Security Frameworks Design and Implementation for Dynamic Management of Data and Information in Cognitive Radio Networks

Obeten O. Ekabua
Department of Computer Science
North West University, Mafikeng Campus
Private Bag, X2046, Mabatho
2735, South Africa

Ifeoma U. Ohaeri
Department of Computer Science
North West University, Mafikeng Campus
Private Bag, X2046, Mabatho
2735, South Africa

Bassey E. Isong
Department of Computer Science
University of Venda
Private Bag X5050, Thohoyandou
South Africa

ABSTRACT
Cognitive radio network is a new innovation wireless technology aiming to improve the utilization of the electromagnetic spectrum. Cognitive radio network consists of several cognitive radio devices which run radio applications software to perform signal processing using the frequency bandwidth. The use of this software enables the device to sense and understands its environment and change its mode of operation based on its observation. These devices are dynamic in nature and require effective dynamic management of the spectrum resources (data and information). The challenge arising from the management of these resources dynamically impedes secure communication. Consequently, these challenges have necessitated the main goal of this research paper which is, to develop an authentication and authorization framework for CRNs that establishes access control to the networks resources, and enhances the management of data and information dynamically. The frameworks developed and implemented in this research paper guarantee secured communication and quality of service in cognitive radio networks.

Keywords
Dynamic Spectrum Access, Security Policy Enforcement Point, Security Policy Decision Point

1. INTRODUCTION
Cognitive radio network is a dynamic, intelligent and multiuser communication network that can automatically sense the environment and adapt the communication parameters accordingly. This type of network has application in dynamic spectrum access (DSA), co-existence of different wireless networks, and interference management. The devices in cognitive radio networks exhibit the automation capability that enables it to learn from the environment, and be able to optimize its transceivers performance in the radio frequency (RF) spectrum.

This means that communication between multiple users in cognitive radio network is achieved in a self-organized manner, to control the communication channels by allocating the available resources properly and to build an environment of self-configuration, self-awareness, self-adaptation, and self-optimization [1].

The growing demand for radio frequency (RF) spectrum has led to the introduction of an efficient technology and a more efficient spectrum management era very necessary. This innovative technology to improve spectrum utilization has the capability to make more efficient use of spectrum resources, and also offer a more versatility, flexibility and interoperability, with the increased ability to adapt their operations based on environmental factors. Management of data and information in cognitive radio network is moving from static to dynamic in other to take advantage of the innovations for a more efficient usage, and effective management [2].

It provides an enabling environment for and efficient resource allocation and effective spectrum access control. The fundamental aims of cognitive radio-based wireless network are; secured communication through an effective access control technique and efficient usage of spectrum resources. In the process of establishing these fundamentals, adequate security measure should be considered [3].

Also, the distributed and wireless nature of cognitive radio networks makes it vulnerable to various malicious attacks which results into huge security challenges which are capable of overriding the advantages of this new and promising technology [4]. Hence a security mechanism such as; authentication and authorization becomes very necessary for dynamic management of data and information [5].

Dynamic management of data and information in cognitive radio network is applied in broad sense and manner which involves processes. These processes depends on networks requirements needs which includes security as a major factor [6]. The cognitive radio network management system should be able to provide a security scheme or framework that will establish the identity of the users (authentication), securing communications (encryption and decryption), and determining who is permitted to perform what actions (authorization), and recording the operations processed by the system (accounting and auditing), for the purpose of verification and detection of malicious users. The security system is customizable and network dependent. This customizable level of security can improve the organizations structure and also capable of adapting to its changing requirement [7].

The security threats in cognitive radio entail majorly illegal information injection and forging of information transmission. This security framework is advantageous as its features allow access to only the right users or groups.

2. RATIONALE OF FRAMEWORK

The purpose of the framework in the context of this paper is to ensure a secure communication in cognitive radio network uses authentication, authorization, and security mechanism to protect data and information along the line of transmission and also prevent malicious secondary users of the spectrum and network attacks. However, the benefits are as follows:

(a) The framework provides scalability: Typical A-A configurations depend on a server to or a group of servers to store user name and password. The essence of this is that local databases are not to be built and updated on every router and access server in the network.

(b) The framework allows the network administrator to configure multiple backup systems. For instance, an access server can be configured to first consult a security server and then the local database before any access is granted.

(c) The framework supports standardized security protocols like TACACS +, RADIUS, and Kerberos.

(d) The framework provides an architectural capability for configuring two different security measures; authentication, authorization.

3. REQUIREMENTS ANALYSIS

Requirement analysis firstly specifies the underlying requirement for designing and developing the authentication and authorization framework. The host network is the object, while the client host is referred to as the subject. Authentication concentrates on the subject requesting for connection to the network, while authorization concentrate on the subject requesting for a resource.

When the user dials into an access server which is configured using authentication protocol, the access server and spectrum manager prompts the user to make a user name and password available. The security policy decision point (SPDP) which is the request admission control and handoff point, checks to verify if the user is who he claims to be. The security policy enforcement point (SPEP) ensures that the service management policy is enforced by granting or denying access based on network policy.

The access server verifies a user by requesting for user name and password. This verification process is referred to as authentication. At this point the user may either be denied access or granted access. If authentication is successful then the user can be able to execute commands on the network server. The server then determines the commands and resources that should be made available to the user and specifies the privileges and rights the user should have. This process is referred to as authorization.

However, the framework is developed through four operational stages via: “login”, “connection and resource request”, decision and,” grant” or “deny” access stage.

3.1 Authentication

Radio Network (CRN) that ensures that entities (users) are truly who they claim to be. This is verified before access to the network is granted. It actually associates a unique identity to each user in CRN, such as user identification name or password as approved by the service security policy. Using these unique forms identification client (users) can freely request for the spectrum resources. It involves the process of verification and validation of users’ identity (ID).

(i) Requirement Name: Login
Description: This feature enables communication with the server.
Justification: This feature allows a new window to open for connection request to the server by the client.

(ii) Requirement Name: Server Request
Description: This request will permit the client access into the network for the service he or she wants to access.
Justification: The framework should request the client identity details by requesting for the user identity (user name and password based on the network configuration, authentication protocols and security policy enforcement point (SPEP).

(iii) Requirement Name: Decision
Description: This feature allows the framework to make decision based on the security data and service profile. This stage is handled by the request admission control and handoff which consists of the security policy decision point (SPDP) and SPEP. **Justification**:The framework should ensure that the client is who he claims to be, before permission to access the network is granted based on SPEP and SPDP.

(iv) Requirement Name: Grant or Deny Access.
Description: The framework should ensures that all the network services and communications are secured from intrusion and unauthorized access.
Justification: The framework should permit all authenticated client to have access to the services available.

3.2 Authorization

Authorization is a security measure that allows access to only the right entities (users) having the approved privilege to the particular resources requested. Different forms of authorization exist such as; out band authorization, signature authentication and password authentication. Moreover, for any communication (interaction or conversation) involving different parties or entities exchanging information, there should exist, a mutual trust relationship across the multiple domains in CRNS.

(i) Requirement Name: Resource Request
Description: This feature will permit the authenticated user, to request for specific services and resources he or she wants to ace ss.
Justification: This framework should validate the users request based on service policies before access is released.

(ii) Requirement Name: Decision
Description: This feature allows framework to make decision based on the privileges the client has over the resources available in the in the network. This stage is usually handled by the request admission control and handoff domain which consists of SPD and SPEP.

Justification: The framework makes sure that the user (client) has access to only the resources which he or she has the right or privilege to access.

(iii) Requirement Name: Grant or Deny Access
Description: The framework should ensure that all the network resources are protected from unauthorized users.
Justification: The framework should ensure that all users strictly conform to service policies for authorizations based on the privileges given to the user so as to have access to the services and resources provided by the network.

3.3 Use Cases

This section of the requirement analysis provides a vivid description of the authentication and authorization framework using use case. It shows how data and information in cognitive radio network is protected and secured using authentication and authorization (A-A) access control measures. Authentication of a user is used to ensure that only the authorized user is allowed into the network and granted access to specific resources and services in CRN. Some of the techniques used to achieve authentication are; user profile, user account, user password, biometrics, network authentication, pin numbers and codes. The server uses this processes to determine the commands and resources that should be made available to the user.

(a) Use Case Diagram Describing Authentication

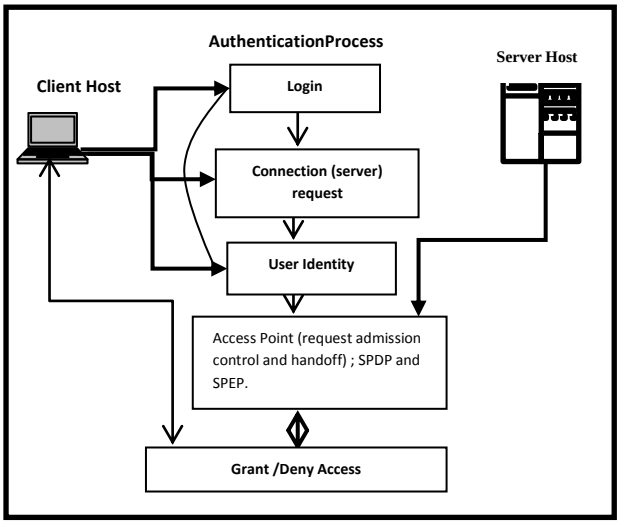

Figure 1: Use Case Diagram Describing Authentication

During registration, the user identity (user ID) or user profile is assigned to each user by the user manager which is a component of the network server. This user profile stipulates the limits to which a user is permitted to access the network (permitted days, and time of the day, geographical areas or physical locations), and permitted number of incorrect login). The user profile or user ID provides access details such as: data and network resources that a user is to access and the type of access like (create, read, write delete). In access by biometric method the user can have access based on finger prints, hand or retina scanning using biometric system. This user information is stored in the user database located in the network server.

However, in this authentication process, the client hosts stores the identification information of the user who wants to have access to the network service. Once the user logs in from the login page of the network using the user profile, requesting for connection to the server host of CRN, the access point which is the request admission control, and handoff intercepts the request and the user ID to verify if the user is who he claims to be, and if profile details and security data correspond with the one captured in the network database by the user manager. The security policy decision point (SPDP) makes conclusion and decides if the request should be granted or not and the security policy enforcement point enforces (implements) the decision of the SPDP. If the user is who he claims to be, access to the CRN service is then granted or denied if otherwise. This process ensures that, only the legitimate users have access to the network service.

(b) Use Case Diagram Describing Authorization

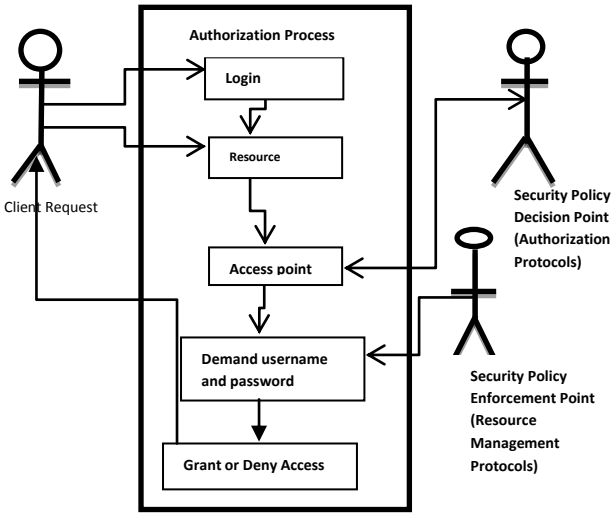

Figure 2: Use Case Diagram Describing Authorization.

The authorization process is slightly different from authentication process at the client request window. The client (user) requests for a specific resource available in the network having been authenticated by the network security check point. The access point which is the SPDP as usual intercepts the request and demand for the user profile and security information to determine the rights and privileges assigned to the user, and check if there are certain conditions attached to it. The decision of the SPDP is passed to the SPEP for enforcement. The SPEP ensures that the decisions of the SPDP are rightly effected. If the user has the access to the resources requested, then the user is granted access to the specific resources requested, otherwise access is denied.

This verification process in authentication and authorization framework is in response to the research objective.

3.3.1 Use Case Analysis

The authentication and authorization requirement is further analyzed using the use case table below. The description process employed in the use case has two sections which are for authentication and authorization respectively. Each section is made up of tables, having two rows and of the login sequence, the connection and server request or resource request for authorization, checks decision, and grant or deny access respectively. The rows contain the use case name, the participating actor, the entry condition, the flow of events, and the exit condition while the columns explain the rows respectively. Consequently, the details are as follows:

(a) Authentication

(i) Login Sequence

Table 3.1 Login Sequence

Use Case Name	**Login.**
Participating Actor	Initiated by Client communicating with the system.
Entry Condition	The client login for connection to CRN server. Requesting connection to the network.
Flow of Events	Server demands for username and password. Client enters Registrations Identity (username and password).
Exit Condition	A new window opens if username and password is authentic.

(ii) Connection (Server) Request

Table 3.2 Connection Request

Use case Name	**Connection Request**
Participating actor	Initiated by Client
Entry condition	Client request for spectrum resource.
Flow of Events	The Security Policy Enforcement Point (SPEP) – checks to verify the user security data and service profile, to identify if the user is who he claims to be based on the network configuration and authentication protocols (AP). The Security Policy Decision Point (SPDP) decides whether or not to grant access based on Resource Management Policy (RMP).
Exit condition	SPEP checks the decision provided by (SPDP) to either grant or deny access.

(iii) Check Decision

Table 3.3 Check Decision

Use case Name	**Check decision**
Participating Actor	Initiated by SPDP-known for Connection Admission Control and handoff.
Entry Condition	SPDP checks the responds of the SPEP based on the client request.
Flow of Events	The SPDP provides authentication to the SPEP based on SPED and RMP.
Exit Condition	The SPEP verify the decision if the client is authenticated and have to access the network service.

(iv) Grant Access or Deny Access

Table 3.4 Grant or Deny Access

Use Case Name	**Grant or Deny Access**
Participating Actor	Initiated by SPED- known for connection admission control and handoff.
Entry Condition	SPED inspects if the decision that was made by SPDP was actually based on the client request for network service.
Flow of Event	SPEP checks if the client was granted access or not and implements the decision.
Exit condition	A new window opens. Access is granted if the client is authenticated, else access is denied and registration details are requested the SPEP.

(b) Authorization

(i) Login Sequence

TABLE 3.5 LOGIN SEQUENCE

Use Case Name	**Login**
Participating Actor	Initiated by client communicating with the system.
Entry condition	The authenticated user login to access resource.
Flow of Events	The user enters username and password in other to access a desired resource.
Exit Condition	A new window opens if the username and password is correct.

(ii) Resource Request

TABLE 3.6 RESOURCE REQUEST

Use Case Name	**Resource Request**
Participating Actor	Initiated by the (authenticated) user
Entry Condition	User requests for a specific resource in the network.
Flow of Events	SPEP and SPDP and enforcement protocols checks if the client is an authorized user of the resources or services.
Exit Condition	Access denied. Server requests for registration details (security data and user profile) for proper identification.

(iii) Check Decision

Table 3.7 Check Decision

Use Case Name	**Check Decision**
Participating Actor	Initiated by SPDP.
Entry Condition	SPDP checks the message sent by SPEP, based on users' request.
Flow of Events	APDP can then make available authorization service to SPED.
Exit Condition	SPEP, checks decision if the user is authorized to have access to the resource.

(iv) Grant or Deny

TABLE 3.8 GRANT OR DENY ACCESS

Use Case Name	**Grant or Deny Access**
Participating Actor	Initiated by SPEP.
Entry Condition	SPED inspects if the decision lines with the users request to the resource, also the AP components and RMP (authentication protocol and resource management protocol.
Flow of Events	SPEP checks if the user is an authorized user to access such services requested, based on the authentication

	protocol (AP) and RMP.
Exit Condition	SPEP checks permission of clients, if user is authorized then SPEP grants access, if otherwise, access is denied. Server request for registration details (security data and service profile) for proper identification.

4. FRAMEWORK CAPABILITIES

In this section the underlying capabilities of the framework are specified to enable the designing of CRN authentication and authorization framework in the next chapter. The capabilities include; interoperability, integration and trust relationship and they ensure reliability and QoS.

(i) Interoperability

This is the capability that allows multiple entities in different domain and hosting environment to interact with each other and exchange messages to identify a user from one domain in another domain, having a central database. It enhances efficient sharing of resources within the network environment.

(ii) Integration

The proposed security infrastructure is required to enable integration and compatibility among the host environment and other new security mechanisms that will be incorporated as the network expands.

(iii) Trust Relationship

It is necessary to establish a trust agreement and relationship between different entities and several components in a distributed network for sharing data and information. It also assists in determining identity profile and security data when necessary. It guarantees and promotes confidence for effective interactions. CRN is a dynamic and multiuser system, consequently, this capability enables efficient and effective resource control stages or processes as used in this research.

CRN is a dynamic and multiuser system, consequently, this capability enables efficient and effective resource control stages or processes as used in this research project such as; connection request for authentication and resource request for authorization, decision stage by the server host based on the particular resource the client request for. However, all the components of authentication and authorizations are carefully specified in other to develop a reliable framework.

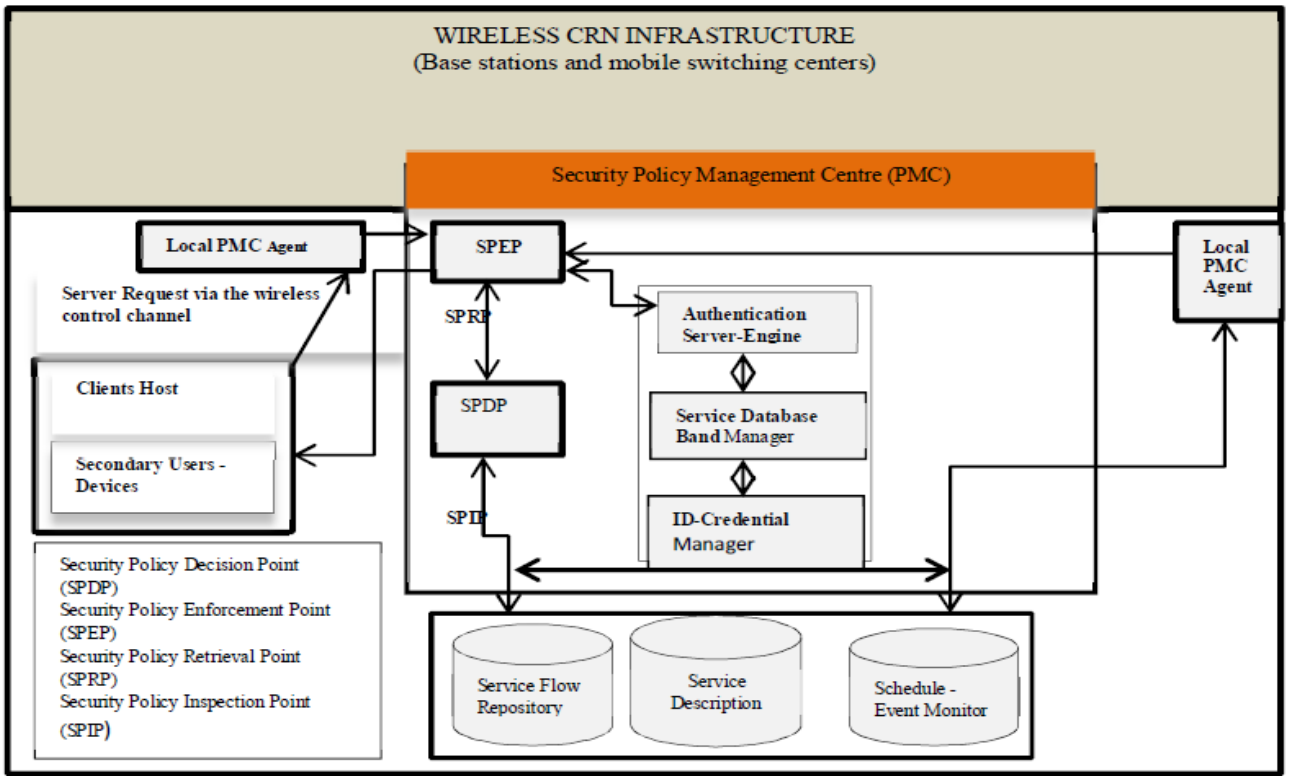

Figure 3: Authentication Framework

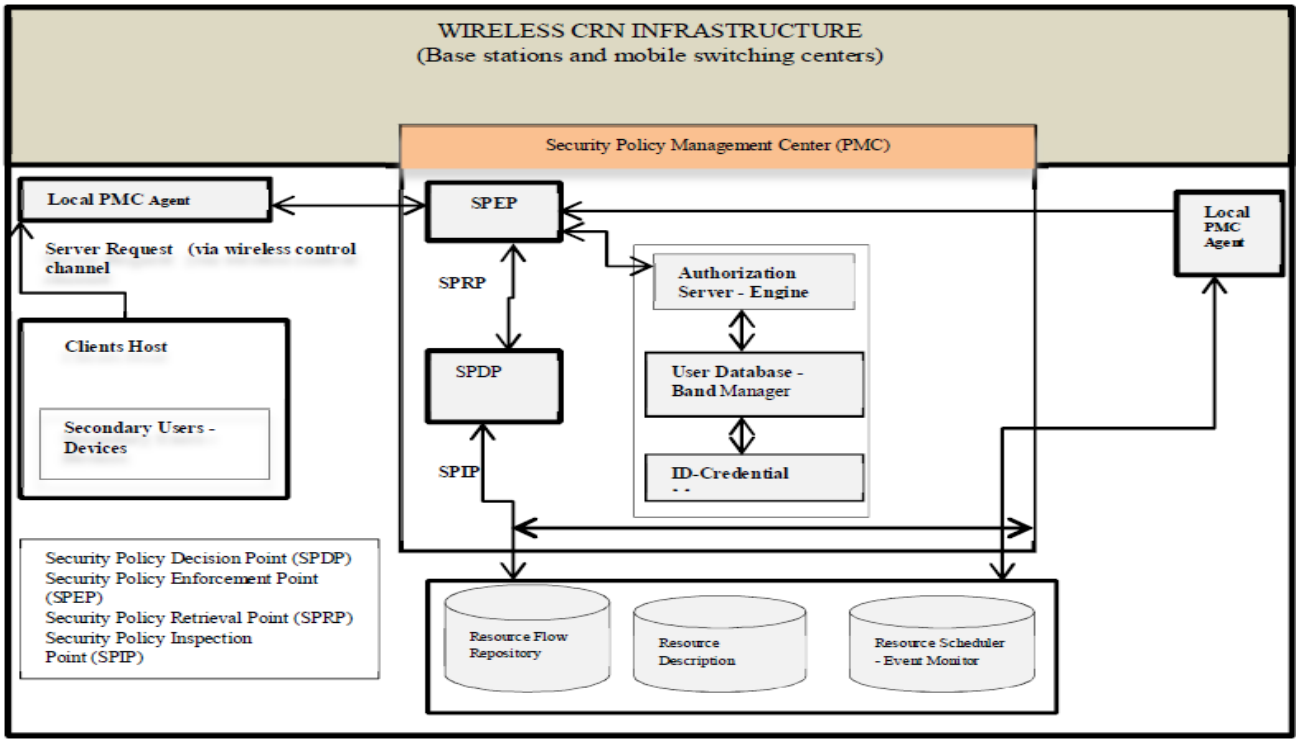

Figure 4: Authorization Framework

5. CRN AUTHENTICATION-AUTHORIZATION FRAMEWORK

Using CRN and its functionality, we introduce the Authentication and Authorization Framework, designed specifically for the network.

5.1 Authentication Framework

Figure 3 above represents the design of authentication framework for cognitive radio network, and the interaction that exist between them to achieve secure communication and quality of Service (QoS) in the CRN networks.

5.2 Authorization Framework

The figure 4 below is the skeletal design of authorization framework for cognitive radio network, showing the relevant components and its functions and how they interact to achieve secured communication and quality of service (QoS).

Authorization and Authentication are interwoven and interrelated because they strive for one purpose, which is to control access to network resources by restricting unauthorized, malicious users and protect network devices to ensure that data and information in CRN are dynamically managed. Consequently, the structure of the authorization framework for CRNs in figure 4 appears to be the same as in authentication except for some features which are specific and particular to authorization. Any request for the resources available in the network is first intercepted by the SPEP, the request interface passage which is located in the SPMC that ensures. The SPMC then ensures that the user has been authenticated and should request for any of the resources available in the spectrum.

The SPMC then enforces the security policy by constructing an authorization decision query based on the user profile security identity and reason for the request. It later sends it across to the authorization server and engine which will verify the user identity and service policy profile to determine the rights and privileges assigned to the user from the database. The result is passed across to SPDP to handle the decision to either grant or deny access. The outcome is returned back to SPEP via the SPRP for enforcement and client notification. If the user is an authorized user of the resources requested, access will be granted otherwise access is denied. By this all access to all network resources are restricted to only the legitimate clients.

Where supported by the client operating system, the wireless network will perform checks for minimum client security standards (client integrity checking) before granting access to the Cognitive Radio Network resources. However, authentication and authorization are inseparable in terms of application. They work together to achieve Cognitive Radio Network security as a common goal.

6. THE CRN THREATS

The high and quality performance of CRN technology lies majorly on an effective security measure. It guarantees the availability and robustness of network service and resources against the security challenges (threats and attacks). The following are some threats and attacks that may transpire in this CRN environment [9]:

(i) Jamming of cognitive radio channels

Cognitive channels that transmit messages can also be made to jam in other to disrupt the messages passing through the network. The cognitive control channels (CCC) are made to transmit wrong messages or right messages in wrong forms. This

makes the network fall short of the quality of service (QoS) assurance

(ii) Denial of Access

This is an unauthorized use of the spectrum band resulting into the primary (licensed) users loosing access to the network resources and services. Most times the network is been hijacked by these malicious users for selfish use and personal gains. When cognitive radio node emits power in an unauthorized spectrum, it makes primary users to lose access and malicious entities takes advantage of this nature to intrude and seize network.

(iii) Eaves dropping of cognitive messages.

Cognitive radio messages can be intercepted by a malicious user who can make use of the information to lunch several other attacks on the primary users of the network or the network itself.

(iv) License user emulation

Licensed users can be emulated by malicious users impersonating their details, camouflaging some trusted nodes, causing other node to join the network undetected, sending false routing information. Transmitted packets can be intercepted while on transit by malicious users thereby having access to cognitive messages to their advantage. Malicious cognitive users can exchange or alter cognitive messages for ulterior motives and as well change cognitive radio nodes causing interference and internal node failure which can result into network failures.

7. AUTHENTICATION-AUTHORIZATION RELATIONSHIPS

The design and implementation of the authentication and authorization security frameworks is capable of controlling access and dynamically manage data and information in cognitive radio network to establish control against unauthorized and malicious intruders.

User authentication and authorization is a crucial management component for a secured communication in CRNs. Authentication and authorization frameworks are tightly-coupled security mechanisms for data and information management in CRNs. However, they differ in some ways. Authorization process depends on secured authentication mechanism which ensures that a user is who he claims to and thus prevent malicious intruders from gaining access to the secured network resources but also differ in some ways. However, they both offer effective and efficient access control for the dynamic management of data and information in cognitive radio network.

Authentication is a security mechanism which provides a means of identifying a user by mandating the user to enter a valid user name and valid password before access to the network service is granted. The process of authentication is determined by each user having a unique identity for gaining access to the network service. The A-A server compares a user's authentication details with the identification details stored in the database. If the details correspond, then the user is granted access to the network. If both information differs the authentication process will fail, then access to the network service is denied.

Authorization is a security mechanism which determines the level of access or specific or particular authenticated user should have to the available and secured network resources. It determines whether a user has the authority to issue certain commands. However, the process enforces policies such as determining what types of activities, resources, or services a user is permitted to perform in the network.

8. COMPARATIVE STUDY OF EXISTING TECHNIQUE

Here we present a tabular format of the comparative study showing existing techniques/main idea, research achievements and the authors.

Table

Techniques / Main Idea	Research Achievements	Research Authors
A novel physical layer authentication technique, light weight authentication technique and light weight authentication protocol in detecting attacks and intrusions.	Thee security mechanism is authenticating primary user signals in cognitive radio networks via integrated cryptographic and wireless link signatures	Liu et al [52]
A light weight public key cryptography mechanism between primary users and secondary users.	The security mechanism used digital signatures for centralized dynamic spectrum access networks.	Mathur et al [54
A distributed and collaborative architecture using anomaly detection technique.	The security mechanism identifies attacks in distributed wireless networks.	B. Sun et al [35]

9. FRAMEWORK IMPLEMENTATION

The implementation phase demonstrates how CRN clients interact with the system with the aim of proving the concept of authentication and authorization framework for cognitive radio network.
It also shows how access to the services provided by the CR network is controlled and monitored using authentication and authorization access control mechanism as a protective measure against unauthorized and malicious users.

The different interfaces presented in this section indicate the clients' interactions with the system before access is either granted or denied to ensure effective and dynamic management of data and information in cognitive radio network.

(a) Jenhosting CRN

The framework is implemented using *Jenhosting* Company (JHC). The company provides numerous services among which are mobile telephony, mobile services, mobile internet and fixed telephony as shown in Fig. 15b. It has numerous clients (subscribers) which include Vodacom, MTN, Celtel, Univen and others. The interface of Fig. 12 shows the CRN home page from which you can navigate to other network domain such as services offered by the network as shown in Fig.16, contact information as shown in Fig.15 and other information about the company as shown in Fig.14, including

how to register as shown in Fig.16 and the login outcomes as shown in Fig.18a, Fig. 18b and Fig.18c.

(1) Jenhosting CRN Company Home Page

The home page of JENHOSTING Company is the main page of the network, which is the entry point to the Cognitive radio infrastructure. It consists of the login button, the register button, including sites of interest shown in figure 5 and other vital information about the services rendered by the company.

Figure 5: Cross Section Jenhosting CRN Home page

(2) Jenhosting Welcome page

This shows the page that comes up when the new member button is clicked

Figure 6: Jenhosting Welcome Page

(3) Jenhosting CRN General Information Section

The figure 7 and figure 8 interface shows the outcome after the 'About us' and 'Contact us' button has been clicked from the home page. All necessary information about the network operations, services offered, including the contact information is viewed from these domains.

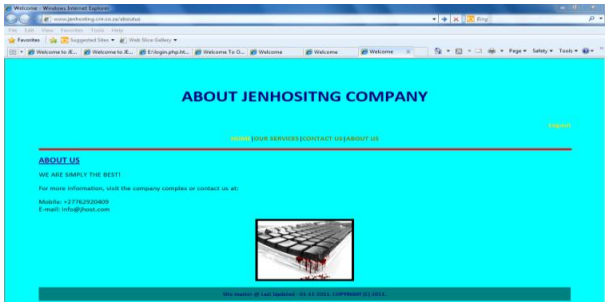

Figure 7: Service Inquiries Page

(4) Jenhosting CRN Contact Information Section

This page displays the contact information page when the contact button is clicked.

Figure 8a: Contact Page

(5) Jenhosting CRN Services

This page displays both the services offered by the cognitive radio network and the available services at the time the service button is clicked.

Figure 8b: CRN Services Page

(6) Clients e-Registration Section

All the basic information required for the registration of the clients based on the network service policy needed for authentication and authorization are captured from this domain and stored in the data base as shown in Fig. 10.

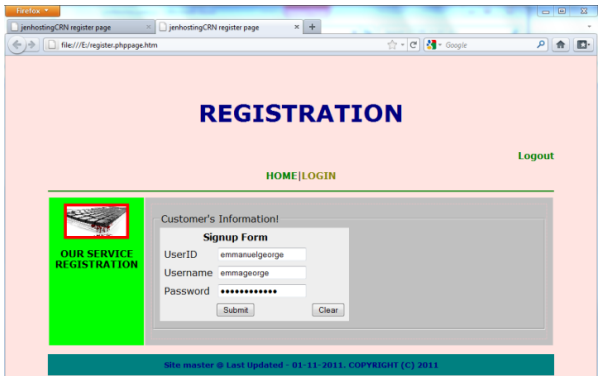

Figure 9: e-Registration Section

(7) Jenhosting CRN Database

This represents the authentication and authorization management database and it consists of all the registered clients of the network. The clients name, service name,

service ID, password, e-mail and year of registration are clearly specified and stored in this domain for authentication, authorization and security policy services.

Figure 10: Jenhosting CRN Database.

(8) Successful Login

When a request for services is initiated, the client would need to login to the system by supplying identification details (username and password). The details would then be verified and validated from information already stored in the CRN client membership database. A successful login access is granted only if the user is who he claims to be as verified and validated from the database information. In situation where access is not granted, it therefore implies that the request is invalid and an unsuccessful login message would be displayed.

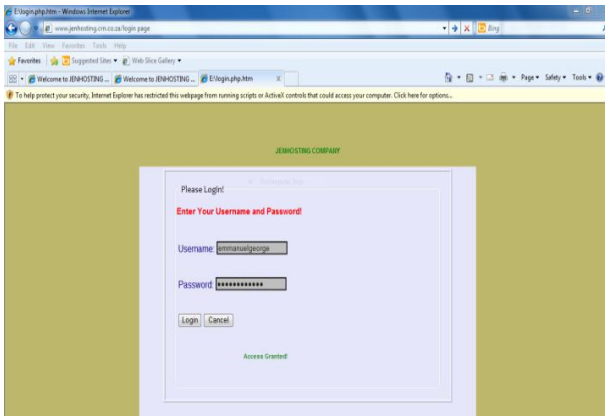

Figure 11a: Successful Login

(9) Unsuccessful Login

Denial of access to resources during identification of users requesting for services is usually displayed with an unsuccessful login message. This usually happens when a non-registered client is attempting to request for rights of service usage. In such a situation, the system would display unsuccessful login message as a means not to allow malicious intruders into the available services. Unsuccessful login can only be adverted by service requesters registering with the service provider to be allowed access into the CRN resources.

Figure 11b: Unsuccessful Login

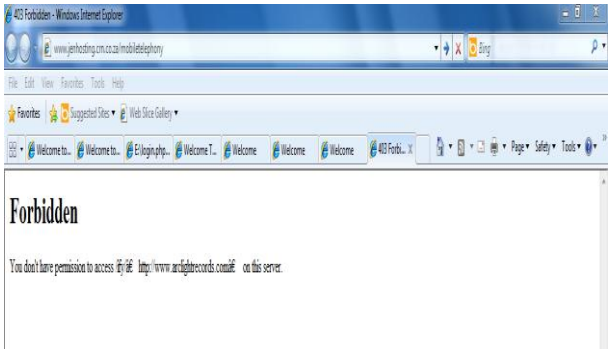

Figure 11c: Unsuccessful Login Section

(10) Delete Account Section

This implementation phase ensures that no unauthorized user or malicious user masquerades as a legitimate user to gain access to the network server or the resources available in the network for malicious use. This section of the network has the capability to delete the user account and disable the root connections to such users to ensure efficient access control and effective dynamic management of data and information in the specified CR Network.

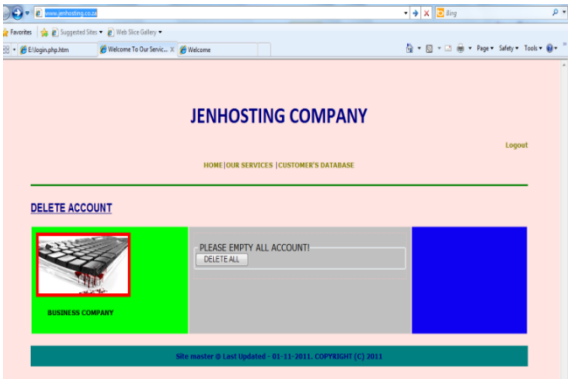

Figure 12: Account Delete Section

10. CONCLUSIONS

Wireless communication technology is transiting to an interactive internet data and multimedia applications from wireless telephony for a higher and efficient rate of data transmission. The rate at which devices go wireless is in the increase, therefore, it becomes necessary to handle the issue

of spectral crowding, and coexistence of wireless devices which is as a result of limited availability of bandwidth. The effort to accommodate this high demand for the limited spectral band introduced this exciting technology referred to as cognitive radio network which offers new ways of exploiting the available radio spectrum which are underutilized by the licensed users.

The spectrum has now become a heterogeneous infrastructure due to the high rate of user capacity, data transmission and deployment of the wireless networks. Consequently, this gives rise to several challenges which cuts across insecurity. Security in Cognitive radio networks is very necessary to ensure secured communication through an effective access control mechanism. Apparently, this enables effective management of data and information in cognitive radio networks. Reported in this paper is the design and implementation of authentication, and authorization security mechanism to alleviate the security challenges encountered in CRNs. We have also presented a use case diagram and its analysis to further illustrate the allocation of spectrum resources its regulation and service policy enforcement to adequately ensure security. Obviously, several tools are on the shelf which is used by intruders or attackers to penetrate networks domain. This results into a rapid increase in cognitive radio networks attacks and intrusions. Therefore, security cannot be over emphasized as further research in security infrastructures for dynamic management of data and information in cognitive radio networks is ongoing.

11. REFERENCES

[1] Wang, B and Liu, K.J.R., "Advances in Cognitive Radio Networks: A survey." Journal of IEEE, 2011.

[2] An K, P., 2008. Cognitive Radio Defying Spectrum Management. In Proceedings.

[3] Hwang J., and Hyenyoung Y., 2008. Dynamic Spectrum Management Policy for Cognitive Radio: An Analysis of Implementation Feasibiliy Issues. In Proceedings of IEEE DySPAN Symposium.

[4] Xiaoyong T, Kenli L.,Zeng Z., and Veeravalli B., "A Novel Security Driven Scheduling Algorithm for Procedure Constrained Tasks in Heterogenous Distributed Systems." Journal of IEEE. 2011.

[5] B.O Pages, I. Foster, F. Siebenlist, and A. Rachans, 2006. A Multipolicy Authorization Framework for Grid Security. In Proceedings of the Fifth IEEE Symposium on Network Computing and Application.

[6] P. Steenkiste, D. Sicker, G. Minder, and R. Dipankar, 2009. Future Directions In Cognitive Radio Network Research. In Proceedings of NSF Workshop Report.

[7] V. Sharma, Y. S Mann, 2010. "Emerging Technologies in Web Intelligence." Journal of Infosys Technologies, 2009.