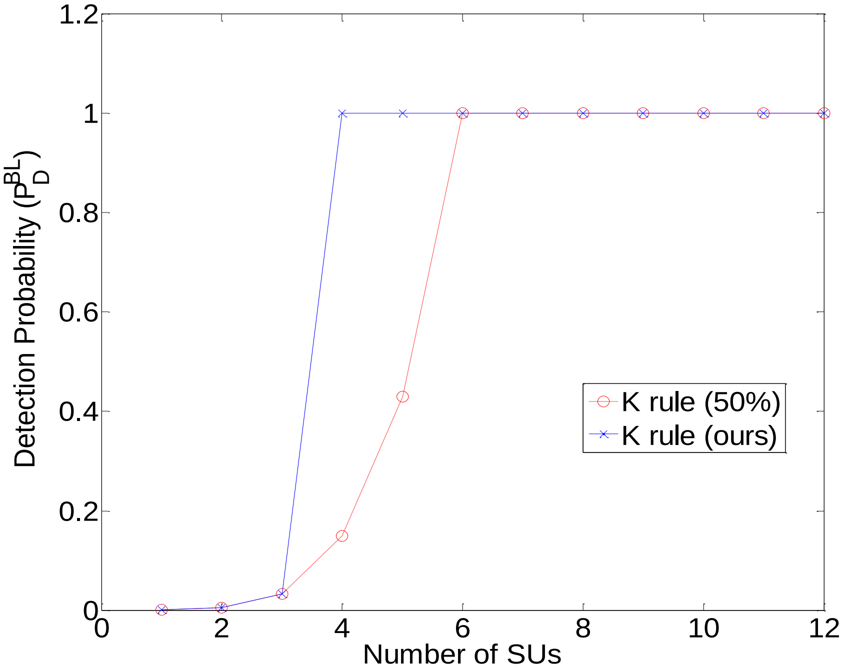


Figure 4.5: Effect of two K rules on Detection Probability in Proposed Approach.

Figure 4.6 compares the detection probability of our proposed model, INCA [44] and Models A and B [39-40]. The detection probability increases when number of sensing SU nodes increases. In INCA, the maximum detection probability is 0.5. In our proposed approach using the proposed K-rule, the detection probability continues to increase to a maximum value of one, where at least nine out of twenty-one nodes in the cluster decide that a node is an adversary node (i.e. number of "*BAD*" reports B=9 nodes). The detection probability in Models A and B keeps increasing; however, it reaches the maximum value of one when all the cluster nodes participate in the detection process. Therefore, our approach outperforms the INCA approach as well as Models A and B as it can reach the maximum value of the detection probability and in a shorter time.

Figure 4.7 compares the false alarm probability of our proposed approach with that of Model A [39] and Model B [40]. In Model A and Model B, the 50% K-rule is applied, while in our proposed model the proposed K-rule is used to calculate the percentage of votes. It is clear from the figure that the false alarm probability decreases as the percentage of votes (i.e. number of the nodes participating in the spectrum sensing process) increases. Our proposed model with the proposed K-rule lowers the false alarm probability compared to the other two models with a reduction of more than 60%. Therefore, our proposed approach outperforms Model A and Model B in terms of lowering the false alarm probability.

In Figure 4.8, the false alarm probability of our proposed model is again compared with that of Model A and Model B, but this time, with respect to the number of malicious (adversary) nodes in the network. It is depicted from the figure that our proposed model with the proposed K-rule outperforms the other two models when the number of malicious nodes increases. The punishment scheme applied by the CH against any malicious node is a possible reason for this advantage. Lowering the false alarm probability increases the security of the network.

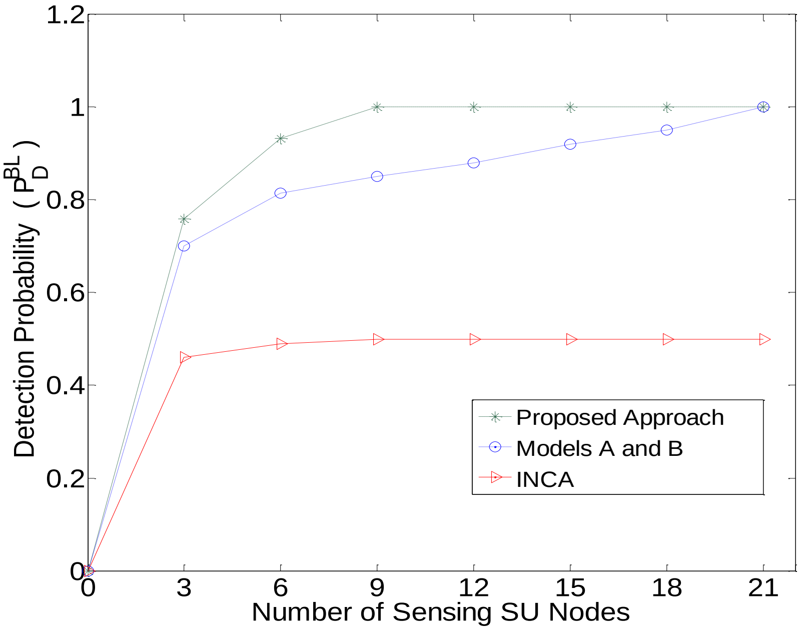


Figure 4.6: Detection Probability (Proposed Approach vs. other Models).

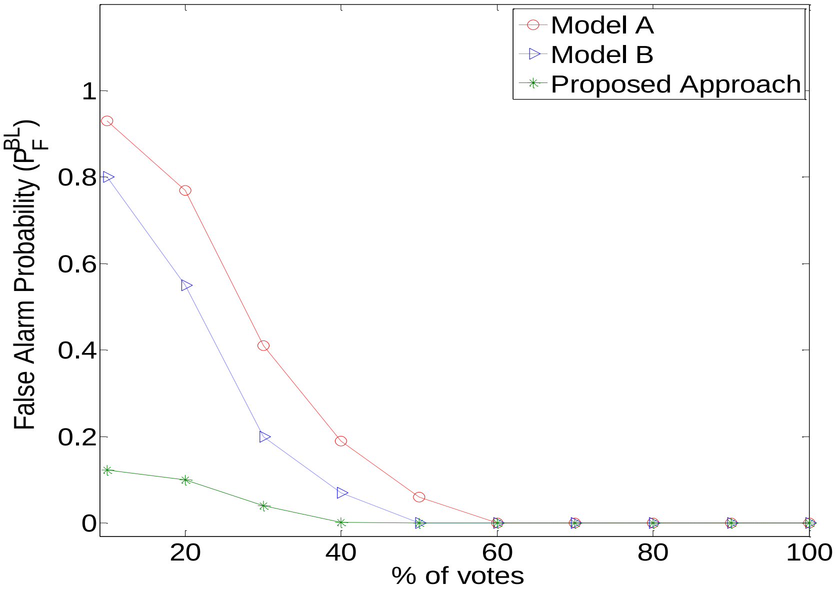


Figure 4.7: A Comparison of False Alarm Probability vs. Percentage of Votes.

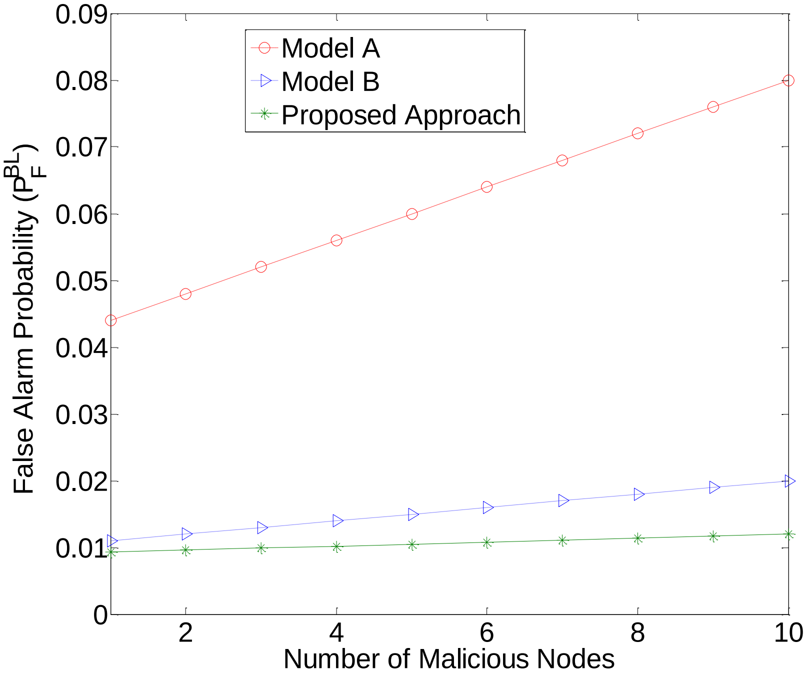


Figure 4.8: A Comparison of False Alarm Probability vs. Malicious Nodes.

4.4 Security Analysis

The proposed model prevents any node from acting in a misbehaving way. Different attacks that might occur because of the abnormal behavior of network nodes (adversary nodes) are eliminated by our proposed collaborative approach.

We show here some attacks that can be detected and mitigated by our collaborative approach. Note that all the simulation results of the detection probability and false alarm probability in the previous section can represent the detection and false alarm probability of the following attacks separately.

4.4.1 PUE Attack Analysis

PUEA is launched when one node emulates the PU by sending signals over PUs channels. When SUs sense the PUs channels, they will receive signals over these channels stating that a PU is present in its channels, while in reality, it is a node that is emulating the real PU. We assume that there is one node emulating PU and sending signals over PUs channels and there is no real PUs using the channels. When SUs sense the PUs channels and receive signals over these channels, each SU compares the received signals with the expected signals in order to check if the received signals belong to a real PU or an adversary node that emulates PU. Based on this comparison, if the sensing node decides that the spectrum is busy, the malicious node is performing as an active PUEA, otherwise it is a passive PUEA. We mitigate both the active and passive PUEA in our approach by applying the collaboration between the different sensing nodes, our belief level mechanism, and making the final sensing decision based on all the sensing nodes' decisions and not based on one node's decision only. More specifically, by applying our proposed K-rule, the SU with the higher BL has a higher weight in making the final decision if the received signal is from a real PU or not. If a node, after analyzing the received signal, decides that this received signal belongs to an emulator, it will send a special sensing-reputation report to its neighbors and CH. CH will collect these special reputation reports and analyze them to make the final decision and based on that the passive PUEA is mitigated. The detection of a PUEA will be faster when the sensing nodes have higher BL; since, the higher BL values give them higher number of votes.

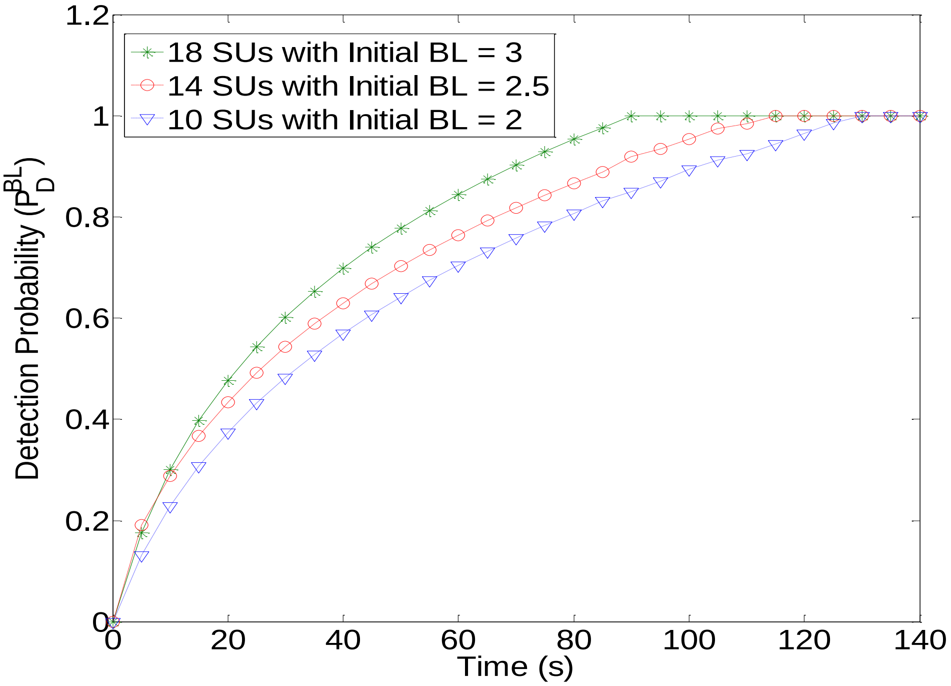


Figure 4.9: Detection Probability of PUEA.

In the case of M SUs sense the spectrum, which have the maximum BL, the detection of PUEA will be faster than that when at least one node does not have the maximum BL. In case of all the nodes are new nodes, which are joining the cluster for the first time (i.e. their BL value is still moderate and have each a value of two), the detection probability will not be high enough in the first sensing round. However, as the sensing is carried out over multiple rounds, the BL of the nodes will increase and the detection probability will continue to increase. The active PUEA is mitigated by the use of the symmetric-key cryptography; since, a node can emulate a PU if it has its shared symmetric key with other nodes, which is not the case in our proposed approach. If a node is an emulating PU, it has to have the PU's symmetric key to send messages over the PUs channels. We simulate a scenario with multiple SUs with different BLs and show the results in Figure 4.9. In this scenario, we assume that a node emulates a PU and it has a BL initially equal to three. We compare the detection probability in three cases: ten SUs with initial BL equal to two, fourteen SUs with initial BL equal to two and a half, and eighteen SUs with initial BL equal to three. It is depicted that the detection probability increases with the time elapse as the BL of the reporting SUs increases and the number of the reporting SUs, which have higher BL, increases. A higher BL of a normal behaving node and a higher number of reporting nodes lead to PUEA detection in a shorter time.

4.4.2 SSDF Attack Analysis

The attacker might send false sensing results to its neighbors stating that the PU is present in its band, when in fact, the PU is not present. The attacker's intention is to gain exclusive access to the spectrum and to prevent other nodes from using the spectrum efficiently. Another form of this attack is when the attacker falsely states that the PU is absent in its band. In this case, the attacker aims to cause interference with the PU and consequently, the PU's QoS is degraded. In both forms, the SSDF might be active or passive. If a malicious node sends its false sensing result to other nodes and the final sensing result was the same as the malicious node's sensing result, active SSDF is launched, otherwise SSDF is passive. Our approach will detect this malicious behavior that leads to active or passive SSDF by applying the collaboration, BL management, and monitoring nodes mechanisms (i.e. each node votes about its neighboring nodes behavior). The final spectrum sensing decision is made based on all the nodes sensing results and in different consecutive sensing rounds (i.e. if one node succeeded to launch SSDF in one sensing round, its chance for relaunching SSDF decreases in the next sensing rounds). With active SSDF attack, the malicious behavior of the node is detected by other nodes that have the opposite sensing decision. Therefore, the votes' weight of the malicious node will be decreased as the sensing time elapse. Moreover, the CH as a trustworthy node can decide if any node is sending false sensing results or false reports about other nodes. In the case of passive SSDF attack, monitoring nodes' behavior and analysis of their behavior, which is done by the CH, reduce the nodes' BL and their votes' weight; hence, passive SSDF is mitigated.

All the nodes will rely on CH's final decision about the spectrum availability. According to our analysis, a malicious node's chance to launch the SSDF attack is high when the node has a high BL or fewer nodes decide that a node is a malicious node. On the other hand, this chance decreases when the number of nodes that decide if a node is a malicious node increases (i.e. when the malicious node's BL decreases). During the reporting rounds, the number of nodes, which decide that a node is a malicious node, increases if the malicious node's sensing results oppose their sensing results, and therefore the malicious node's BL decreases with the reporting time elapse. When the malicious node sends false reports to the CH, the other cluster nodes will vote "BAD" for it and consequently, its BL is decreased.

4.4.3 DoS Attack Analysis

It might be launched at the CH; since, a joining node might show a good behavior at the joining time to become a CH, and then it acts abnormally and cheats about the honesty of other nodes. This adversary joining node aims to reduce the other nodes' belief level value and reduce the network throughput. Such a behavior is prevented by our proposed approach as the clusters are being dynamically reformed whenever a new node is admitted to the network or when a node has a BL that is higher than the CH's BL. Therefore; the cluster heads are not fixed all the time. Moreover, each normal behaving cluster node that is penalized by its malicious CH contacts the FC, which takes appropriate actions against the malicious CH.

It might be launched at SU level as an SU might send any sensing result about the spectrum to its neighbors or send "BAD" reports about its neighboring nodes in order to degrade their QoS and prevent them from achieving their desired service. It is prevented by applying our proposed reports analysis and punishment mechanisms, as any node, which sends false sensing information or false opinion about other nodes, will be punished with proper penalty action depending on the severity of the launched DoS attack. Every node is monitored and its behavior is evaluated at the end of every reporting round. Therefore, for any node to stay in the network and keep using its resources, it has to act normally in the network.

4.4.4 Objective Function Attack Analysis

The attacker tries to change the radio parameters (such as center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size) to reduce the network objective, which is always to have higher security and higher transmission rate. Any change in these parameters will lead to false sensing results of other nodes and might lead to launch PUE attack. However, by applying our proposed BL management scheme and penalty mechanism, a node will not have the opportunity to change any of these parameters. Our proposed approach reduces the resources assigned to the misbehaving node, which reduces the opportunity for the misbehaving node to change the radio parameters. If a node launches this attack, other nodes will notify CH about the abnormal behavior of this node. Therefore, CH applies appropriate penalty actions, such as deallocating part of the resources, which weakens its ability to perform such an attack.

4.4.5 Collusion Attack Analysis

As the collusive reporting node sends false reports about its neighboring node(s), CH uses the reports sent by its next node(s) to determine the correctness of its reports. Incorrect reports are determined upon the comparison of the reports sent by the reporting node, other nodes' reports and CH's sensing decision itself. Such a comparison leads to identify the compromised and collusive nodes in the network. No node will like to have its belief level reduced, or be considered as compromised or collusive node. By the role of CH and applying the penalty scheme, a node will send true reports about its neighboring node(s) and will not send false reports to protect itself from being penalized or considered as a collusive or compromised node.

Another form of collusion attack is when multiple nodes agreed about reporting a benign node as a “BAD” node, when the node is not “BAD”. When CH receives the reputation reports from the collusive nodes about the benign node, it analyzes the reports sent by the collusive nodes about the benign node and the reports sent by the benign node about the collusive. Based on that analysis, CH can tell if the “BAD” reports are true or false reports. Consequently, the CH takes the appropriate actions against the collusive nodes or the misbehaving node. Hence, detecting the collusive nodes will become easier and faster with time as the BL of the collusive nodes will be decreased. As a result, their reports will have no high effect on other benign nodes.

4.5 Summary

Securing the spectrum sensing process in CRN is very important as adversary nodes might behave in different abnormal ways to launch different attacks that degrade the spectrum sensing reliability. Therefore, the network security and throughput will be reduced. Current mechanisms of attack detection focus on addressing the attacks independently or two kinds of attacks a time, which is not realistic, as multiple attacks can exist simultaneously.

Monitoring nodes behavior during the spectrum sensing process helps to identify and eliminate adversary nodes from the network, which improves the accuracy of the sensing results, the network security and the performance.

In this paper, we propose a collaborative approach during the spectrum sensing process that focuses on monitoring the nodes’ behavior rather than addressing the attacks themselves. It works as a proactive approach to passive attacks and as a reactive approach to active attacks. In the proposed approach, all sensing nodes monitor the behavior of each other to identify the adversary nodes.

The simulation results show the performance of our proposed approach compared to other models. This approach improves the detection probability and false alarm probability, which increases the network security and implicitly enhances the spectrum utilization and network throughput. Moreover, the security analysis shows the different kind of active and passive attacks that can be detected and mitigated through the proposed approach by monitoring the sensing nodes behavior.

Chapter 5: A Routing Algorithm for Spectrum Management phase

In this chapter, a compound secure routing algorithm based on nodes' behavior during the spectrum sensing phase is proposed. It uses node's belief level (BL), proposed in Chapter 4, which measures how secure the nodes' behavior is during the spectrum sensing phase. The routing algorithm combines security (node's BL) as a routing metric with two other routing metrics, which are the probability of PU presence and the channel cost in terms of delay. The algorithm proposed relies on the public-key and symmetric-key cryptography to encrypt/decrypt the messages transmitted during the route establishment, route maintenance, and data forwarding phases. Therefore, this cryptography prevents any malicious node from eavesdropping on these messages, from altering them and/or from participating in the packets routing over the network. The proposed approach aims at building secure routes that contain trusted nodes only, which improves the network performance in terms of end-to-end delay, packet delivery ratio, packet loss ratio and routing overhead. The nodes' behavior during the routing phase is monitored by each other. The nodes will send reputation reports, same as in the sensing reputation reports (Chapter 4), about their neighboring nodes behavior to the CH, which takes care of analyzing them to identify the adversary nodes that selectively drop or does not forward the routing packets to its neighboring node(s). The process of analyzing these reputation reports is same as that used in Chapter 4.

The main contributions and the characteristics of the proposed approach can be summarized as follows:

- To the best of our knowledge, this work is the first to address the issue of considering security as a routing metric in the CRNs. Security in the proposed approach is in terms of providing resources' access to secure nodes only, as well as securing the message exchange process over the network. By doing so, we secure the different routes and therefore the network security and performance are implicitly enhanced.

- To the best of our knowledge, this work is the first to combine the spectrum sensing and the routing phases in the CRNs by using the nodes' behavior during the spectrum sensing phase to find the best secure paths.
- The proposed approach uses three different routing metrics combined: the nodes' BL, the probability of PU presence, and the channel cost.
- The proposed approach is able to adapt any changes in the PUs activity as the probability of the PU's presence is considered as a routing metric. Therefore, the routing paths will be more stable, which makes the proposed approach more reliable.
- The proposed approach is a cross-layering approach as the channel status and the PU's activity at the physical and data link layers affect the routes establishment at the network layer.
- The proposed approach assigns different weight to the three-routing metrics used for finding the best paths. It focuses more on the nodes' BL, which is the main metric. Therefore, it implicitly minimizes the route establishment time and maintenance cost.
- The proposed algorithm is evaluated and verified in terms of security functionality, its correctness and its performance. This proves that it is safe against attacks and it performs better in comparison to the other approaches.

This chapter is organized as follows: firstly. the system requirements and the general assumptions are shown in Section 5.1. It is followed by describing the proposed routing algorithm and showing its complexity in Section 5.2. Next, a case study is investigated by applying the proposed routing in Section 5.3. After that, the performance of the proposed algorithm is measured and compared with other approaches in the literature in Section 5.4. Next in Section 5.5, the proposed approach is validated formally through a verification tool. The chapter is concluded with a summary in Section 5.6.

5.1 System Requirements and General Assumptions

The system requirements and general assumptions used in Chapter 4 are also applied to the routing algorithm as the routing algorithm is built based on the monitoring nodes behavior technique proposed in Chapter 4.

5.2 The Routing Algorithm

5.2.1 Preface

As described in Chapter 4, all the clusters nodes perform the spectrum sensing process to find the vacant spectrum channels. Each sensing node forwards its sensing decision which is saved in a parameter called sensing result (SR) to its neighbors. Then, it compares its own SR with the received SR from its neighboring node and if they match, the sensing node decides that its neighboring node is a “GOOD” node; otherwise it is a “BAD” node. Finally, it prepares sensing-reputation reports about their neighboring node(s). CH makes the final decision about the spectrum availability based on the reports sent by different nodes and their BL values and forwards the final decision to its cluster nodes as described in Algorithm 4.1 (Chapter 4). The calculated BL will be used in the routing algorithm as a routing metric combined with other routing parameters.

5.2.2 The Algorithm

Our proposed approach aims to find the best path between the source and the destination nodes. As mentioned earlier, a best path is a one that includes all the best next nodes that have the highest

BL, the lowest probability of PU presence, and the lowest channel cost. Best next node (BNN) of each node is found according to the following general objective function in equation 5.1:

$$F(BNN) = \max\left(BL_{SU_j}\right) + \min(P_{PU}) + \min(Cost_{ch}) \tag{5.1}$$

where $F(BNN)$ is the function of best next node, BL_{SU_j} is the next node's BL, P_{PU} is the probability of PU's presence over next channel, and $Cost_{ch}$ is the cost of the channel between the current node and its next node, which is the delay in our proposed routing algorithm.

The proposed routing algorithm is described step by step in Algorithm 5.1. It defines all the parameters and the functions that are used to implement the algorithm. The algorithm starts where CH sends to each node the BL of its next node(s), the channel(s) cost and the probability of PU presence over those channels. Then, each current cluster node (SU_i) finds the inverse of its next node(s) BL as $BL_{SU_j}^{inverse} = 1/BL_{SU_j}$ and saves it with the channel(s) cost and the probability of PU presence over those channels in a table called Next Nodes Information (NNI) shown in Table 5.1. Each node (SU_i) has its own NNI table that is used by each node to find its best next node among its different neighboring nodes. After that, (SU_i) arranges the nodes, for each parameter, in an ascending order by using the $Sort(Parameter)$ function. Then, (SU_i) applies the weight coefficient of each parameter to the nodes' order in order to find a value namely, V_{SU_j}, which will be used to find the best next node. The objective function, shown in equation (5.2), is used to find the best next node. According to the objective function, the best next node is the node that has the smallest V_{SU_j}. Finally, all the best next nodes are appended together to form the best path.

$$F(BNN) = MIN(\left(\mu * Order\left(BL_{SU_j}^{inverse}\right)\right) + \left(\varepsilon * Order(Cost_{ch})\right) + \ (\vartheta * Order(P_{PU}))) \tag{5.2}$$

where, μ is the weight coefficient of the inverse BL parameter and equals to 0.5, ε is the weight coefficient of the channel cost parameter and equals to 0.2, and ϑ is the weight coefficient of the probability of PU presence parameter and equals to 0.3.

TABLE 5.1 NEXT NODES INFORMATION (NNI)

Next Node ID	Inversed BL	Channel Cost	Probability of PU Presence

ALGORITHM 5.1 THE ROUTING ALGORITHM

Parameters:
M: the set of SUs.
X: a subset of M that represents the next nodes of the current node.
K: the set of Channels.
$Cost_{ch}$: the Channel's cost.
SU_{src} : the source node.
SU_{des} : the destination node.
SU_{cur} : the current node.
SU_{next} : the next node.
SU_{best} : the best next node.
$K_{cur\to next}$: the channel between the current node and its next node.
$Cost_{K_{cur\to next}}$: the cost of the channel between the current node and its next node.
$BL_{Node}^{inverse}$: the node's inverse BL.
P_{PU}: the probability of PU's presence.
$V_{SU_{next}}$: the calculated value in the objective function.
Next Nodes Information (NNI) Table: a table maintained by current SU which includes information about its neighboring (next) nodes: Node ID, Inverse BL, Channel Cost, and Probability of PU Presence.
Save (Inverse BL, Channel Cost, and Probability of PU Presence): a function applied by current SU to save the information of its next nodes in NNI.
$\boldsymbol{BPath}\{\boldsymbol{BNN}\}$: a list used to build the best path between any two nodes by appending the best next node of each node in the path.

<u>**Initialize**</u>

```
For each $SU_i \in M$
   CH sends $(BL_{SU_{next}}, Cost_{K_{i\to next}}, P_{PU})$
EndFor
For each $SU_i \in M$
   $SU_{cur} = SU_i$
   For each $SU_j \in X$
        $SU_{next} = SU_j$
        $BL_{SU_j}^{inverse} = 1/BL_{SU_j}$
        $Save(BL_{SU_j}^{inverse}, Cost_{K_{i\rightarrow j}}, P_{PU})$
    EndFor
EndFor
```

Sort of Next Nodes

```
For each $SU_i \in M$
    For each $SU_j \in X$
        $Sort(BL_{Node}^{inverse})$
        $Sort\left(Cost_{K_{i\rightarrow j}}\right)$
        $Sort(P_{PU})$
    EndFor
EndFor
```

Finding the Best Next Node

```
For each $SU_i \in M$
     For each $SU_j \in X$
     $V_{SU_j} = \left(\mu * Order\left(BL_{SU_j}^{inverse}\right)\right) + \left(\varepsilon * Order\left(Cost_{K_{i\rightarrow j}}\right)\right) + (\vartheta * Order(P_{PU}))$
      EndFor
     $small = MIN(V_{SU})$
    $BNN = IndexOf(small)$
```

Append the Best Next Node to the Best Path List

```
$BPath\,\{BNN\}$
 EndFor
```

Special Cases:

1. If the current node has multiple nodes as BNN, i.e. multiple nodes have the same value of $V_{SU_{next}}$:
   - The current node chooses the neighboring node that has $MIN(BL_{SU_{next}}^{inverse})$.
   - If multiple nodes have the same $BL_{SU_{next}}^{inverse}$, the current node chooses the neighboring node that has $MIN(P_{PU})$.
   - If multiple nodes have the same P_{PU}, the current node chooses the neighboring node that has $MIN(Cost_{K_{cur\rightarrow next}})$.
   - If multiple nodes have the same $BL_{SU_{next}}^{inverse}$, P_{PU}, and $Cost_{ch_{cur\rightarrow next}}$, the current node chooses any of the neighboring nodes.
2. If P_{PU} over a channel is equal to 1, this channel is eliminated from the routes establishment.

5.3 Case Study

In this section, we study a case scenario in order to show how our proposed routing algorithm works. Figure 5.1 shows the network scenario.

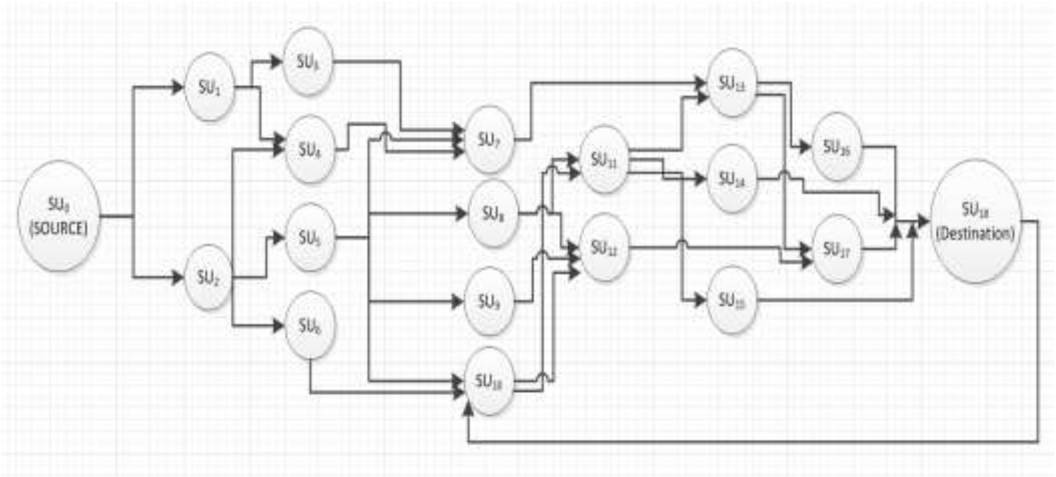


Figure 5.1: A Routing Scenario.

In Table 5.2, we show each node's information, which is its ID, its BL, its neighbors, the channel cost, and the probability of PU presence over each channel, with the assumption that there is at least one channel between each two SUs. We assume that SU_0 wants to communicate with SU_{18}. We apply our proposed algorithm to find the best path between the source node (SU_0) and the destination node (SU_{18}). Each node finds its best next hop, and then each next hop is added to a list. When these nodes accumulate in this manner, the best path is formed. The values of the weight coefficients used in this case study are same as in Section 5.2.2.

TABLE 5.2 THE ROUTING METRICS VALUES USED FOR THE SCENARIO

Node ID	**Node's BL**	**Neighbor node(s)**	**Channel Cost(delay)**	**PU's presence probability over that channel**
0	3.4	1,2	9, 6	0.4, 0.52

1	2.8	3,4	6, 3	0.36, 0.29
2	3.8	4,5,6	8, 7, 4	0.18, 0.43, 0.72
3	2.4	7	5	0.25
4	3	7	3	0.74
5	3.7	7, 8, 9, 10	3, 5, 6, 4	0.16, 0.24, 0.31, 0.36
6	2.5	10	12	0.17
7	2.4	13	9	0.81
8	3.4	11,12	4, 3	0.31, 0.19
9	2.7	12	3	0.23
10	2.8	11,12	6,9	0.54, 0.19
11	3.7	13, 14, 15	4, 8, 2	0.34, 0.21, 0.76
12	3.3	17	3	0.41
13	3	16, 17	5, 2	0.34, 0.12
14	2.5	18	8	0.43
15	2.7	18	16	0.27
16	2.6	18	4	0.68
17	2.5	18	5	0.19
18	3.4	10	3	0.35

At the source Node (SU_0):

The source node SU_0 can choose either SU_1 or SU_2 as its next node. The source node SU_0 does the following calculations:

Next Node ID	**~~BL Inverse~~ →order**	**~~Channel cost~~→order**	**~~Prob. of PU presence~~→order**	V_{SU}
SU_1	~~0.36~~→2	~~9~~ →2	~~0.40~~ →1	~~0~~ →1.7
SU_2	~~0.26~~→1	~~6~~ →1	~~0.52~~ →2	~~0~~ →1.1

Based on the objective function calculation results and according to the routing algorithm, the Source SU_0 chooses SU_2 as its next hop.

The best path includes SU_0→SU_2

At SU_2

SU_2 can choose SU_4, SU_5, or SU_6 as its next node. SU_2 does the following calculations:

Next Node ID	**~~BL Inverse~~ →order**	**~~Channel cost~~→order**	**~~Prob. of PU presence~~→order**	V_{SU}
SU_4	~~0.33~~→2	~~8~~ →3	~~0.18~~ →1	~~0~~ →1.9
SU_5	~~0.40~~→1	~~7~~ →2	~~0.43~~ →2	~~0~~ →1.5
SU_6	~~0.27~~→3	~~4~~ →1	~~0.72~~ →3	~~0~~ →2.6

Based on the objective function calculation results and according to the routing algorithm, SU_2 chooses SU_5 as its next hop.

The best path includes SU_0→SU_2→SU_5

At SU_5

SU_5 can choose SU_7, SU_8, SU_9, or SU_{10} as its next node. SU_5 does the following calculations:

Next Node ID	**~~BL Inverse-~~ →order**	**~~Channel cost~~→order**	**~~Prob. of PU presence~~→order**	$\mathbf{V_{SU}}$
SU$_7$	~~0.42~~→4	~~3~~ →1	~~0.16~~ →1	~~0~~ →2.5
SU$_8$	~~0.29~~→1	~~5~~ →2	~~0.24~~ →2	~~0~~ →1.5
SU$_9$	~~0.37~~→3	~~6~~ →4	~~0.31~~ →3	~~0~~ →3.2
SU$_{10}$	~~0.36~~→2	~~4~~ →3	~~0.36~~ →4	~~0~~ →2.8

Based on the objective function calculation results and according to the routing algorithm, SU$_5$ chooses SU$_8$ as its next hop.

The best path includes SU$_0$→SU$_2$→SU$_5$→SU$_8$

At SU$_8$

SU$_8$ can choose either SU$_{11}$ or SU$_{12}$ as its next node. SU$_8$ does the following calculations:

Next Node ID	**~~BL Inverse-~~ →order**	**~~Channel cost~~→order**	**~~Prob. of PU presence~~→order**	$\mathbf{V_{SU}}$
SU$_{11}$	~~0.27~~→1	~~4~~ →2	~~0.31~~ →2	~~0~~ →1.5
SU$_{12}$	~~0.30~~→2	~~3~~ →1	~~0.19~~ →1	~~0~~ →1.6

Based on the objective function calculation results and according to the routing algorithm, SU$_8$ chooses SU$_{11}$ as its next hop.

The best path includes SU$_0$→SU$_2$→SU$_5$→SU$_8$→SU$_{11}$

At SU$_{11}$

SU$_{11}$ can choose SU$_{13}$, SU$_{14}$, or SU$_{15}$ as its next node. SU$_{11}$ does the following calculations:

Next Node ID	**~~BL Inverse-~~ →order**	**~~Channel cost~~→order**	**~~Prob. of PU presence~~→order**	V_{SU}
SU$_{13}$	~~0.33~~→1	~~4~~ →2	~~0.34~~ →2	~~0~~ →1.5
SU$_{14}$	~~0.40~~→3	~~8~~ →3	~~0.21~~ →1	~~0~~ →2.4
SU$_{15}$	~~0.37~~→2	~~2~~ →1	~~0.76~~ →3	~~0~~ →2.1

Based on the objective function calculation results and according to the routing algorithm, SU$_{11}$ chooses SU$_{13}$ as its next hop.

The best path includes SU$_0$→SU$_2$→SU$_5$→SU$_8$→SU$_{11}$→SU$_{13}$

At SU$_{13}$

SU$_{13}$ can choose SU$_{16}$ or SU$_{17}$ as its next. SU$_{13}$ does the following calculations:

Next Node ID	**~~BL Inverse-~~ →order**	**~~Channel cost~~→order**	**~~Prob. of PU presence~~→order**	V_{SU}
SU$_{16}$	~~0.38~~→1	~~5~~ →2	~~0.34~~ →2	~~0~~ →1.5
SU$_{17}$	~~0.40~~→2	~~2~~ →1	~~0.12~~ →1	~~0~~ →1.5

Based on the objective function calculation results and according to the routing algorithm, SU$_{16}$ and SU$_{17}$ are the best next hop for SU$_{13}$. However, SU$_{13}$ has to choose one of them. In this case the user that has a higher BL is chosen as the next hop; therefore, SU$_{13}$ chooses SU$_{16}$ as its next hop.

The best path includes SU$_0$→SU$_2$→SU$_5$→SU$_8$→SU$_{11}$→SU$_{13}$→SU$_{16}$

At SU_{16}

SU_{16} chooses SU_{18} as its next hop because it has no other next hops.

The best path is $SU_0 \rightarrow SU_2 \rightarrow SU_5 \rightarrow SU_8 \rightarrow SU_{11} \rightarrow SU_{13} \rightarrow SU_{16} \rightarrow SU_{18}$

Hence, the path shown above is the best path and it is secure, which guarantees that no adversary node can overhear or alter it. If a message is sent over this path, the nodes in the path should forward the message to its next hop with no problems assuming that the channels are error-free.

5.4 Performance Evaluation

5.4.1 Complexity Analysis

In this section, we discuss the complexity of the routing algorithm proposed, including the sensing phase, in terms of number of messages exchanged (communication overhead) and memory usage (storage overhead). First for the communication overhead, the messages exchanged are sent by each sensing node and the CH. Each sensing cluster node sends sensing-reputation reports to its CH, and each CH forwards the neighboring nodes' information to each cluster node, which saves this information in NNI table. Suppose we have a cluster of N SUs and each SU has certain neighbor nodes denoted by 'M, then number of messages exchanged by sensing nodes to its CH can be given approximately as $N * M$, while the CH sends N messages. Therefore, the total messages exchanged can be given approximately as $N * M + N$, which is a complexity of second order ($\approx O(N^2)$).

Second, with respect to the memory usage, each CH in our model requires $N * N$ entries of memory to save all the cluster nodes' information, where N is number of SUs in the cluster. While for each node in the cluster, it requires M entries of memory in order to save its neighboring nodes' information, where M is the number of the neighboring nodes of an SU.

Hence, the total memory usage can be given approximately as $N * N + N * M$, which is a complexity of second order ($\approx O(N^2)$). Increasing the number of SUs in the network increases the memory utilization in addition to the processing time at the CH level.

5.4.2 Network Performance Measures

In order to evaluate the performance of our routing algorithm, we consider multiple performance metrics. We apply our proposed routing algorithm to three different networks, each of which has a different number of SUs. Then, we compare the performance of our proposed approach with three other routing algorithms in terms of different metrics, which are:

- Average end-to-end delay: represents the total time from packet generation at source node until packet reception at destination node.
- Packet delivery ratio: represents the ratio of the number of packets received by the destination node to the number of packets generated by the source node.
- Packet loss ratio: represents the packets that have been generated and transmitted by the source node but not received by the destination node.
- Routing Overhead: represents the ratio of routing packets to the total number of packets sent over the network.

5.4.3 Simulation Environment Setup

The simulation model is built by using QualNet and analyzed through MATLAB. Table 5.3 shows the simulation parameters used referring to [78] and [79]. We compare our proposed routing algorithm with three different state-of-the-art routing protocols used in CRNs, which are CAODV [66], SEARCH [63], and LAUNCH [73]. Four performance measures are used in the comparison which are: average end-to-end delay, packet delivery ratio, packet loss ratio, and routing overhead.

TABLE 5.3 SIMULATION PARAMETERS

Parameter	**Value**
Channel Type	Channel/WirelessChannel
Radio propagation model	Propagation/FreeSpace
Network Interface Type	Phy/WirelessPhy
MAC Type	Mac/802_11
Interface queue type	Queue/DropTail/PriQueue
Antenna Model	Antenna/OmniAntenna
Max. Packets in queue	50
# of mobile nodes	[0-100], [100-500]
Routing protocol	PERP
X- dimensions of topology	100
Y- dimensions of topology	100
# of channels/radio	20
Packet size	512 bytes
Application	FTP
Number of malicious nodes	5% of SUs
α	0.3
β	0.7
μ	0.5
ε	0.3
ϑ	0.2

5.4.4 Numerical Results and Performance Comparison

In this section, we show the comparison between the proposed routing algorithm and the three routing algorithms mentioned before CAODV, SEARCH, and LAUNCH. Note that we did not simulate the other models and we just used their results shown in their research papers.

Figure 5.2 illustrates the end-to-end delay in our proposed approach compared to that in CAODV. It is depicted that as the number of SUs increases the end-to-end delay decreases in both the approaches, however our proposed approach outperforms the CAODV routing algorithm i.e. the end-to-end delay is improved up to 60% when the number of SUs equals to hundred. The end-to-end delay decreases with the increment of number of SUs, because having more SUs will increase the chance of having more paths; therefore, the packets will be rerouted if one path is congested.

We then compare the end-to-end delay in our proposed approach to the two other routing algorithms, SEARCH and LAUNCH, as shown in Figure 5.3. Incrementing the number of trusted SUs decreases the end-to-end delay; since, more nodes in the network, increases the number of paths. Our approach outperforms the other two routing approaches as secure nodes will forward packets to their next hop without delaying/dropping them. When the number of SUs is 500 users, the end-to-end delay is improved up to 41% and 80% compared to that in LAUNCH and SEARCH, respectively.

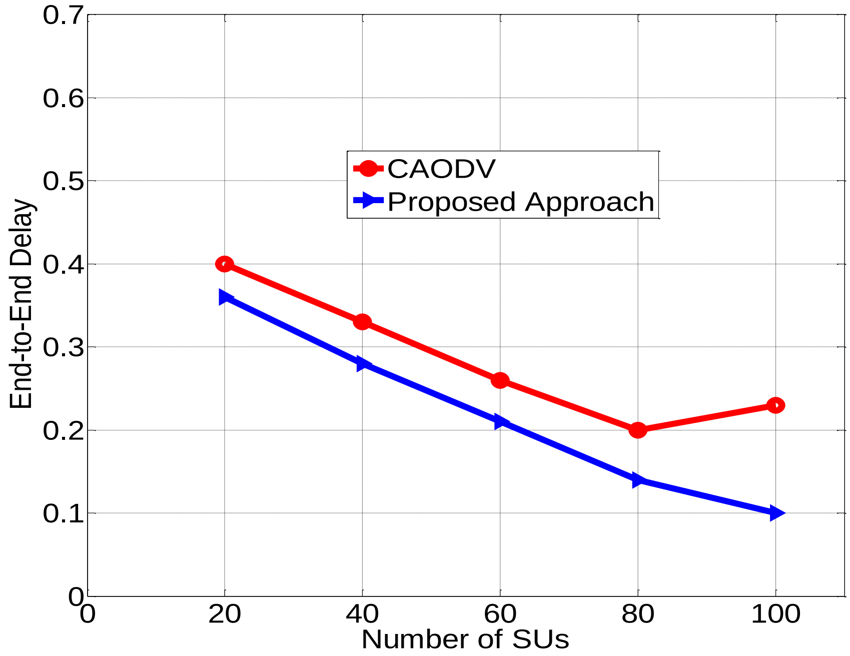


Figure 5.2: End-to-End Delay (Proposed Approach vs. CAODV).

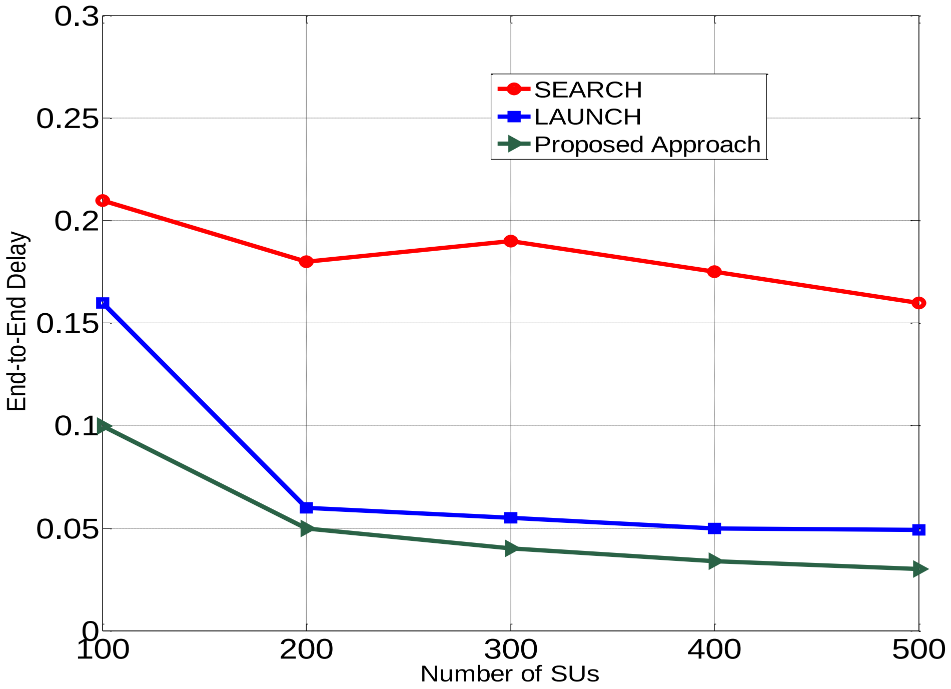


Figure 5.3: End-to-End Delay (Proposed Approach vs. SEARCH vs. LAUNCH).

Next, the packet delivery ratio in our proposed approach is compared with CAODV routing protocol as shown in Figure 5.4. It is clear from Figure 5.4 that the packet delivery ratio increases with the increment of the number of trusted SUs in the network as multiple routes exist. It can reach up to 95% in our proposed approach compared to that in CAODV. On the other hand, we compare the packet loss ratio in our proposed routing algorithm with two other routing algorithms, which are LAUNCH and SEARCH as shown in Figure 5.5. Under the simulation scenario used to measure the packet loss ratio in the three routing algorithms, it is clear that the packet loss ratio decreases rapidly when more trusted SUs are participating in routing the packets over the network. When the number of trusted SUs is equal to 100 users, the packet loss ratio is equal to 100%, 80%, and 70% in SEARCH, LAUNCH, and our proposed approach, respectively.

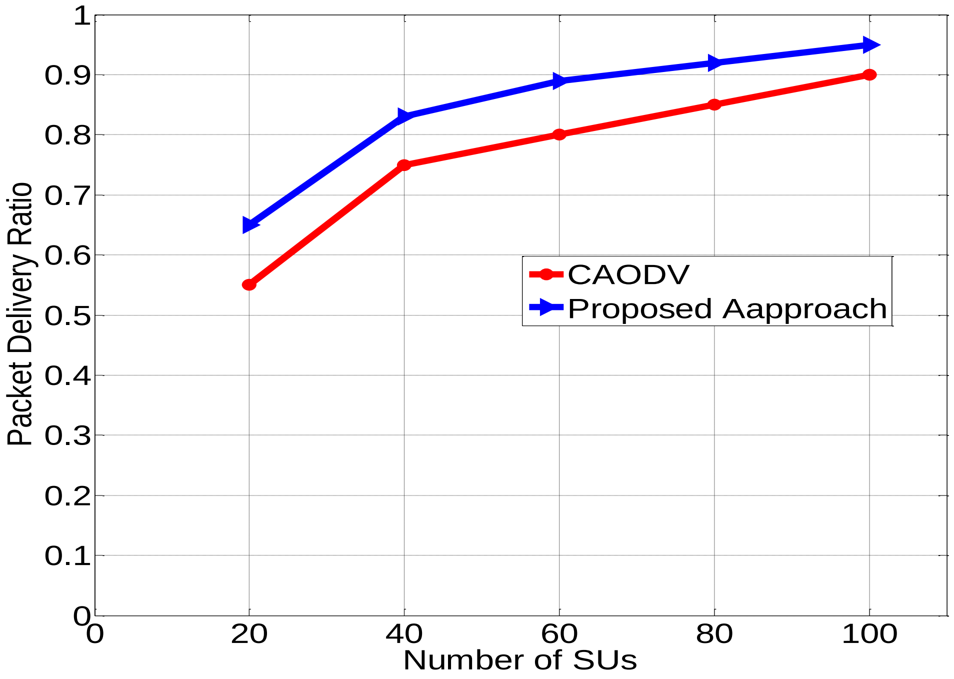


Figure 5.4: Packet Delivery Ratio (Proposed Approach vs. CAODV).

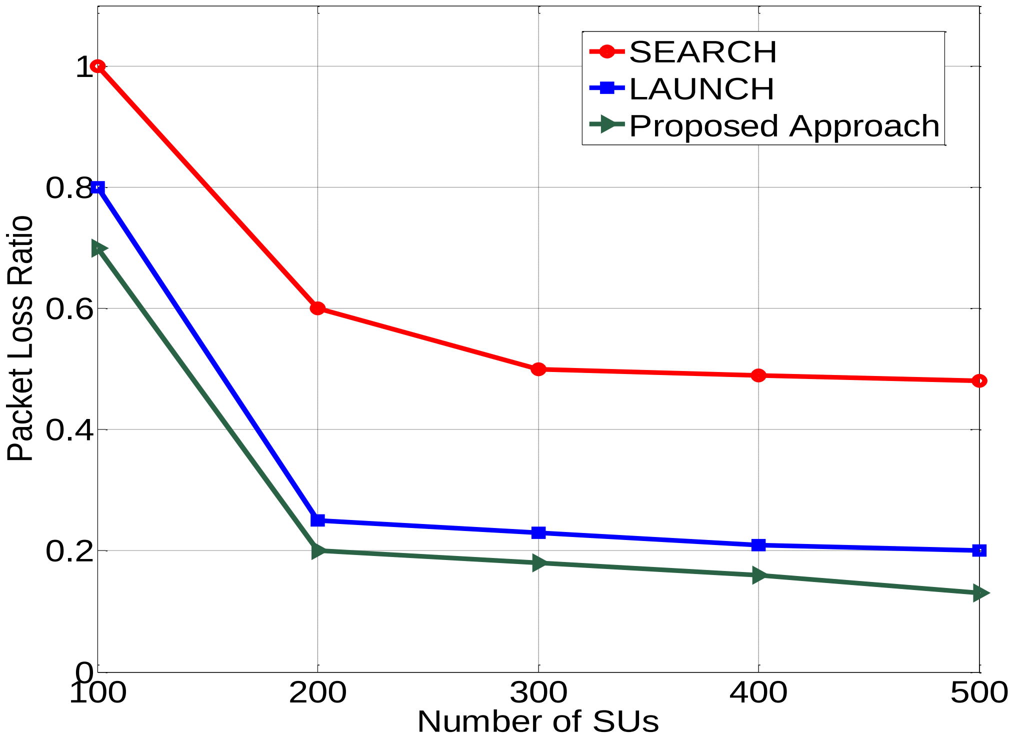


Figure 5.5: Packet Loss Ratio (Proposed Approach vs. SEARCH vs. LAUNCH).

Our proposed routing algorithm succeeds in having the minimum packet loss ratio compared to that in SEARCH and LAUNCH, which shows that our proposed approach outperforms the SEARCH and LAUNCH routing algorithms.

Next, Figure 5.6 and Figure 5.7 compare the routing overhead in our proposed approach with CAODV, SEARCH, and LAUNCH routing algorithms. In Figure 5.6, the routing overhead represents the ratio of the routing packets to the total number of packets sent over the network. It is clear that the routing overhead decreases when the number of available channels increases; since, the nodes have more channels for sending more routing requests. Our proposed approach outperforms the CAODV and keeps the routing overhead at a minimum ratio compared to that in CAODV. In Figure 5.7, we measure the routing overhead in terms of number of packets routed over the network. It is clear that the routing overhead increases with the increase of the number of SUs; however, our proposed approach has a lower routing overhead compared to that in SEARCH and LUANCH routing algorithms.

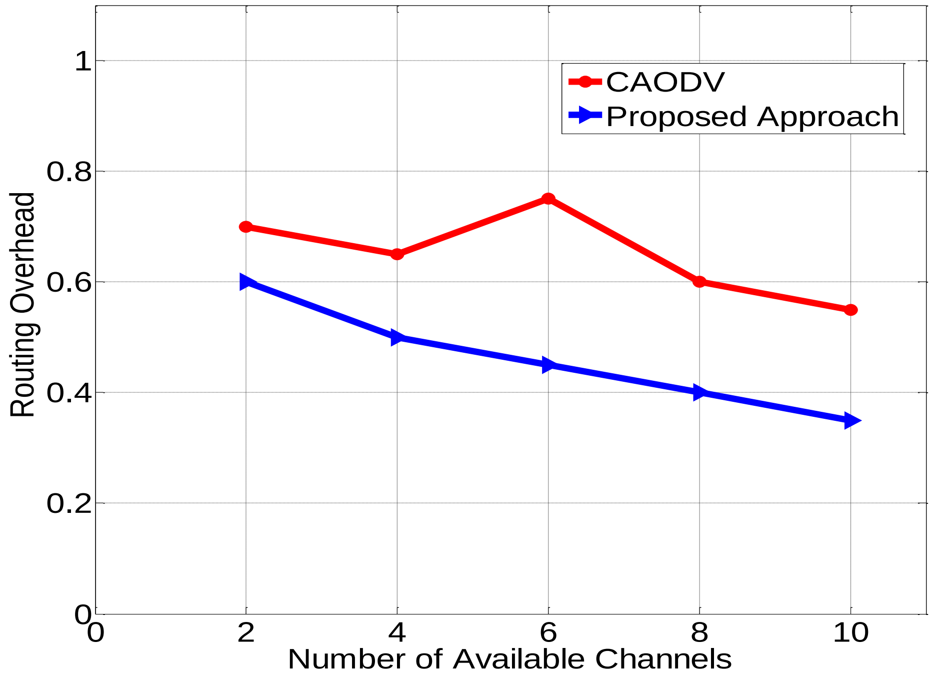


Figure 5.6: Comparison of Routing Overhead (CAODV vs. Proposed Approach). The Routing overhead is measured as No. of Routing Packets / Total No. of Packets).

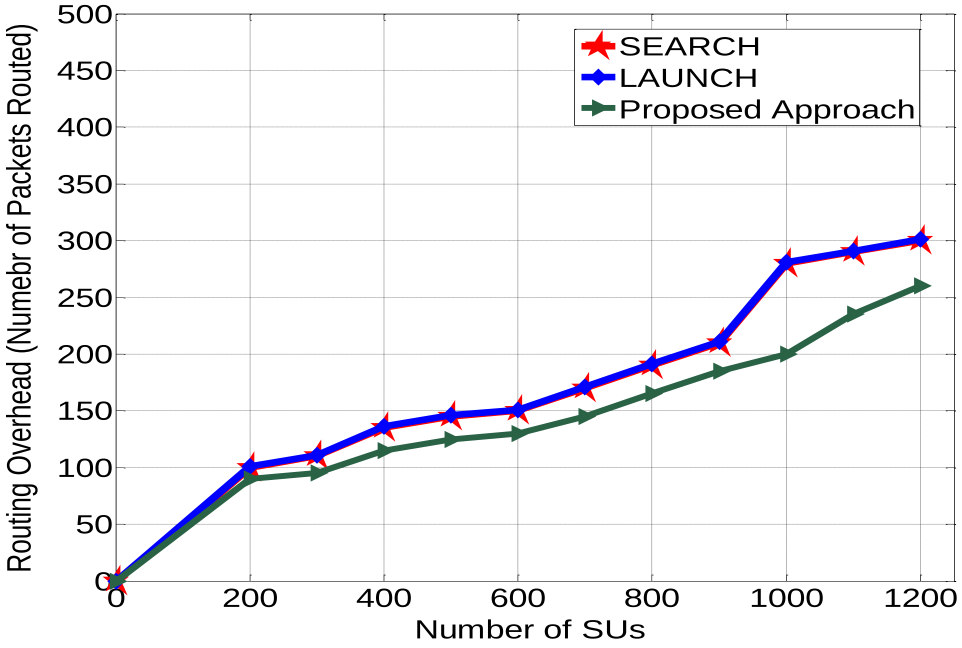


Figure 5.7: Routing Overhead (Proposed Approach vs. SEARCH vs. LAUNCH).

Next, in Table 5.4 and Table 5.5, we compare our proposed approach to the CAODV, LUANCH, and SEARCH routing protocols in terms of the routing metrics used and the characteristics that they can support. It is depicted in Table 5.4 that the different routing algorithms combine multiple routing metrics to fulfill different goals of finding the best paths; however, they do not consider security as a routing metric. Therefore, their algorithms are vulnerable to attacks and they do not properly work in case of adversary nodes participate in route establishment. While in our approach, security is used as a routing metric; therefore, adversary nodes are identified and eliminated from participating in route establishment.

In Table 5.5, we compare the different routing protocols based on different characteristics that they can support. These characteristics are:

- Centralized/Distributed: in central routing algorithms, a central node collects the different nodes' information and uses them to find the best path, while in distributed routing algorithms the different nodes participate in finding the best path over the network.
- Route Maintenance Support: represents the routing algorithm's ability to reconfigure the routes in case of PU presence.
- Mobility Support: represents the routing algorithm ability of considering the mobility of SUs.
- Common Control Channel: represents the routing algorithm requirement of having a pre-set channel, which is known to all SUs and used to forward the routing packets.
- Secure Routes: represents if the different paths are secure, as well as if the security is considered in finding the best paths.

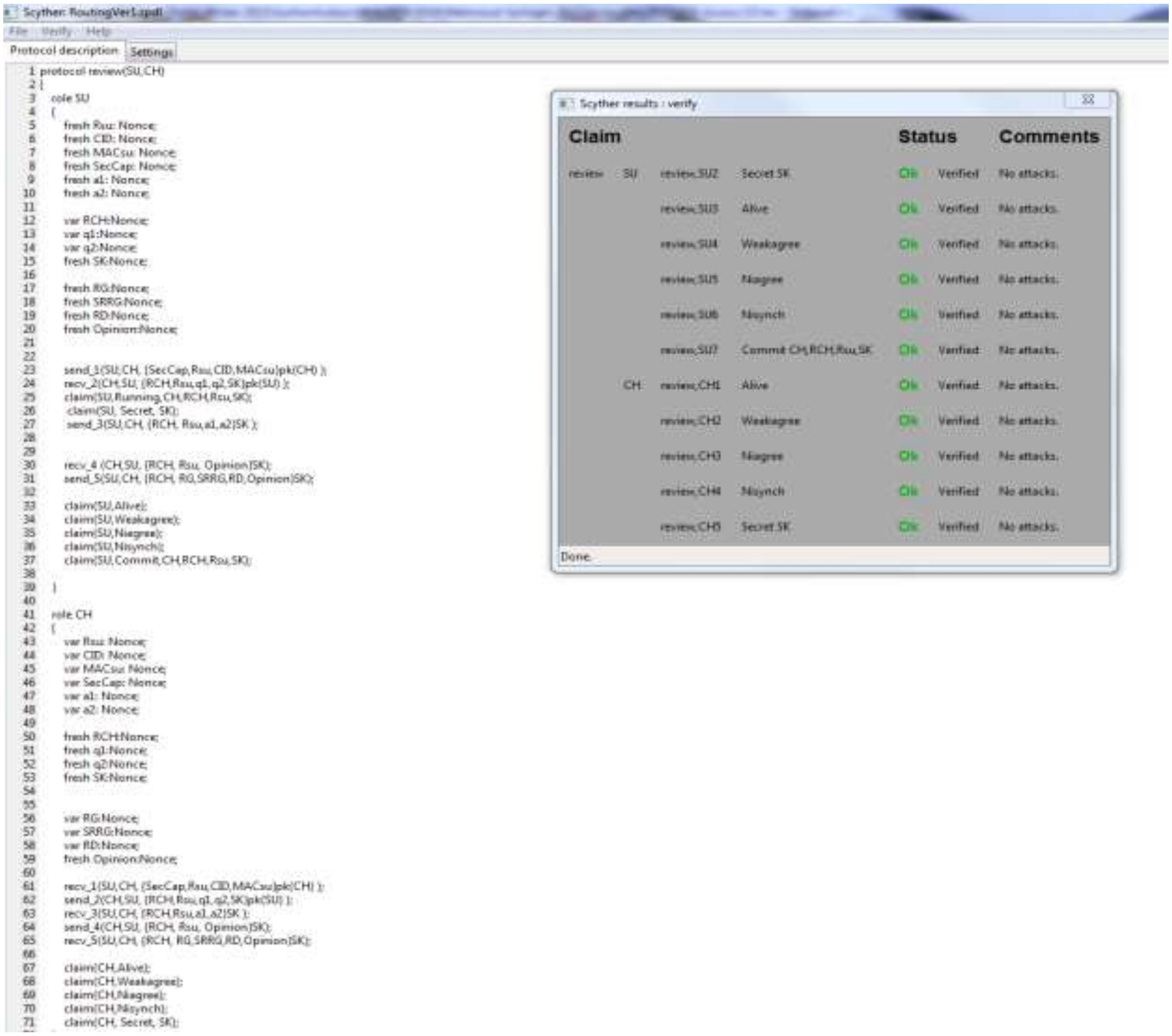
It is depicted that all the routing protocols support most of the characteristics and lack some of them; however, our proposed approach supports all of them. It fulfills the “route maintenance support” characteristic as if a path is congested, the cluster nodes will reroute the packets through the back-up paths, which are already found using the algorithm proposed. The “mobility support” feature is fulfilled in the proposed algorithm as if a node moves to another cluster, its information are forwarded to the CH of the new cluster; therefore, the cluster nodes can find new paths that include the new joining node. Therefore, the proposed approach is shown to be a better choice to be applied in CRNs.

TABLE 5.4 ROUTING METRICS USED BY DIFFERENT ROUTING ALGORITHMS IN CRNS

Routing Protocol/Metric	**Delay**	**Spectrum Availability**	**Location-based**	**Security**
SEARCH	YES	NO	YES	NO
LAUNCH	YES	NO	YES	NO
CAODV	NO	YES	NO	NO
Proposed Approach	YES	YES	YES	YES

TABLE 5.5 CHARACTERISTICS OF DIFFERENT ROUTING ALGORITHMS IN CRNS

Routing Protocol/characteristic	**Centralized/Distributed**	**Route Maintenance Support**	**Mobility Support**	**Common Control Channel**	**Secure Routes**
SEARCH	Distributed	YES	YES	NO	NO
LAUNCH	Distributed	YES	YES	YES	NO
CAODV	Distributed	YES	YES	NO	NO
Proposed Approach	Distributed	YES	YES	YES	YES



Scyther: RoutingVer1.spdl

```
protocol review(SU,CH)
{
  role SU
  {
     fresh Rsu: Nonce;
     fresh CID: Nonce;
     fresh MACsu: Nonce;
     fresh SecCap: Nonce;
     fresh a1: Nonce;
     fresh a2: Nonce;

     var RCH:Nonce;
     var q1:Nonce;
     var q2:Nonce;
     fresh SK:Nonce;

     fresh RG:Nonce;
     fresh SRRG:Nonce;
     fresh RD:Nonce;
     fresh Opinion:Nonce;


     send_1(SU,CH, {SecCap,Rsu,CID,MACsu}pk(CH) );
     recv_2(CH,SU, {RCH,Rsu,q1,q2,SK}pk(SU) );
     claim(SU,Running,CH,RCH,Rsu,SK);
      claim(SU, Secret, SK);
      send_3(SU,CH, {RCH, Rsu,a1,a2}SK );


     recv_4 (CH,SU, {RCH, Rsu, Opinion}SK);
     send_5(SU,CH, {RCH, RG,SRRG,RD,Opinion}SK);

     claim(SU,Alive);
     claim(SU,Weakagree);
     claim(SU,Niagree);
     claim(SU,Nisynch);
     claim(SU,Commit,CH,RCH,Rsu,SK);

  }

  role CH
  {
     var Rsu: Nonce;
     var CID: Nonce;
     var MACsu: Nonce;
     var SecCap: Nonce;
     var a1: Nonce;
     var a2: Nonce;

     fresh RCH:Nonce;
     fresh q1:Nonce;
     fresh q2:Nonce;
     fresh SK:Nonce;


     var RG:Nonce;
     var SRRG:Nonce;
     var RD:Nonce;
     fresh Opinion:Nonce;

     recv_1(SU,CH, {SecCap,Rsu,CID,MACsu}pk(CH) );
     send_2(CH,SU, {RCH,Rsu,q1,q2,SK}pk(SU) );
     recv_3(SU,CH, {RCH,Rsu,a1,a2}SK );
     send_4(CH,SU, {RCH, Rsu, Opinion}SK);
     recv_5(SU,CH, {RCH, RG,SRRG,RD,Opinion}SK);

     claim(CH,Alive);
     claim(CH,Weakagree);
     claim(CH,Niagree);
     claim(CH,Nisynch);
     claim(CH, Secret, SK);
```

Scyther results : verify

Claim				Status		Comments
review	SU	review,SU2	Secret SK	Ok	Verified	No attacks.
		review,SU3	Alive	Ok	Verified	No attacks.
		review,SU4	Weakagree	Ok	Verified	No attacks.
		review,SU5	Niagree	Ok	Verified	No attacks.
		review,SU6	Nisynch	Ok	Verified	No attacks.
		review,SU7	Commit CH,RCH,Rsu,SK	Ok	Verified	No attacks.
	CH	review,CH1	Alive	Ok	Verified	No attacks.
		review,CH2	Weakagree	Ok	Verified	No attacks.
		review,CH3	Niagree	Ok	Verified	No attacks.
		review,CH4	Nisynch	Ok	Verified	No attacks.
		review,CH5	Secret SK	Ok	Verified	No attacks.

Done.

Figure 5.8: The Results of Verifying the Proposed Routing Algorithm in the Scyther Environment.

5.5 Verification through Scyther

We verified the correctness of our routing algorithm by using a well-known verification tool namely Scyther [76]. We set up the verification environment by using the settings parameters shown previously in Table 3.4 (Chapter 3). We then, described the algorithm messages sent between the two entities, the joining node and the CH. After the verification run has completed, a “no attacks” messaged popped up as shown in Figures 5.8. It shows that our protocol is safe against the multiple attacks (mentioned in Chapter 3), as “no attacks” break the verification process. Moreover, the “status” of each message is “OK, verified”, which means that each message has been received correctly by the destination with no alteration (i.e. same at it has been sent by the source). It is depicted in Figure 5.8 that our routing algorithm is secure and no attacks can eavesdrop on messages sent between the reporting node and the CH. Moreover, the sensing-reputation reports are sent and received safely by the reporting node and the CH. Therefore, we can depict from the verification process applied to our routing algorithm that the algorithm is effective in increasing the packet reception rates with effectively no overhead on the CH. The formal verification of the algorithm provided useful insights of the routing algorithm during its developing phase and indeed, helped in the algorithm development.

5.6 Summary

Spectrum sensing is the main phase in making the CR technology an effective solution to the spectrum scarcity problem. However, investigating the reliability of sensing nodes is important, as the presence of adversary nodes can make the spectrum sensing results ineffective. Therefore, security of the sensing nodes has to be taken into consideration before data is being routed over the network. Analyzing nodes behavior during spectrum sensing is important in order to build secure routing protocols/algorithms that enhances the network performance and increases network reliability.

Current routing mechanisms in CRNs do not consider security as a routing metric. They are focusing more on securing the routes messages exchange, which is important; however, considering security as a routing metric is also important to prevent intruders from targeting the networks, and therefore decreasing the network performance.

In this chapter, we propose a routing algorithm based on nodes' behavior during the spectrum sensing phase. The routing algorithm uses security as a routing metric combined with other metrics. The proposed approach aims to build secure routes that include trusted sensing nodes, which improves the network performance in terms of end-to-end delay, packet delivery ratio and routing overhead. The simulation results show the performance of our proposed approach compared to other models. It improves the network performance measures, which increases the network security, and implicitly enhances the spectrum utilization and the network throughput.

Chapter 6: Conclusion and Future Work

6.1 Conclusion

The number of subscriptions for commercial mobile services in the world is rapidly increasing. In fact, the increase in mobile subscriptions has been accompanied by the adoption of more sophisticated mobile devices with internet-access, such as smart phones and tablets. However, spectrum is a limited resource, and the "usable" spectrum range (given current technologies) is completely allocated to existing services. As a result, service providers over the world must rely on new technologies in order to meet the spectrum needs of new or growing services and to use the spectrum efficiently. The greater spectrum use efficiency can be achieved by adopting and applying innovative technologies (such as 5G wireless mobile broadband technologies and Cognitive Radio (CR) technology). However, as in any other type of wireless networks, cognitive radio networks (CRNs) are vulnerable to many security attacks (both passive and active) especially during the spectrum sensing phase. The radio technology itself is vulnerable to attacks as any radio frequency can be blocked or jammed when a transmitter sends a signal of adequate strength at the same frequency. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. Therefore, stronger security mechanisms should be proposed to avoid the harmful effects of different attacks to the network performance.

This research focuses on addressing the network security in the two main functionalities of cognitive radio networks, spectrum sensing and spectrum management. Securing the spectrum sensing process in CRN is very important as adversary nodes might behave in different abnormal ways to launch attacks that degrade the spectrum sensing reliability and therefore reduce the network security and throughput. A CR node cannot access the spectrum unless it has been authenticated by a reliable node. We propose a two-level secure authentication scheme in CRN wherein the authenticating node and the joining node accept a key agreement. We adopt the advantages of using the public key and the symmetric key cryptography to secure the messages exchanged between the communicating nodes. The authentication process ends with assigning to each node a value called belief level (BL), which measures the node's sensing reliability to participate in spectrum sensing and data transmission over the network. The belief level of each node is the key element of the proposed research; since, it is used to correctly monitor the sensing nodes' behavior and detect the adversary nodes during the spectrum sensing phase as well as a routing metric during the spectrum management phase. Next, we proposed a collaborative approach during the spectrum sensing process that focuses on monitoring the nodes' behavior. BL is used to make the final sensing decision and to identify the adversary nodes. It works as a proactive approach to passive attacks and as a reactive approach to active attacks. Finally, we proposed a routing algorithm based on the nodes' behavior during spectrum sensing. The routing algorithm uses security (BL) as a routing metric combined with other metrics. The proposed approach aims at building secure routes that include trusted sensing nodes, which improves the network performance in terms of end-to-end delay, packet delivery ratio and routing overhead.

The performance of the developed models is evaluated using simulation. The proposed authentication scheme, in comparison to the existing authentication approaches, reduces the number of cryptographic operations and the authentication time needed to complete the authentication process. The simulation results of the monitoring nodes behavior approach illustrate that the detection probability and the false alarm probability have improved. The simulation results of the routing algorithm suggested that the network security implicitly enhances the spectrum utilization and network throughput in terms of end-to-end delay, packet delivery ratio and routing overhead.

6.2 Future Work

Many ideas can be applied to enhance the efficiency of the three developed models in this research. In the spectrum sensing phase, the way of forming the clusters, choosing the cluster heads, and exchanging the sensing results could be improved to further increase the accuracy of the spectrum sensing results.

New encryption/decryption methods can be proposed to improve the security of message exchange between the different communicating nodes. Moreover, the method used for making final sensing decision can be improved by giving more weight to the nodes' votes that have the correct sensing decision.

The game theory can be applied to our routing approach to improve its performance. The nodes that form the best path can play a game to gain a higher profit from forwarding data through them. Optimization techniques can be used to make every communicating node achieve its highest quality of service (QoS) without interfering with other nodes. We have already enough experience in applying game theory [82-89], therefore we believe that applying the game theory leads to better performance in CRNs.

References

1. http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09444.html#fig5, Industry Canada. Accessed May 16th, 2017.
2. https://www.emarketer.com/Article/Over-Half-of-Canadas-Population-Use-Smartphones-2015/1011759. Accessed May 16th, 2017.
3. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html. Accessed May 16th, 2017.
4. S. M. Mishra, D. Cabric, C. Chang, et al., “A real time cognitive radio testbed for physical and link layer experiments”, in Proc. IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pp. 562–567, 2005.
5. I.F. Akyildiz, W.Y. Lee, M.C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey”, Computer Networks Journal, Vol. 50, No. 13, pp. 2127-2159, 2006.
6. L. Lai, Y. Fan, and H. V. Poor, “Quickest detection in cognitive radio: A sequential change detection framework”, in Proc. IEEE Global Telecommunication Conference. (GLOBECOM), New Orleans, LA, Nov.–Dec. pp. 1–5, 2008.
7. S. Alrabaee, M. Khasawneh, A. Agarwal, N. Goel and M. Zaman, “Applications Architectures and Protocol Design Issues for Cognitive Radio Networks: A Survey”, International Journal of Wireless and Mobile Computing, Vol. 7, No.5, pp. 415-427, 2014.
8. W. El-Hajj, H. Safa and M. Guizani, “Survey of Security Issues in Cognitive Radio Network”, Journal of Internet Technology, Vol. 12, No.2, pp. 1-18, 2011.

9. J. Mitola, “Cognitive Radio For Flexible Multimedia Communications”, IEEE International Workshop on Mobile Multimedia Communications (MoMuC), San Diego, USA, pp. 3-10, 1999.

10. A. A. Khan, M. H. Rehmani and M. Reisslein, "Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols", IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 860-898, 1st quarter 2016. doi: 10.1109/COMST.2015.2481722

11. I. Akyildiz and Y. Li, “OFDM-based cognitive radio networks”, Broadband and Wireless Networking Laboratory Technical Report, OCRA, March, 2006.

12. S. Sodagari and T. C. Clancy, “An Anti-Jamming Strategy for Channel Access in Cognitive Radio Networks”, Decision and Game Theory for Security, Lecture Notes in Computer Science (LNCS), Vol. 7037, pp. 34-43, 2011.

13. J. Zhao and G. Cao, “Robust Topology Control In Multi-Hop Cognitive Radio Networks”, IEEE International Conference on Computer Communications (INFOCOM), pp. 2032-2040, 2012.

14. M. Khasawneh, I. Kajman, R. Alkhudaidy and A. Althubyani, “A Survey on Wi-Fi Protocols: WPA and WPA2”, International Conference on Security in Computer Networks and Distributed Systems (SNDS), pp. 496-511, 2014.

15. M. Youssef, M. Ibrahim, M. Abdelatif, L. Chen, and A. Vasilakos, “Routing metrics of cognitive radio networks: a survey”, IEEE Communication Survey and Tutorials, vol. 16 no. 1, pp. 92–109, 2014.

16. https://tools.ietf.org/html/rfc5246, accessed on August 20th, 2017.

17. K. Wong, Y. Zheng, J. Cao and S. Wang, “A Dynamic user authentication scheme for WSN”, IEEE International Conference on Sensor Networks, Ubiquitous Computing, and Trustworthy Computing (SUTC), pp. 244-251, 2006.

18. H. Tseng, R. Jan and W. Yang, “An Improved Dynamic User Authentication Scheme for WSN”, GLOBECOM, pp. 986-990, 2007.

19. K. Han, T. ShiakShon and K. Kim, “Efficient Mobile Sensor Authentication in Smart Home”, IEEE Transaction on Consumer Electronics, Vol. 56, No. 2, pp. 591-596, 2010.

20. S. Zhu, S. Setia and S. Jajodia, “LEAP: efficient security mechanisms in large scale distributed networks”, 10th ACM Conference on Computers and Communication Security (CCS), pp. 62-72, 2003.

21. P. Ning, A. Liu and W. Du, “Mitigating DOS attacks against broadcast authentication in WSN”, ACM Transactions on Sensor Networks, Vol. 4, No. 1, pp. 1-35, 2008.

22. X. Tan, K. Borle, W. Du and B. Chen, “Cryptographic Link Signatures for Spectrum Usage Authentication in Cognitive Radio,” 4th ACM conference on Wireless Network Security, (WiSec), pp. 1-12, 2011.

23. HS. Kim, “Location-based authentication protocol for first cognitive radio networking standard”, Journal of Network and Computer Applications, Vol. 34 No. 4, pp. 1160-1167, 2011.

24. S. Parvin and H. F. Khadeer, “Digital signature-based secure communication in cognitive radio networks”, Broadband and Wireless Computing, Communication and Applications (BWCCA), pp. 230-235, 2011.

25. S. Parvin, S. Han, B. Tian and H.F. Kadeer, “Trust based authentication for secure communication in cognitive radio networks”, IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), pp. 589-596, 2010.

26. S. Parvin, F. H. Khadeer and O. H. Khadeer, “Digital signature-based authentication framework in cognitive radio networks”, 10th International Conference on Advances in Mobile Computing & Multimedia (MoMM), pp. 136-142, 2012.

27. K. Chatterjee, A. De and D. Gupta, “A secure and efficient authentication protocol in wireless sensor network”, Wireless Personal Communication, Vol. 81, No.1, pp. 17-37, 2015.

28. X. Chen, H.-H. Chen, and W. Meng, “Cooperative communications for cognitive radio networks—From theory to applications,” IEEE Communication Surveys Tutorials., vol. 16, no. 3, pp. 1180–1192, 3rd Quart. 2014.

29. M. Khasawneh, S. Alrabaee, A. Agarwal, N. Goel and M. Zaman, “Power Trading in Cognitive Radio Networks”, Elsevier Journal of Network and Computer Applications, Vol.65, pp. 155-166, 2016.

30. G. Ozcan, M. C. Gursoy, N. Tran and J. Tang, "Energy-Efficient Power Allocation in Cognitive Radio Systems With Imperfect Spectrum Sensing," in IEEE Journal on Selected Areas in Communications, vol. 34, no. 12, pp. 3466-3481, Dec. 2016. doi: 10.1109/JSAC.2016.2621399.

31. N. Michelusi and U. Mitra, "Cross-Layer Estimation and Control for Cognitive Radio: Exploiting Sparse Network Dynamics," in IEEE Transactions on Cognitive Communications and Networking, vol. 1, no. 1, pp. 128-145, March 2015. doi: 10.1109/TCCN.2015.2503287.

32. H. Kpojime and G. Safdar, “Interference mitigation in cognitive radio based femtocells,” IEEE Communication Surveys Tutorials, vol. 17, no. 3, pp. 1511–1534, 3rd Quart. 2015.

33. D. Das and S. Das, “Primary user emulation attack in cognitive radio networks: A survey”, International Journal of Computer Networks and Wireless Communications, Vol. 3, No. 3, pp. 312-318, 2013.

34. Z. Jin, S. An and, K.P. Subbalakshmi, “Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks”, IEEE International Conference on Communications (ICC), Dresden, Germany, pp. 1-5, 2009.

35. A. Alahmadi, M. Abdelhakim, J. Ren and T. Li, “Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard”, IEEE Transactions on Information Forensics and Security, Vol. 9, No. 5, pp. 772-781, 2014.

36. F. R. Yu, H. Tang, M. Huang, Z. Li and P. C. Mason, “Defense against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios”, IEEE Military Communications Conference (MILCOM), Boston, USA, pp. 1–7, 2009.

37. H. Chen, M. Zhou, L. Xie, K. Wang and K. Li, “Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack”, IEEE Transactions on Vehicular Technology, Vol. 65 No. 11, pp.9181-9191, 2016.

38. A. Rawat, P. Anand, H. Chen and P. Varshney, “Collaborative Spectrum Sensing In The Presence Of Byzantine Attacks In Cognitive Radio Networks”, IEEE Transactions on Signal Processing, Vol. 59, No. 2, pp. 774–786, 2011.

39. S. Althunibat, V. Sucasas, H. Marques, J. Rodriguez, R. Tafazolli and F. Granelli, “On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio”, IEEE Communications Letters, Vol. 17 No. 8, pp. 1564–1567, August 2013.

40. V. Sucasas, S. Althunibat, A. Radwan, H. Marques, J. Rodriguez, S. Vahid, R. Tafazolli and F. Granelli, “Lightweight security against combined IE and SSDF attacks in cooperative spectrum sensing for cognitive radio networks”, Security and Communication networks, Vol. 8, No. 18, pp. 3978-3994, 2015.

41. F. Lin, Z. Hu, S. Hou, J. Yu, C. Zhang, N. Guo, M. Wicks, R. Qiu and K. Currie, “Cognitive Radio Network As Wireless Sensor Network Security Consideration”, IEEE National In Aerospace and Electronics Conference (NAECON), Dayton, USA, pp. 324–328, 2011.

42. Z. Yuan, D. Niyato, H. Li, J. B. Song and Z. Han, “Defeating Primary User Emulation Attacks Using Belief Propagation In Cognitive Radio Networks”, IEEE Journal on Selected Areas in Communications, Vol. 30, No. 10, pp.1850–1860, 2012.

43. L. Li and C. Chigan, “Fuzzy C-Means Clustering Based Secure Fusion Strategy In Collaborative Spectrum Sensing”, IEEE International Conference on Communications (ICC), Sydney, Australia, pp. 1355-1360, 2014.

44. J. Soto, S. Queiroz, M. Gregoriy and M. Nogueira, “A Flexible Multi-Criteria Scheme to Detect Primary User Emulation Attacks in CRAHNs”, International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Madrid, Spain, pp. 1-6, 2013.

45. M.J. Saber and S.M.S. Sadough, “Optimal Energy Detection In Cognitive Radio Networks In The Presence Of Malicious Users”, 3rd International e-Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 2013, pp. 173-177, 2013.

46. W. Wang, H. Li, Y. Sun and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks”, 43rd Annual Conference on Information Sciences and Systems (CISS), Baltimore, USA, pp. 130–134, 2009.

47. AW. Min, KG. Shin and X. Hu, “Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation”, IEEE Transactions on Mobile Computing, Vol. 10, No. 10, pp. 1434–1447, 2011.

48. D. Lingjie, AW. Min, H. Jianwei and KG. Shin, “Attack prevention for collaborative spectrum sensing in cognitive radio networks”, IEEE Journal on Selected Areas in Communications, Vol. 30, No. 9, pp.1658–1665, October 2012.

49. Y. Han, Q. Chen and JX. Wang, “An enhanced D-S theory cooperative spectrum sensing algorithm against SSDF attack”, IEEE Vehicular Technology Conference (VTC Spring), Yokohama, Japan, pp. 1–5, May 2012.

50. HA. Shah, M. Usman and I. Koo, “Bioinformatics-inspired quantized hard combination-based abnormality detection for cooperative spectrum sensing in cognitive radio networks”, IEEE Sensors Journal, Vol. 15, No. 4, pp. 2324–2334, April 2015.

51. W. Wang, L. Chen, KG. Shin, L. Duan, “Thwarting intelligent malicious behaviors in cooperative spectrum sensing”, IEEE Transactions on Mobile Computing 2015, Vol. 14, No. 11, pp. 2392-2405, 2015.

52. V. Zlomislic, K. Fertalj, and V. Sruk, “Denial of service attacks: An overview”, Iberian Conference on Information Systems and Technologies (CISTI), Barcelona, Spain, pp. 1-6, 2014.

53. C. Cormio and K. R. Chowdhury, “A Survey on MAC Protocols for Cognitive Radio Networks,” Ad Hoc Networks, vol. 7, no. 7, pp.1315–1329, 2009.

54. J. Peng, H. Yue, K. Xue, Y. Luo, P. Hong and Y. Fang, "Energy-Aware Scheduling for Multi-Hop Cognitive Radio Networks," in IEEE Transactions on Cognitive Communications and Networking, vol. 2, no. 4, pp. 397-410, Dec. 2016. doi: 10.1109/TCCN.2016.2614838

55. M. Youssef, M. Ibrahim, M. Abdelatif, L. Chen, and A. Vasilakos, "Routing metrics of cognitive radio networks: a survey", IEEE Communication Survey and Tutorials, vol. 16 no. 1, pp. 92–109, 2014.

56. I. Akyildiz, W. Y. Lee, and K. Chowdhury, "CRAHNs: Cognitive Radio Ad hoc Networks", Ad Hoc Networks, vol. 7, no. 5, pp. 810– 836, 2009.

57. L. Ding, T. Melodia, S. Batalama, and J. D. Matyjas, "ROSA: Distributed Joint Routing and Dynamic Spectrum Allocation in Cognitive Radio Ad Hoc Networks", in Proc. 12th ACM international conference on Modeling analysis and simulation of wireless and mobile systems (MsWim), pp. 13–20, 2009.

58. H. P. Shiang and M. van der Schaar, "Distributed Resource Management in Multihop Cognitive Radio Networks for Delay-Sensitive Transmission", IEEE Transactions on Vehicular Technology, vol. 58, no. 2, pp. 941–953, Feb. 2009.

59. X. M. H. Ma, L. Zheng and Y. luo, "Spectrum Aware Routing for Multi-Hop Cognitive Radio Networks with a Single Transceiver", 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp. 1-6, 2008.

60. G. Cheng, W. Liu, Yunzhao L., and W. Cheng, "Spectrum Aware On-Demand Routing in Cognitive Radio Networks", IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pp. 571-574, 2007.

61. G. Cheng, W. Liu, Yunzhao L., and W. Cheng, "Joint on-demand routing and spectrum assignment in cognitive radio networks", IEEE International Conference on Communications (ICC), pp. 6499- 6503, 2007.

62. G. C. Z. Yang and W. C. W. Liu, and W. Yuan, “Local coordination based routing and spectrum assignment in multi-hop cognitive radio networks”, Mobile Networks and Applications, Vol.3, No. 1-2, pp. 67-81, 2008.

63. M. F. K. Chowdhury, “SEARCH: a routing protocol for mobile cognitive radio ad-hoc networks”, Computer Communications, Vol. 32, No. 18, pp. 1983-1997, 2009.

64. S. C. Lin and K. C. Chen, “Spectrum Aware Opportunistic Routing in Cognitive Radio Networks,” IEEE Global Communications Conference (GLOBECOM), pp. 1–6, 2010.

65. Y. Liu, L. Cai, and X. Shen, “Spectrum-aware opportunistic routing in multi-hop cognitive radio networks”, IEEE Journal on Selected Areas in Communications, Vol. 30, No. 10, pp. 1958–1968, 2012.

66. A. S. Cacciapuoti, M. Caleffi, and L. Paura, “Reactive Routing for Mobile Cognitive Radio Ad Hoc Networks”, Ad Hoc Networks, Vol. 10, No. 5, pp. 803–815, 2012.

67. H. Yi Shi and Y.T., “SAMER: Spectrum Aware Mesh Routing in Cognitive Radio Networks”, IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pp. 1-5, 2008.

68. S. j. Lee and M. Gerla, “Split multipath routing with maximally disjoint paths in ad hoc networks,” in IEEE International Conference on Communications (ICC), vol. 10, pp. 3201–3205, 2002.

69. X. Li and L. Cuthbert, “On-demand Node-Disjoint Multipath Routing in Wireless Ad hoc Network”, Annual IEEE Conference on Computer Networks (LCN), pp. 419–420, 2004.

70. Y. Le., X. Cheng, D. Chen, N. Zhang, T. Znati, M.A. Al-Rodhaan and A. Al-Dhelaan, “Distributed back-pressure scheduling with opportunistic routing in cognitive radio networks”, EURASIP Journal on Wireless Communications and Networking, pp.1-14, 2015.

71. F. Tang, L. Barolli, and J. Li, “A Joint Design for Distributed Stable Routing and Channel Assignment Over Multi-Hop and Multi-Flow Mobile Ad Hoc Cognitive Networks”, IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, pp. 1606–1615, 2012.

72. Ch. Pyo and M. Hasegawa, “Minimum Weight Routing based on A Common Link Control Radio for Cognitive Wireless Ad Hoc Networks”, Proc. 2007 International Conference on Wireless Communications and Mobile Computing (IWCMC), pp. 399-404, 2007.

73. K. Habak, M. Abdelatif, H. Hagrass, K. Rizc, and M. Youssef, “A Location-Aided Routing Protocol for Cognitive Radio Networks”, International Conference on Computing, Networking and Communications (ICNC), 2013, pp. 729-733, 2013.

74. Crypto++ 5.6.0 Benchmarks, Available at: http://www.cryptopp.com/benchmarks.html, (2017). Accessed January, 29th, 2017.

75. M. Burrows, M. Abadi and R. Needham, “A logic of authentication”, ACM Transactions on Computer Systems, Vol. 8, No. 1, pp. 18-36, 1990.

76. Cremers. C.: Scyther User Manual, Available at:http://profs.info.uaic.ro/cbirjoveanu/web/Ps/Scyther/scyther-manual.pdf, (2017). Accessed May 16th, 2017.

77. M. Khasawneh, A. Agarwal, N. Goel, M. Zaman and S. Alrabaee, “Sureness Efficient Energy Technique for Cooperative Spectrum Sensing in Cognitive Radios”, 2012 International Conference on Telecommunications and Multimedia (TEMU), Heraklion, Greece, 2012, pp. 25-30.

78. A. Kulkarni and A. Agarwal, “Energy-Efficient QoS based Route Management in Cognitive Radio Networks”, IEEE International Conference on Green Computing and Communications (GreenCom), 2015, pp. 304-310.

79. M. Khasawneh and A. Agarwal, “A Collaborative Approach towards Securing Spectrum Sensing in Cognitive Radio Networks”, The 11th International Conference on Future Networks and Communications (FNC), Procedia Computer Science, pp. 302 – 309, 2016.

80. M. Khasawneh and A. Agarwal, “A Secure and Efficient Authentication Mechanism Applied to Cognitive Radio Networks”, IEEE Access Journal, vol. 5, pp. 15597-15608, 2017, doi: 10.1109/ACCESS.2017.272332.

81. M. Khasawneh and A. Agarwal, “A Secure Routing Algorithm based on Nodes Behavior during Spectrum Sensing in Cognitive Radio Networks”, The 35th IEEE International Performance Computing and Communications Conference (IPCCC2016), pp. 1-8 Las Vegas, NV, USA, doi: 10.1109/PCCC.2016.7820642.

82. M. Khasawneh, A. Agarwal, N. Goel, M. Zaman and S. Alrabaee, “A Game Theoretic Approach to Power Trading in Cognitive Radio Systems”, The 20th International Conference on Software, Telecommunications and Computer Networks - SoftCOM 2012, September 11-13, 2012, Split, Croatia.

83. M. Khasawneh, A. Agarwal, N. Goel, M. Zaman and S. Alrabaee, “A Price Setting Approach to Power Trading in Cognitive Radio Networks”, The 4th International Workshop on Mobile Computing and Networking Technologies 2012, WMCNT 2012, St. Petersburg, Russia.

84. S. Alrabaee, A. Agarwal, D. Anand and M. Khasawneh, “Game Theory for Security in Cognitive Radio Networks”, International Conference on Advances in Mobile Network, Communication and its Applications – MNCApps 2012, Bangalore, India, Aug 1-2, 2012, Pages 60-63.

85. S. Alrabaee, A. Agarwal, N. Goel, M. Zaman and M. Khasawneh, “A Game Theory Approach: Dynamic Behaviors for Spectrum Management in Cognitive Radio Network”, GC'12

Workshop: The 4th IEEE International Workshop on Management of Emerging Networks and Services - MENS 2012, December 3-7, 2012, Anaheim, California USA.

86. S. Alrabaee, A. Agarwal, N. Goel, M. Zaman and M. Khasawneh, "Comparison of Spectrum Management without game theory (SMWG) and Spectrum Management with game theory (SMG) for Network performance in Cognitive Radio Network", 2012 Seventh International Conference on Broadband and Wireless Computing, Communication and Applications, Nov 12-14, Victoria, Canada
87. S. Alrabaee, A. Agarwal, N. Goel, M. Zaman and M. Khasawneh, "Routing Management Algorithm based on Spectrum Trading and Spectrum Competition in Cognitive Radio Networks", 2012 Seventh International Conference on Broadband and Wireless Computing, Communication and Applications, Nov 12-14, Victoria, Canada.
88. Saed Alrabaee, Anjali Agarwal, Nishith Goel, Marzia Zaman, Mahmoud Khasawneh, "QoS-CRNSM: QoS Routing Algorithm for Cognitive Radio Network Based on Spectrum Management", The 20th International Conference on Software, Telecommunications and Computer Networks - SoftCOM 2012, September 11-13, 2012, Split, Croatia.
89. S. Alrabaee, A. Agarwal, N. Goel, M. Zaman and M. Khasawneh, "A Game Theoretic Approach to Spectrum Management in Cognitive Radio Network", The 4th International Workshop on Mobile Computing and Networking Technologies 2012, WMCNT 2012, St. Petersburg, Russia.