A Secure Spectrum Aware MAC layer protocol for Cognitive Radio Wireless Sensor Network.

By

Student Name:Md Shamiun Hossain
ID:012201045

Submitted in partial fulfilment of the requirements
of the degree of Master of Science in Computer Science and Engineering

March 4, 2026

Department of Computer Science and Engineering
United International University

Approval Certificate

This thesis titled **'A Secure Spectrum Aware MAC layer protocol for Cognitive Radio Wireless Sensor Network'** submitted by **'Md Shamiun Hossain'**, Student ID: **'012201045'**, has been accepted as **Satisfactory** in fulfillment of the requirement for the degree of Master of Science in Computer Science and Engineering on 'Date of approval'.

Board of Examiners

1.

_____ **Supervisor**

Name of the supervisor:Prof. Dr. A.K.M Muzahidul Islam
Designation:Professor, Dept. of CSE
Affiliation:united international university

2.

_____ **Head Examiner**

Name of the Head Examiner:Prof. Dr. Md. Motaharul Islam
Designation:Professor, Dept. of CSE
Affiliation:united international university

3.

_____ **Examiner-I**

Name of the Examiner-I: Mr. Mohammad Mamun Elahi
Designation:Assistant Professor, Dept. of CSE
Affiliation:united international university

4.

_____ **Examiner-II**

Name of the Examiner-II:Prof. Dr. Mohammad Shahriar Rahman
Designation:Professor, Dept. of CSE
Affiliation:united international university

5.

_____ **Ex-officio**

Name of the Ex-officio:Prof, Dr. Prof. Khondaker A. Mamun
Designation:Professor, Dept. of CSE and Director-MSCSE Program and IRIIC
Affiliation:united international university

Declaration

This is to certify that the work entitled **'A Secure Spectrum Aware MAC layer protocol for Cognitive Radio Wireless Sensor Network '** is the outcome of the research carried out by me under the supervision of **'Prof. Dr. A.K.M Muzahidul Islam'**

Student Name:Md Shamiun Hossain
MSCSE Program
Student ID: 012201045
Dept. of Computer Science and Engineering
United International University
Dhaka, Bangladesh

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

Name of the supervisor:Prof. Dr. A.K.M Muzahidul Islam
Designation:Professor, Dept. of CSE
Affiliation:united international university

Abstract

Persistent Secure Spectrum Aware MAC layer, scalability and load balancing are important requirements for numerous ad-hoc sensor network. Secure Clustering sensor nodes is an effective technique for achieving these goals. In this work, we present a secure, spectrum-aware cross-layer MAC protocol designed for Cognitive Radio Ad Hoc Networks (CRAHN), where cluster formation is defined maximum edge biclique problem, enhance the security of the cluster formation process and ensure both a stable number of common channels and robustness to varying spectrum availability. The clustering process concludes in $\mathcal{O}(1)$ of iterations, independent of the network's structure or scale. By carefully choosing the secondary clustering parameter, the process can significantly reduce the hassle of re-clustering. This thoughtful selection ensures that the workload is evenly spread across the cluster heads, preventing any one cluster from becoming overloaded, and keeping the network running smoothly and efficiently. Dynamic approach maintains a stable network structure despite node mobility. These protocols focus on secure and efficient spectrum sharing among nodes to enhance network performance. It also achieves fairly uniform cluster head distribution across the network. The cluster-based architecture is designed to be highly flexible, allowing it to build and adjust itself as needed. This dynamic nature is supported by two key operations: *Node-Move-In* and *Node-Move-Out*. These operations enable the network to easily integrate new nodes and remove existing ones, ensuring that the system can adapt to changes and maintain optimal performance without manual intervention. A pseudocode analysis focused on enhancing the security of the cluster formation process is also applied in two topology management operations. Overall, the time complexity for the *Node-Move-In* and *Node-Move-Out* algorithms is $\mathcal{O}(n)$, where n represents the number of members in the cluster. This means that the algorithms handle a number of operations proportional to the number of nodes involved, making them efficient and scalable as the network grows..

Acknowledgements

All the praises and thanks are to Allah, the most gracious and the ever merciful. HE has given me the strength, courage, and patience to carry out this work.

Then, this thesis represents a great deal of time and effort not only on my part but also on the part of my supervisor, Prof. Dr. A.K.M Muzahidul Islam

A big thank you to Prof. Dr. Md. Motaharul Islam, Assistant Prof. Mohammad Mamun Elahi and Prof. Dr. Mohammad Shahriar Rahman for your helpful feedback.

I'm grateful for the support from United International University and, most importantly, to my family and friends for their patience and encouragement.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In recent years, there has been significant advancement in microelectronics which has led to the development of data-hungry devices. This growth is expected to greatly enhance the standard of living, providing convenience and comfort. As a result, it initiated an ever-increasing request for new radio spectrum [1]. The requests being put on the scarce supply of usable radio waves are quickly developing, as the world gets to be progressively reliant on this advancing cluster of administrations [2]. Moreover, the modern technology forces a challenge from the spectrum scarcity problem for developing new technologies and expanding existing ones because this spectrum is a crucial and finite resource, and its scarcity poses real problems [3, 4].

However, existing radio spectrum is allocated by a command-and-control based method which creates remain under-utilized radio spectrum [5]. A concept developed by Joseph Mitola III, cognitive radio networks (CRNs) enable spectrum sharing and efficiently utilize the available bands, specifically the underutilized spectrum [6]. Cognitive radio networks rely on smart algorithms that constantly watch the network's conditions. These algorithms make decisions, take actions, and plan ahead based on what they observe, helping to keep the network running smoothly and efficiently. It is a smart and self-managing communication system that can change how it operates depending on the conditions of the network. This means it can adjust its performance and capabilities to make the most of the available resources and adapt to varying network situations [7, 8].

A CRN is an advanced wireless communication system where the technology, called cognitive radios (CRs), is designed to be highly adaptable and intelligent. These radios are designed to be flexible and intelligent, so they can automatically adjust their settings to improve performance in a dynamic and efficient way. This means the network can make the best use of available frequencies, avoid interference, and adapt to changes in the wireless environment, leading to better overall performance. In CRNs the user community is divided into two main groups: Primary Users (PUs) and Secondary Users (SUs) (see Fig. 1).

PUs have official licenses that grant them exclusive rights to certain frequency bands in the radio spectrum. This means they have priority access to these frequencies and

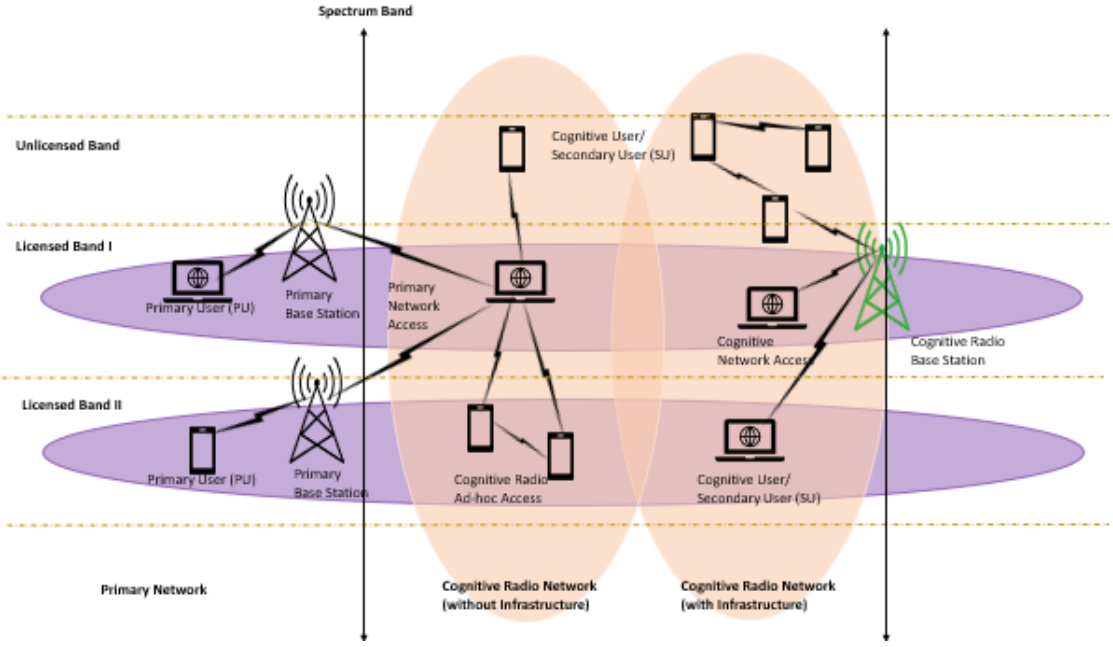


Figure 1.1: Cognitive Radio Network

can operate without interference from other users. Alternatively, SUs do not possess these official licenses and are therefore considered unlicensed users [9]. PUs have the first priority to use specific frequencies, whereas SUs can only access these frequencies opportunistically when PUs are inactive. This opportunistic access mechanism enhances overall spectrum utilization efficiency by making better use of available frequencies and minimizing wasted capacity.

CRNs are generally classified into two main categories based on their infrastructure: *infrastructure-based* and *infrastructure-less* CR networks, the latter also known as CRAHNs. The infrastructure-based CRNs operate under a fixed network architecture where a central controller manages the cognitive radios and their functionalities. The infrastructure typically includes a set of base stations, similar to conventional cellular networks, which facilitate coordination and communication among the CRs [10, 11].

In contrast, CRAHNs are decentralized networks where cognitive radio nodes establish *ad hoc* connections and communicate directly without relying on any fixed infrastructure. These networks are particularly useful in scenarios where pre-existing communication infrastructure is unavailable. Ad hoc networks thus represent a promising technology that enables reliable wireless communication in dynamic and challenging environments.

Among different ad hoc architectures, the clustering approach is widely adopted due to its scalability and efficiency advantages compared to flat network structures [12]. In a flat network, all nodes communicate directly with each other, leading to increased signaling overhead and reduced efficiency as the network size grows. Conversely, cluster-based networks minimize overhead by organizing nodes into clusters, where communication primarily occurs between *cluster heads* and their respective members. Nodes within each cluster

are grouped based on proximity, feature similarity, or specific application requirements. This article presents a Secure spectrum aware cross-layer MAC protocol for CRAHNs. In [13, 14, 15], The Secure Spectrum Aware MAC layer protocols for CRAHNs are designed to address the security challenges that arise in cognitive radio networks. The approach involves maintaining secure cluster formation based on a graph G. A new cluster model is introduced to tackle existing security issues and the maximum edge biclique problem. The *Cluster Head Determining Factor* (CHDF) is an important parameter that considers the number of sensed channels and neighboring nodes to choose the cluster leader or head.

The proposed clustering approach focuses on keeping a larger number of reserved channels within each cluster, which helps reduce the frequency of re-clustering when the availability of spectrum changes. The CHDF value is securely signed, encrypted, and transmitted to neighboring nodes that are announcing themselves as cluster heads. To further reduce re-clustering issues due to node mobility, each cluster includes an auxiliary cluster head that takes control when the current cluster head moves out.

The paper outlines a super-frame structure designed to integrate the proposed secure clustering scheme. This structure also includes two key topology management operations: the *Node-Move-In* and *Node-Move-Out* algorithms. The super-frame structure helps organize and manage the network efficiently by coordinating the secure clustering approach and ensuring smooth adjustments when nodes enter or leave the network.These protocols aim to ensure secure and efficient spectrum sharing among nodes in the network while optimizing network performance.

Therefore, the main contributions of this article are summarized as follows:

- This work introduces a secure, spectrum-aware clustering approach for CRAHNs. This scheme facilitates seamless channel switching by incorporating a set of shared free channels within each cluster and includes a *Secondary Cluster Head* (SCH) to address re-clustering challenges caused by the mobility of the *Cluster Head* (CH) or changes in spectrum availability. During cluster formation, the scheme ensures that transmissions remain confidential and that data integrity and authenticity are maintained.

- To realm the robustness of the proposed Secure Spectrum Aware MAC layer protocols model, a Node Move-In protocol is illustrating the process of a new node joins in cluster Additionally, a Node Move-Out protocol is created to manage the process when an existing node leaves the cluster.

- A pseudocode analysis shown during the cluster formation as well as *Node-Move-In* and *Node-Move-Out*. Overall, both algorithms complexity $\mathcal{O}(n)$ is driven by the linear number of nodes involved in these processes, ensuring efficient scalability with respect to the size of the network.

The remainder of the article is organized into the following sections. A brief overview of the latest MAC protocols developed for CRAHNs is provided in Chapter 2. Then,

in Chapter 3.0.1, a network model of secure spectrum aware MAC layer protocols is discussed. Chapter 3.0.2 covers the maintenance algorithms for the secure cluster-based architecture, detailing how the clustering process concludes in $\mathcal{O}(1)$ iterations, irrespective of the network's topology or size. Finally, in Chapter 3.0.3 and Chapter 3.0.4, two topology management operations, *Node-Move-In* and *Node-Move-Out*, are discussed, where a pseudocode analysis with time complexity $\mathcal{O}(n)$ is presented.

Chapter 2

Background and Literature Review

A Cognitive Radio Wireless Sensor Network consists of sensor nodes, each equipped with a set of sensors, a control processor, and a transceiver communication unit. There is growing interest in self-organizing multi-hop wireless sensor networks, where multiple independent nodes communicate via radio signals without the need for any previously established infrastructure. These nodes/devices frequently encounter constraints in essential resources like power and radio frequency bandwidth. A flat network topology is established when the sensor nodes are physically deployed, and a link exists between nodes if they are within each other's communication range. In such flat network topology where no built-in structure to facilitate efficient commutation, this problem often arises. Clustering is employed to optimize the flat sensor network topology by introducing a hierarchical organization [16-18]. The fundamental approach involves partitioning the network into clusters based on physical proximity, thereby facilitating more efficient management by dividing the network into smaller, more manageable units. Recently, there has been considerable interest in Cognitive radio networks due to their potential to offer solutions in a range of fields including healthcare, the environment, defense, surveillance, industry, and transportation. The primary focuses of the examined networks are understanding spectrum usage and assigning local control channels. A clustering algorithm is suggested in [20] for forming clusters based on factors like available channels, physical placement, and past spectrum usage. However, this algorithm encounters problems of re-clustering when spectrum availability changes or nodes move. In the self-organized CRAHN network in MAC protocol [21] divided network in two user groups a PU and a SU. A significant challenge within this protocol involves the need for regrouping, as groups must be reorganized when a PU emerges. Additionally, the protocol lacks mechanisms for neighbor discovery and group upkeep. An algorithm known as Spectrum Opportunity Clustering (SOC) is introduced in [22],which operates in a distributed manner to establish clusters using shared unused channels. While this approach achieves a favorable trade-off between common channels and cluster size,it is notable that [22] has the potential to generate an extensive quan-

tity of clusters and the issue of re-clustering for mobile nodes is also a limitation in this algorithm.

The clustering technique employed in [23] involves utilizing the Affinity Propagation message-passing approach, potentially resulting in the creation of sizable clusters within the protocol. The presence of a large number of members in a cluster can induce delays in communication within the cluster. Furthermore, this protocol assumes static nodes, which introduces the problem of re-clustering when nodes are in motion. Like the approach in [23], this MAC protocol forms clusters with many members, even though the available shared channels are limited. The re-clustering problem re-emerges when PUs become active. In [24], the MAC protocol outlined is classifies nodes according to their degree, with the degree derived from network statistics and clusters rely on 2-hop communication. Each node in the network necessitates additional processing capacity as it holds comprehensive network data. Furthermore, when a node is in motion, the problem of re-clustering becomes pronounced within the framework. A MAC protocol for CRAHN multi-channel multi-hop neighbor discovery scheme, a distributed Clustering algorithm is presented in [25]. While the clustering technique remains comparatively stable when the spectrum availability changes, the problem of re-clustering becomes significant in scenarios involving node mobility. However, the approach introduces additional delay in intra-cluster communication due to potentially large cluster sizes, and re-clustering is necessary to accommodate node mobility as discussed in [25]. A centralized clustering technique based on identification, outlined in [26] for CRAHN, restores broken connections at a local level, while maintaining the original routes unchanged. The issue of re-clustering is a common challenge in this approach, affecting both scenarios where spectrum availability changes and when nodes are in motion. The protocol detailed in [27] introduces a distributed clustering approach specifically for nodes that are disconnected. This method relies on a combined weight metric that integrates multiple factors: the history of spectrum usage, the physical distance between nodes, the current state of each node, and the effects of interference. By considering these elements together, the protocol aims to create more effective and adaptive clusters even in dynamic and challenging network conditions. A PU is detected because this method doesn't just adapt to changes in spectrum availability during re clustering. Additionally, the clustering mechanism described in [27] does not adequately address node mobility. A structure for establishing a CogMesh network within the framework of an open spectrum sharing scheme is presented in [28]. The MAC protocol forms clusters using a specific localized channel referred to as the master channel. However, changes in control channel assignment could introduce variations in the presence of diverse channel conditions, resulting in network instability. Nevertheless, not every cluster is equipped with the means to handle the re-clustering challenge when nodes are mobile. A clustering algorithm is presented in [29], incorporating parameters such as channel availability, geographical proximity, and historical spectrum utilization. Although the method yields an optimal cluster count, increasing network size amplifies the likelihood of re-clustering, primarily due to the reduction in shared channels per clus-

Table 2.1: Recent Studies on CRSN Clustering Protocols

Ref.	Year	Major Contribution	Advantages	Disadvantages	Method
[1]	1999	Introduced the concept of cognitive radio,enabling dynamic spectrum access.	Groundbreaking idea; adaptable communication.	Early conceptual work; not practically implemented.	Cognitive Radio, SDR
[3]	2008	Surveyed spectrum management in cognitive radio networks.	Comprehensive overview of CRN architecture.	Mostly theoretical; lacks implementation.	Spectrum Management, CRNs
[4]	2015	Proposed full-duplex CR design for better spectrum usage.	Doubles spectral efficiency.	Requires advanced signal processing.	Full-Duplex CR
[7]	2015	Reviewed CR ad hoc network architectures.	Identified architectures and challenges.	Lacked practical frameworks.	CRN Architecture Survey
[8]	2017	Surveyed MAC protocols in CR ad hoc networks.	Outlined MAC challenges and solutions.	No unified MAC protocol.	MAC Layer, CRNs
[12]	2016	Survey on node clustering in CR wireless sensor networks.	Discusses design aspects of clustering.	No experimental validation.	Clustering, CR-WSNs
[13]	2014	Proposed stable cluster-based architecture for CR ad hoc networks.	Enhances stability in clustering.	Affected by node mobility.	Cluster-based Architecture
[14]	2016	Designed on-demand routing for clustered CR ad hoc networks.	Improves route discovery and response.	Complex in dense networks.	On-Demand Routing
[15]	2018	Introduced a cross-layer MAC protocol with spectrum awareness.	Better spectrum use and lower collision.	Overhead in protocol integration.	Cross-layer MAC, Spectrum Awareness
[20]	2013	Designed cluster-based MAC protocol for CR ad hoc networks.	Optimized resource access in clusters.	Delay due to cluster size.	MAC, Cluster-based
[23]	2011	Message-passing based clustering for CRNs.	Adaptive to dynamic environments.	Message overhead in large networks.	Distributed Clustering
[24]	2010	Cluster-based distributed topology management.	Enhanced topology control.	Delay from frequent re-clustering.	Topology Management
[25]	2010	Protocol for cluster formation in CR ad hoc networks.	Reduces overhead.	Fails in high-mobility networks.	Cluster Formation
[30]	2021	Developed an energy-efficient clustering protocol for CRSNs.	Extends lifetime and enhances throughput.	Less suitable in high-dynamics.	Energy-aware Clustering
[31]	2021	Proposed localized clustering for CRNs.	Lower communication overhead.	Sensitive to mobility.	Localized Clustering
[32]	2021	Secure clustering using evolutionary game theory and fuzzy logic.	Trust-based robust clustering.	High computational cost.	Evolutionary Game, Fuzzy Logic
[33]	2023	Multi-hop clustering routing protocol with imperfect spectrum sensing.	Enhances spectrum usage and routing efficiency.	Less effective under mobility.	Spectrum Sensing, Multi-hop Routing
[34]	2021	SACR protocol for stable cluster-based routing.	Increases network stability and lifetime.	Cluster head selection delays.	Stability-Aware Clustering
[35]	2013	GSM: Gateway selection using bipartite graphs and edge biclique maximization for CRN cluster coordination.	Improves inter-cluster communication; optimal channel sharing.	May face computation complexity with large graphs.	Bipartite Graphs, Edge Biclique, Gateway Coordination

ter.A clustering approach that considers spectrum usage is introduced for CRAHNs in [15]. In this strategy, each cluster is equipped with a set of accessible shared channels that enable smooth switching between different channels. Additionally, each cluster includes a SCH to manage re-clustering challenges that arise from the movement of CHs or changes in spectrum availability. In [30], network stability-aware clustering techniques are discussed, and an improved approach is proposed that takes into account residual energy and the quality of available common channels. This enhancement aims to increase the overall network performance and energy efficiency in cognitive radio sensor networks (CRSNs). In [31], an analytical framework for parameter tuning and performance analysis of clustering protocols is provided. The study proposes a localized clustering scheme to improve stability, scalability, and spectrum management while reducing communication overhead, comparing its performance with existing protocols. In [32], an evolutionary game-based secure clustering protocol for wireless sensor networks (WSNs) is introduced. The protocol incorporates fuzzy trust evaluation and outlier detection, enhancing network security and reliability by assessing the trust levels among nodes and identifying abnormal behaviors, which is crucial for dynamic WSN environments. In [33] proposes a multi-hop clustering routing protocol for *cognitive radio sensor networks* (CRSNs), which makes use of imperfect spectrum sensing. This method improves performance by considering the impact of imperfect spectrum sensing on multi-hop communications, thereby contributing to the robustness and scalability of CRSNs. In, [34] introduces the SACR *(Stability-Aware Cluster-Based Routing)* protocol, designed to enhance the stability and efficiency of cluster-based routing in CRSNs. This protocol adapts to changing network conditions by focusing on stability awareness, which helps to extend network lifetime and improve the reliability of data transmission within cognitive radio sensor networks. In their [35] paper, Zhang et al. introduce a Gateway Selection Mechanism (GSM) aimed at improving inter-cluster coordination in CRAHNs. These networks rely on SUs opportunistically accessing underutilized spectrum, which poses significant challenges for maintaining stable, efficient communication—especially when nodes are grouped into clusters. To address this, the authors propose modeling the relationships between secondary users and idle channels as a bipartite graph, where one set of nodes represents the users and the other set represents the channels. An edge is drawn between a user and a channel if that channel is available for use by the user. This modeling technique allows for a clear visualization of spectrum compatibility among users. From Figure 2.1 this bipartite graph, the framework extracts maximum edge bicliques subgraphs in which every user is connected to every channel in a subset. These bicliques represent optimal groupings of users who can all access the same set of channels, making them ideal for forming robust and spectrum-compatible clusters. Once clusters are formed based on these bicliques, GSM then selects gateway nodes from users who share idle channels across neighboring clusters, ensuring seamless inter-cluster communication. This approach not only improves coordination and reduces control overhead but also enhances throughput and reliability in dynamic radio environments.The literature indicates that newly developed MAC protocols address several crucial consid-

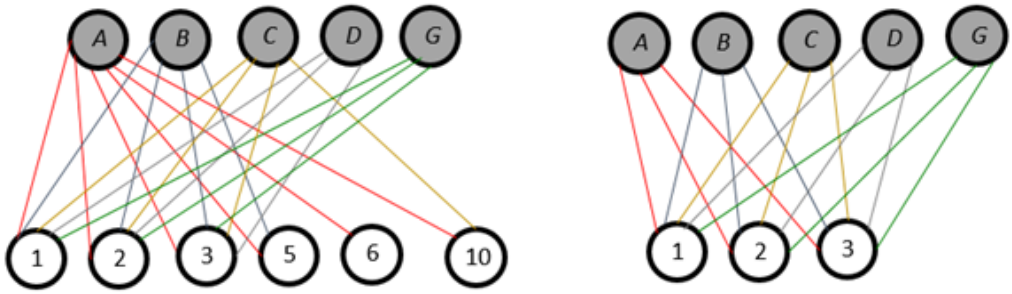


Figure 2.1: Bipartite graph formed by node a and its maximum-edge biclique subgraph.

erations essential for the practical advancement of CRAHNs. A resilient, cluster-oriented MAC protocol for CRAHNs is introduced, integrating secure spectrum awareness and node mobility considerations. To mitigate the shortcomings of prior approaches, a secure, spectrum-aware cross-layer MAC framework is proposed, the details of which are outlined in the subsequent section

2.0.1 Cluster based architecture

This section describes the self-organized, cluster-based architecture for an ad-hoc network. A cluster in graph G is a star-shaped subgraph where one node, the *cluster head*, is connected to all other nodes, known as *cluster members*, but no connections exist between the members themselves. Clustering divides the graph into disjoint groups of nodes.The self-organized cluster-based connected graph is represented as $G = (V, E)$, where V represents the nodes and E represents the edges between cluster heads and their members.Nodes u and v are connected by an edge if they are located within mutual transmission range.

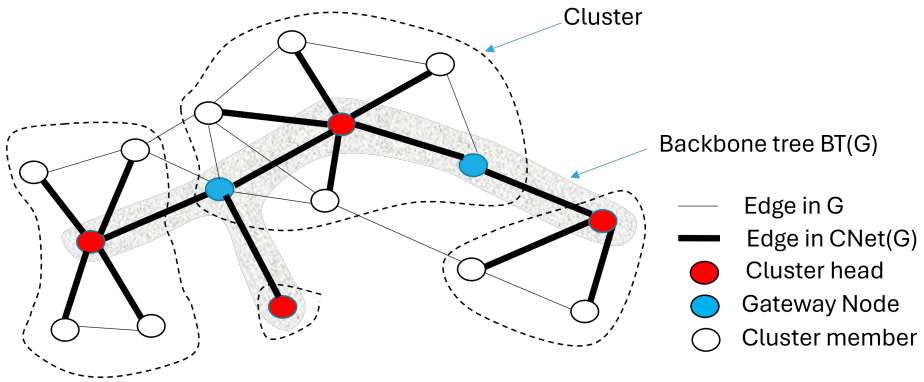


Figure 2.2: Cluster base network CNet (G).

To minimize the number of clusters, the clustering ensures that no two cluster heads are adjacent, forming a maximal independent set. Cluster heads are connected by a special node called a *gateway*, which serves as a link between the neighbors of two cluster heads. This clustering transforms a flat graph into a hierarchical structure.

The backbone of G consists only of cluster heads and gateway nodes, with a gateway

node connecting two or more cluster heads. Since cluster heads cannot be neighbors, any backbone edge must connect a cluster head to a gateway node. As G is a connected bidirectional graph, a backbone will always exist.

2.0.2 Network Model

Below is the ad hoc self-organized network model:

- The network consists of SU equipped with cognitive radios, making use of the available spectrum for their communication needs.
- Each cognitive radio node is equipped with two transceivers: one for handling control signals and the other for managing data signals.
- The traffic of PUs on a specific channel is represented by a semi-Markov ON–OFF process, where the channel can be in one of two states: busy (ON) or idle (OFF).
- The network is independent of any spectrum sensing model.
- All cognitive radios possess an identical transmission range.
- A link exists iff two cognitive radios are within mutual communication range and share a common channel.
- The network is equipped with Carrier Sense Multiple Access with Collision Avoidance.
- Individually cognitive radio autonomously detects available spectrum.

Chapter 3

Methodology

3.0.1 Proposed Cluster Model

In this section, we delve into the proposed secure cluster-based architecture that utilizes super-frame MAC layer protocols for its implementation. This clustering scheme operates in a distributed manner, with each cluster organizing its channel access through a carefully synchronized sequence of super frames. The super-frame structure is divided into four key periods: the beacon period, spectrum sensing period, neighbor discovery period, and contention-free data period. For secure cluster formation the Cluster Head initiates beacon message in bacon period which contain ID, Auxiliary Security Header and synchronization information and the sensing band assigned to the cluster.

Beacon Period During this phase, the CH sends out a beacon message with a super-frame preamble and control header. By using the *Distributed Coordination Function* (DCF), the CH checks the channel status before transmitting and identifies whether the channel is busy or available. If the channel is busy, the CH waits for the current transmission to end. After that, it waits a short additional period—equal to a *DIFS* interval—before randomly picking a back-off period to try again.This beacon message is crucial as it contains the cluster ID, time synchronization information, the ID of the *Secondary Cluster Head* (SCH), an *Auxiliary Security Header*, and data related to control and resource allocation within the cluster, as illustrated in Figure 4. This period ensures that all nodes within the cluster are synchronized and aware of the cluster's configuration.

The *Cluster ID* field in the super-frame holds the unique identifier for the cluster, while time synchronization assists in determining the nodes' locations, proximity, or speed. After the calculation of the CHDF value, it is shared with neighboring nodes along with appropriate security measures.Regarding security, the process initiates with the generation of a digital signature for the calculated CHDF value. This signature, generated using the node's private key, ensures the authenticity and integrity of the CHDF data in the *Auxiliary Security Header*. The SCH ID is included to notify all cluster members.Common channels chosen by the CH are part of every cluster, with a *Channel-hopping Sequence* (CS) generated for access. If a PU appears during transmission, the CH switches to the

<table>
<tr><td>Beacon</td><td>Spectrum Band for sensing</td><td>Channel hopping sequence(CS)</td><td>SCH ID</td><td>Time synchronization</td><td>Cluster ID</td><td>Super frame preamble and control header</td><td>Auxiliary Security Header</td></tr>
<tr><td>Spectrum sensing</td><td>CM 1 Sensing</td><td>CM 1 Sensing</td><td>……..</td><td>……..</td><td>……..</td><td>……..</td><td>CH Sensing</td></tr>
<tr><td>Neighbour Discovery</td><td>CM 1</td><td>CM 2</td><td>……..</td><td>……..</td><td>……..</td><td>……..</td><td>CH</td></tr>
<tr><td rowspan="11">Contention Free Period</td><td rowspan="5">Intra-Cluster Communication</td><td colspan="6">Mini Slot 1</td></tr>
<tr><td colspan="6">Mini Slot 2</td></tr>
<tr><td colspan="6">……..</td></tr>
<tr><td colspan="6">Mini Slot n</td></tr>
<tr><td colspan="6">Reserved</td></tr>
<tr><td rowspan="5">Inter-Cluster Communication</td><td colspan="6">Mini Slot 1</td></tr>
<tr><td colspan="6">Mini Slot 2</td></tr>
<tr><td colspan="6">……..</td></tr>
<tr><td colspan="6">Mini Slot n</td></tr>
<tr><td colspan="6">Reserved</td></tr>
</table>

Figure 3.1: Proposed Secure MAC super frame Structure.

next channel in the CS to avoid interference. This routine action safeguards against PU interference, and the super-frame includes the spectrum band for sensing.

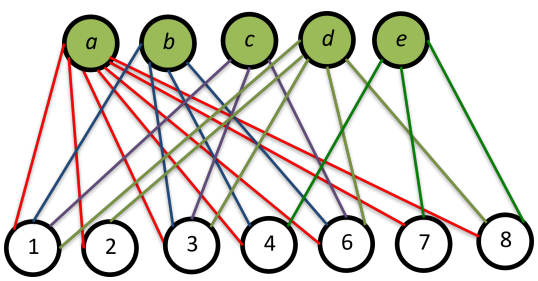
Spectrum Sensing Period During this period, nodes within the cluster perform spectrum sensing to detect available channels and assess the current spectrum conditions. They update their *Access Control Lists* (ACLs) based on the sensed information. Synchronized sensing reduces false alarms.If a node detects a PU, it switches to the next channel and informs the CH. The CH adjusts its beacon accordingly, and other nodes follow suit if they do not receive the beacon within a set time. This information is critical for making informed decisions about channel usage and ensuring that the network operates efficiently.

Contention Free Period The proposed super-frame has a contention-free data period where CRs can send their packets during designated time slots. Within clusters, any available channel can be used for data transmission. Each node in the cluster is assigned a mini-slot by the CH for sending data, with additional slots set aside for forthcoming use.The contention-free period is divided into intra-cluster and inter-cluster communication phases. During the intra-cluster phase, nodes transmit within the cluster using their assigned mini-slots, taking into account the departure of the CH, *Forwarding Node* (FN), and *Cluster Members* (CM). When a CH or FN leaves, they inform the cluster and, if needed, appoint a successor for seamless connectivity. Leaving nodes' mini-slots are removed from communication periods. If a CM moves, it informs the CH, and the assigned mini-slot is removed. The CH notifies neighboring CHs of an approaching node, which is initially treated as a member. This ensures mobile node connectivity.Inter-cluster communication involves packet transmission between neighboring clusters, with the CH using the FN as a relay for inter-CH communication.

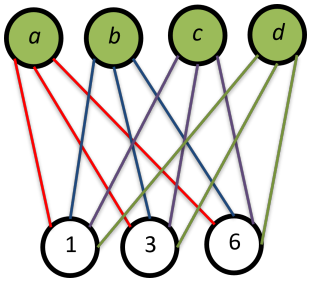
Neighbor Discovery To join a network, a CR identifies nearby nodes and exchanges control information by sequentially hopping between channels. During this neighbor discovery process, the CR relies on a global common control channel for time synchronization

and spends a specific amount of time on each channel to ensure sufficient identification of neighboring nodes. The CR node sends a *HELLO* message to the *Cluster Head* (CH) after receiving a beacon and awaits a *RESPONSE* from neighboring CHs. A timer is activated during HELLO transmission, prompting retransmission in case of expiration, ensuring reliable data delivery during the neighbor discovery phase.Successful reception of a beacon and REPLY initiates the node joining process, while the absence of these triggers the cluster formation process. Cluster formation optimizes clusters based on spectrum availability, striving to minimize the number of clusters while maximizing common channels. This involves constructing bipartite graphs and maximizing edge biclique graphs for each node.

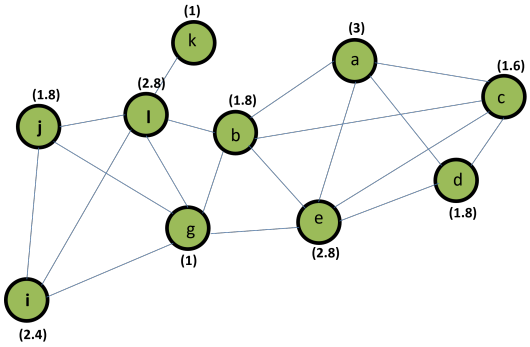
3.0.2 Cluster formation Algorithm



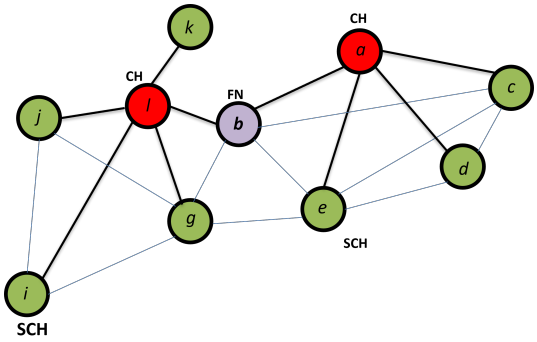
(a) Bipartite graph constructed by node CRa



(b) Maximum edge biclique graph of node CRa



(c) Nodes with CHDF value



(d) Proposed cluster-based network

Figure 3.2: (a) Bipartite graph constructed by node CRa, (b) Maximum edge biclique graph of node CRa, (c) Nodes with CHDF value, (d) Proposed cluster-based network.

Using spectrum availability, a new clustering method sorts the network into logical groups. Nodes detect their nearby neighbors, compile lists of these neighbors, and exchange access information with them. The aim is fewer clusters, emphasizing clusters sharing the most channels. Clusters are formed using Algorithm 3.1, as outlined in Table 3.1, with the goal of creating the largest clusters with common channels.

Each CR_i first constructs an undirected bipartite graph $G_i(A_i, B_i, E_i)$ using its neighbor list N_i and *Access Control List* (ACL) C_i, where i ranges from 1 to n. A graph

Table 3.1: Symbol used in cluster information

Symbol	**Instruction / Description**
i, j, k, l, x, y, N	Positive integers (e.g., 1, 2, 3...)
CR_i	Any positive node
CR_j	New joining node
CR_k	Departure node
CR_N	Any neighbor of CR_i
CH_i	Neighboring cluster heads of CR_i
FN_i	Neighboring forward nodes of CR_i
CM_i	Cluster member of CH_i
ACL_x	Accessible list of CR_i
N_i	Neighbor list of CR_i
Gp_x	Bipartite graph of CR_i
Gc_x	Maximum edge biclique graph of CR_x
$CHDF_i$	Cluster head decision factor value of CR_i
ID_i	Identifier (ID) of CR_i

$G(V, E)$ is classified as bipartite if its vertices can be divided into two separate sets, A and B, where every edge links a vertex in set A to a vertex in set B. For a node CR_i, A_i is the part of CR_i's neighbor list N_i, and B_i is CR_i's ACL, C_i. An edge (x, y) connects vertices x from A_i and y from B_i if y is included in CR_i's ACL, meaning channel y is within CR_i's access list. Figure 4(a) shows a bipartite graph $G_i(A_i, B_i, E_i)$ generated by CR_a. In this graph, A_a contains the 1-hop neighbors $N_a = \{b, c, d, e, a\}$, while B_a includes CR_a's accessible channels list $C_a = \{1, 2, 3, 4, 6, 7, 8\}$. Vertex a in A_a is connected to all vertices in B_a because B_a matches C_a.The maximum edge biclique graph for a node is determined from its corresponding bipartite graph. Figure 3.2(b) presents the maximum edge biclique graph for CR_a, which is derived from the bipartite graph of node a. In this graph, CR_a's maximum edge biclique is formed with neighboring CR_b, CR_c, and CR_d, all of which share channels $\{1, 3, 6\}$. Each node in the network independently constructs its own maximum edge biclique graph. Constructing these graphs involves processing each node and edge. The graph construction time complexity is $\mathcal{O}(n + e)$, where e is the number of edges. Assuming e is proportional to n, the graph construction time complexity becomes $\mathcal{O}(n)$. The clustering scheme in the secure protocol aims to use as many unused channels as possible for communication within clusters while minimizing the total number of clusters. To achieve this, the CHDF is introduced. The CHDF considers two key factors: the number of neighboring nodes and the common channels shared, based on the maximum edge biclique graph. Each cognitive node calculates the CHDF using Equation 3.1 to help reach this objective.

In Equation 3.1, C_i represents the number of free channels a node has, while N_i counts the number of neighboring nodes, both taken from the node's maximum edge biclique graph. The CHDF calculation values shared idle channels more than neighboring

nodes.As it involves processing each node and edge, the CHDF computation has a time complexity of $\mathcal{O}(n)$. This focus on idle channels boosts communication strength within clusters, allowing nodes to switch channels more easily and reducing the need to frequently reorganize clusters when spectrum availability changes.Equation 3.1 uses a square root to adjust the CHDF value:

$$CHDF_i = \sqrt[c_i]{c_i^{N^i}} = \left(c_i^{N^i}\right)^{\frac{1}{c_i}} = c_i^{\frac{N^i}{c_i}} \tag{3.1}$$

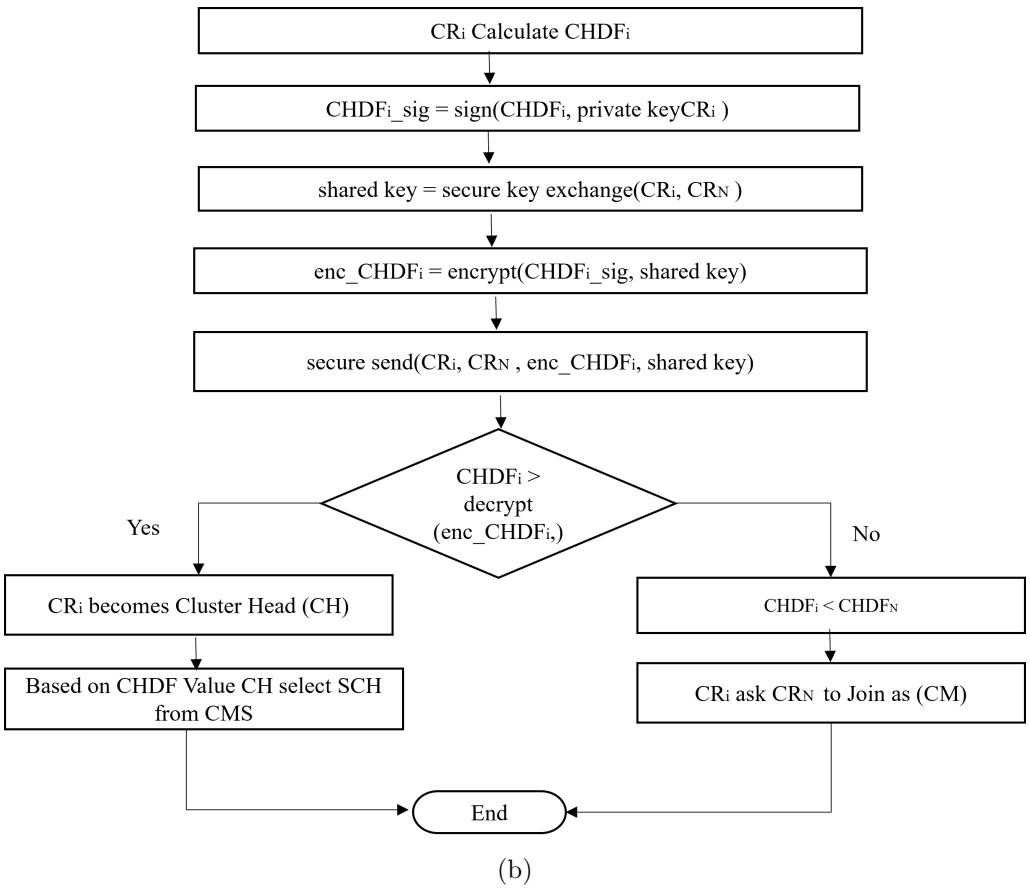
Each cognitive node within the network computes its CHDF value autonomously (illustrated in Figure 3.2(c)) and shares this computed value with its immediate neighboring nodes using appropriate security measures (illustrated in Figure 3.3).Regarding security, the process initiates with the generation of a digital signature for the calculated CHDF value. This signature, generated using the node's private key, ensures the authenticity and integrity of the CHDF data.

Next, the implementation of a *Secure Key Exchange Protocol* facilitates the establishment of a shared key between the (CR_i) and (CR_N). This shared key, generated through a secure exchange mechanism, ensures secure and confidential communication between the node and its 1-hop neighbors.

Algorithm 3.1: Secure Cluster Formation

1: START
2: CR_i begins sensing and creates ACL_i
3: CR_i transmits ACL_i and N_i to CR_N
4: CR_i constructs bipartite graph G_{pi} and biclique graph G_{ci}
5: CR_i computes $CHDF_i$
6: $CHDFi\_sig \leftarrow \text{sign}(CHDF_i, private\_key_{CR_i})$
7: $shared\_key \leftarrow \text{secure\_key\_exchange}(CR_i, CR_N)$
8: $enc\_CHDFi \leftarrow \text{encrypt}(CHDFi\_sig, shared\_key)$
9: $\text{secure\_send}(CR_i, CR_N, enc\_CHDFi, shared\_key)$
10: **if** $CHDF_i > decrypt(enc\_CHDFi, shared\_key, public\_key_{CR_i})$ **then**
    CR_i becomes Cluster Head (CH)
    CR_i selects SCH based on CHDF of CM nodes
11: **else if** $CHDF_i < decrypt(enc\_CHDFN, shared\_key)$ **then**
    if $|N| > 1$ **then**
        if $|CHDF_{highest}| > 1$ **then**
            CR_i requests to join CR_N with smallest ID among top CHDF
        else
            CR_i joins CR_N with highest CHDF_N
    else
        CR_i requests to join CR_N as CM
12: **if** $ID_i < ID_N$ **then**
    CR_i becomes CH and forms the cluster
13: **else**
    CR_i joins CR_N as CM where ID_N is smallest
14: END

(a)



(b)

Figure 3.3: (a) and (b) Security measures during CHDF value transfer to neighbor nodes.

Subsequently, the securely encrypted CHDF value and its corresponding digital signature are transmitted to one-hop neighbor nodes using a secure transmission mechanism. This mechanism utilizes an established shared key to ensure confidentiality and prevent unauthorized access, interruption, or modification of the data during transit.

To maintain authenticity and integrity, each CHDF signature is verified by the receiving cognitive node using the sender's public key. Successful verification confirms that the CHDF value originates from the claimed node (CR_i) and has not been tampered with.The process ensures secure and trustworthy exchange of CHDF values between nodes and their one-hop neighbors. Communication typically requires $\mathcal{O}(n)$ time, where n is the number of nodes. Broadcasting CHDF values may involve sending messages to multiple neighbors in $\mathcal{O}(1)$ rounds, while cryptographic operations such as digital signature generation, encryption, and verification contribute an additional complexity of $\mathcal{O}(k)$, where k is the size of the data. Specifically:

- The CHDF_i value is encrypted using the shared key before transmission.
- A digital signature is generated using the private key of CR_i ($private\_key_{CR_i}$) to ensure authenticity.
- Upon receipt, CR_N verifies the signature using $public\_key_{CR_i}$.

Once verified, CHDF values are used for clustering decisions. The node with the highest CHDF among its neighbors is selected as the Cluster Head (CH). If CR_i has a lower CHDF than its neighbors, it joins the cluster of the node with the highest CHDF as a Cluster Member (CM).

Cluster formation completes in $\mathcal{O}(n)$ rounds due to graph construction and CHDF computation. Secure message handling occurs in $\mathcal{O}(1)$ time per operation. The combined cryptographic overhead, including decryption and signature verification, adds $\mathcal{O}(k)$ complexity.Following cluster formation:

- The CH manages channel assignments and intra-cluster communication.
- Communication follows a *star topology*—all messages are routed via the CH; CMs do not directly communicate with each other.
- A SCH is selected from among CMs based on the highest CHDF. The SCH ensures stability and takes over when the CH leaves the cluster.
- The CH may assign FNs to enhance inter-cluster communication, based on CHDF values and connectivity.

This hierarchical structure is illustrated in Figure 3.2(d), where CHs, SCHs, and CMs are shown in a structured cluster-based topology. Overall, the proposed secure cluster formation algorithm has a dominant time complexity of $\mathcal{O}(n)$, influenced by node-level operations like graph construction and CHDF computation, with additional cryptographic

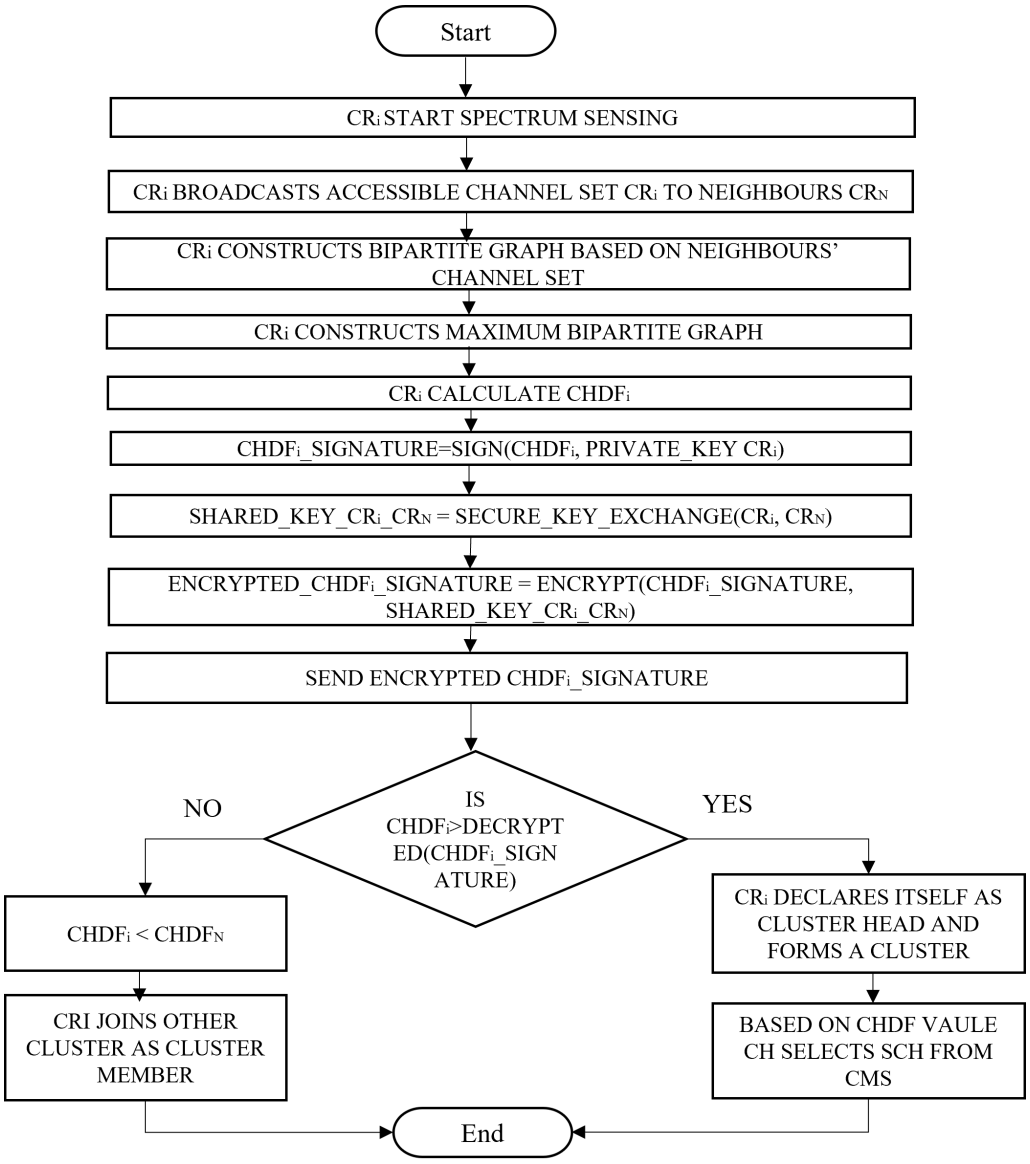


Figure 3.4: Secure propose cluster formation.

operations contributing $\mathcal{O}(k)$.However, in dynamic network environments where nodes can freely join or leave clusters, specialized protocols are required to maintain the stability of the cluster structure. These protocols are discussed in detail in the following section.

3.0.3 Node Move-In Algorithm

This protocol explains how a node can join a cluster if it is not already a member. The process begins when the node detects a beacon from a nearby Cluster Head (CH), allowing it to either join an existing cluster or establish a new one. Algorithm 2 illustrates this process using definitions from Table 2.When a node, referred to as CR_j, wants to join, it starts by identifying available channels and establishing its Access Control List (ACL). It then scans channels sequentially in $\mathcal{O}(s)$ rounds, where s is the number of spectrum channels to sense, in order to detect beacons from neighboring clusters. This sensing period is designed to be longer than the longest super-frame. In the received beacon, CR_j identifies potential neighbor list CR_N and broadcasts its neighbor and channel lists. Neighboring nodes (CR_N) reciprocate by broadcasting their ACLs, which operates in $\mathcal{O}(n)$ time, where n is the number of nodes.After receiving the broadcast messages from its neighbors, CR_j constructs two graphs: the bipartite graph

G_{pj} and the maximum edge biclique graph G_{cj}.Using this information, CR_j calculates its CHDF, as previously discussed.Since the CHDF is computed individually from each neighbor's information, the time complexity remains $\mathcal{O}(n)$.Once the CHDF value is calculated (via Equation 3.1), it is encrypted using a shared key, $shared\_key_{CR_j\text{-}CR_N}$, to ensure its privacy and security. Following encryption, CR_j shares the encrypted CHDF value with its neighboring nodes (CR_N) via broadcasting.Initially, CR_j checks for the presence of any Cluster Head in its vicinity and takes steps to join the cluster by sending an encrypted acceptance message. If CR_N includes multiple CHs, CR_j selects the CH with the highest CHDF value. This selection and communication are performed securely via encrypted messages, which are constant-time operations $\mathcal{O}(1)$.In cases where multiple neighboring CHs have identical highest CHDF values, CR_j chooses the CH with the smallest ID. This ensures deterministic tie-breaking and supports secure and stable cluster formation. Afterward, CR_j compares its CHDF_j with the CHDF value of the chosen Cluster Head (CH). If the selected CH has a higher CHDF, CR_j seeks to join the cluster as a CM. In this case, CR_j sends a join request to the CH. To be accepted into the cluster, CR_j must share a set of channels with the CH, with at least two of them being common. The number of common channels ($|n|$) must be greater than 2^n and included in the CH's ACL for CR_j to be accepted. This condition ensures a backup communication channel, improving cluster stability.If CR_j does not meet the required number of shared channels or if there are no reserved mini-slots available in the super-frame, the CH may reject the join request. Upon acceptance, the CH assigns CR_j a mini-slot from the reserved set and sets up its communication schedule within the cluster. CR_j may take the role of a FN if it provides better connectivity than existing FNs, as determined by its CHDF value. If the request

Algorithm 3.2: Cluster Join and CH Selection Process

1 **1:** START
2 **2:** CR_i begins the sensing process
3 **3:** CR_j creates ACL_j
4 **4:** CR_j creates CR_N
5 **5:** CR_j forms ACL_j and CR_N
6 **6:** CR_j forms G_{pj}
7 **7:** CR_j forms G_{cj} based on G_{pj}
8 **8:** CR_j computes $CHDF_j$
9 **9:** $encrypted\_CHDF_j \leftarrow encrypt(CHDF_j, shared\_key_{CR_j,CR_N})$
10 **10:** CR_j shares $encrypted\_CHDF_j$ with CR_N
11 **11: if** $CR_j \in CR_N$ **then**
12 **12: if** $j > 1$ **then**
13 **13: if** $|ACL_j \cap ACL_{CH}| > 2^n$ *and mini-slot is available* **then**
14 **14:** CR_j joins CH_j as CM
15 **15:** $encrypted\_acceptance \leftarrow encrypt(\text{"}ACCEPTED\text{"}, shared\_key_{CR_j,CH_j})$
16 **16:** CR_j sends $encrypted\_acceptance$ to CH_j
17 **17:** $decrypted\_acceptance \leftarrow$ $decrypt(encrypted\_acceptance, shared\_key_{CR_j,CH_j})$
18 **18: if** $decrypted\_acceptance == \text{"}ACCEPTED\text{"}$ **then**
19 **19:** CR_j forms new cluster and becomes CH
20 **21: else if** $CHDF_j > CHDF_{CH}$ **then**
21 **22: if** $CR_N == CH_N$ **then**
22 **23:** $encrypted\_become\_CH \leftarrow$ $encrypt(\text{"}BECOME\_CH\text{"}, shared\_key_{CR_j,CH_j})$
23 **24:** CR_j sends $encrypted\_become\_CH$ to CH_j
24 **25:** $decrypted\_become\_CH \leftarrow decrypt(encrypted\_become\_CH,$
25 $\text{shared\_key}_{CR_j,CH_j})$
26 **26: if** $decrypted\_become\_CH == \text{"}BECOME\_CH\text{"}$ **then**
27 **27:** CR_j becomes new CH
28 **28:** CH_j becomes SCH
29 **29: else if** $CH_N \subset CR_N$ **then**
30 **30:** CR_j calculates new CHDF for $CR_N^{new} = CH_N$
31 **31:** $encrypted\_new\_CHDF \leftarrow encrypt(CHDF_j^{new}, shared\_key_{CR_j,CR_N^{new}})$
32 **32:** CR_j sends $encrypted\_new\_CHDF$ to CRN^{new}
33 **33:** $decrypted\_new\_CHDF \leftarrow$ $decrypt(encrypted\_new\_CHDF, shared\_key_{CR_j,CR_N^{new}})$
34 **34: if** $decrypted\_new\_CHDF > CHDF_{CH}$ **then**
35 **35:** go to step 15
36 **36:** go to step 15
37 **37: else**
38 go to step 15
39 **38: else if** $FN_j \in CR_N$ **then**
40 **39: if** $j > 1$ **then**
41 **40:** Choose FN_j with highest CHDF
42 **41:** CR_j establishes a new cluster and becomes CH
43 **42: else**
44 **43:** CR_j establishes a new cluster and becomes CH
45 **44: else**
46 **45:** CR_j establishes a new cluster and becomes CH
47 **46:** CR_j selects CM with highest CHDF as SCH
48 **47:** END

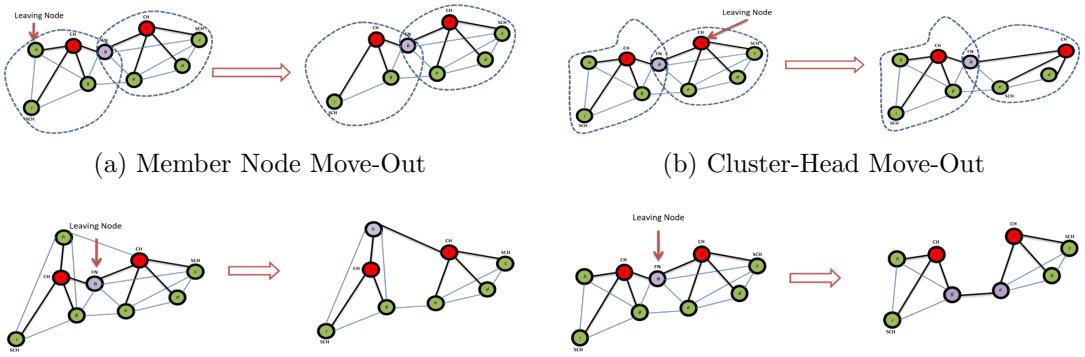
is rejected, CR_j will attempt to join another cluster in accordance with Algorithm 3.2. In the event that CR_j's CHDF value is higher than that of the current CH, it then compares its neighbor set, CR_N, with the neighboring nodes of the CH, denoted as Cluster Members (CH_N). If the two sets are identical ($CR_N = CH_N$), CR_j assumes the role of the new CH, and the former CH becomes the Secondary Cluster Head (SCH). If $CH_N \subset CR_N$, indicating that the CM set is a subset of CR_j's neighbors, CR_j recalculates its CHDF using an updated neighbor set $CR_N^{new} = CR_N$.With the new CHDF value, CR_j securely compares $CHDF_j^{new}$ with $CHDF_{CH}$ by sending an encrypted message. If $CHDF_j^{new} > CHDF_{CH}$, CR_j becomes the new CH, while the previous CH transitions to the SCH role. However, if $CH_N \not\subset CR_N$, CR_j remains in the cluster as a CM. Should CR_j offer better inter-cluster connectivity than the existing FN, it assumes the FN role.If CR_j fails to discover or join an existing cluster, it may declare itself a CH and initiate a new cluster. The overall time complexity of the algorithm remains linear that is , $\mathcal{O}(n)$.

3.0.4 Node Move-Out Algorithm

When the beacon signal weakens and there is no indication that the CH has moved, the CM or FN infers that it is the one drifting away and initiates the departure process.If a special node, denoted as CR_k, begins to leave, it first sends a departure message to its neighbors and checks its adjacent node list, referred to as the neighbor list. If the departing node is an FN, CR_k may discover one CH and several FNs in its neighbor list. Throughout the departure process, CR_k ensures secure communication by employing encryption, key exchange, and digital signatures to preserve message integrity and authenticity. CR_k is a special node directly connected to multiple CHs. It notifies its primary cluster head, CH_k, about the planned departure. If CH_k detects any node from a nearby cluster CH_N, it selects that node to become the new FN to maintain the inter-cluster link.If there are many nodes from the same cluster in the nearby area CH_N, it picks the one with the strongest connection quality. The selected node informs CH_k about the key exchange plan. Upon approval, it assumes the FN role and connects the two clusters. CH_k also allocates a dedicated time slot for the new FN to handle inter-cluster communication. If the main cluster head (CH_k) cannot directly connect with a nearby cluster, it delegates one of its cluster members (CM_k) to check for nearby clusters. If there are multiple options ($l > 1$), the member CM_l with the highest CHDF value is selected. Two cases are then possible: if the neighbor of CM_l is a main CH, CM_l becomes the main connecting node FN and links the two clusters. Otherwise, if the neighbor is another CM, further steps are required.When both the main leader ($CH_k \in CR_N$) and the forwarding node ($FN_k \in CR_N$) are in the neighbor list of the departing node CR_k (where $k = 1$), CR_k is a forwarding node connected to one CH and one or more FNs. In this scenario, the leaving FN notifies both the main CH_k and forwarding node FN_k of its departure. If CH_k finds a regular node CM from a nearby cluster in its neighbor list, it assigns that CM to become the new FN and maintain the link. The selected CM then requests approval from its CH, and upon

Algorithm 3.3: Secure Cluster Move-Out Procedure

1: START
2: CR_k generates a session key for secure communication with neighboring nodes
3: CR_k broadcasts `SECURE_LEAVE_MESSAGE` to CR_N
4: if $CH_k \in CR_N$ **then**
  5: if $k > 1$ **then**
    6: CR_k notifies CH_k about its departure
    7: while CH_k *active* **do**
      8: if $(CM_l \in CH_k) \wedge (CM_l \notin CH_N)$ **then**
        9: if $l > 1$ **then**
          10: Select CM_l with highest CHDF
          11: $shared\_key_{CR_k,CM_l} \leftarrow secure\_key\_exchange(CR_k, CM_l)$
          12: $encryptedMessage \leftarrow EncryptMessage(message, shared\_key_{CR_k,CM_l})$
          13: $signature \leftarrow SignMessage(encryptedMessage, CR_k^{priv})$
          14: CH_k requests CM_l to be FN
          15: CM_l forwards the request to CH_l
          16: $shared\_key_{CM_l,CH_l} \leftarrow secure\_key\_exchange(CM_l, CH_l)$
          17: CM_l becomes FN
        18: else
          goto step 14
      19: else
        CH_k sends a message to CM_k for other clusters in CM_N
        20: if $CH_l \in CM_N$ **then**
          CM_k forwards request to CH_l
          $shared\_key_{CM_k,CH_l} \leftarrow secure\_key\_exchange(CM_k, CH_l)$
          CM_k becomes FN
        21: else if $CM_l \in CM_N$ **then**
          CM_l forwards request to CH_l
          $shared\_key_{CM_l,CH_l} \leftarrow secure\_key\_exchange(CM_l, CH_l)$
          CM_k becomes FN
          CM_l becomes FN
          continue
  22: else
    if $FN_k < CR_N$ **then**
      goto step 7
    else
      if CR_k *is SCH* **then**
        Select new SCH from CM
        $shared\_key_{CR_k,newSCH} \leftarrow secure\_key\_exchange(CR_k, newSCH)$
      else
        CR_k leaves the cluster
23: else
  CR_k informs all CM and updates cryptographic keys for secure communication within the cluster
  SCH becomes CH
  Select new SCH based on CHDF from CMs
  $shared\_key_{SCH,newSCH} \leftarrow secure\_key\_exchange(SCH, newSCH)$
24: END



(a) Member Node Move-Out (b) Cluster-Head Move-Out

(c) Forwarding Node Move-Out (Case 1) (d) Forwarding Node Move-Out (Case 2)

Figure 3.5: Node Move-out Protocol: (a) Member Node Move-Out, (b) Cluster-Head Move-Out, (c) and (d) Forwarding Node Move-Out.

approval, assumes the FN role. CH_k also allocates a small time slot for the new FN to enable inter-cluster communication.

If CH_k cannot connect directly to the neighboring cluster, it instructs its regular node CM_k to verify whether the neighboring cluster exists in its neighbor list. Again, if there are multiple candidates ($k > 1$), the CM_k with the strongest connection is chosen. Two outcomes are possible: if the neighbor of CM_k is a CH, CM_k becomes the FN and bridges the clusters. However, if the neighbor is a regular node, then two regular nodes from the respective clusters are designated as the new FNs.If the departing node CR_k is itself the cluster head, it informs all CMs of its intention to leave. This communication is done securely with time complexity $\mathcal{O}(n)$, where n is the number of neighboring nodes or cluster members. The CH then appoints a secondary cluster head (SCH) as the new leader via secure communication. The new CH selects another SCH based on CHDF value.If the departing node is a FN, it notifies the neighboring cluster of its exit. If CH_k is present in the neighbor list of the departing FN_k, the process continues as normal. However, if FN_k does not include CH_k in its neighbor list, the departing node is identified as a regular node (CM). The regular node notifies the main CH_k of its departure. CH_k checks if the leaving node is an SCH; if so, a new SCH is selected from among the CMs. Additionally, the time slot used by the departing node is de allocated. CH_k also notifies the adjacent cluster about the departure and performs a secure key update through cryptographic key exchanges within the cluster.Specifically, broadcasting and secure key exchange operations incur $\mathcal{O}(n)$ complexity due to the need to reach multiple nodes. Similarly, node selection and forwarding processes also contribute $\mathcal{O}(n)$ complexity. Since each node is processed individually, the overall time complexity remains linear. Therefore, the total time complexity of the algorithm is $\mathcal{O}(n)$, where n represents the number of cluster members being processed.

3.0.5 Security Threat Model

In the proposed protocol, the network is made up of cognitive radio users that form clusters to share spectrum efficiently. Each cluster is managed by a CH, which handles communication, beacon signals, and channel assignments, while a SCH acts as a backup in case the CH moves or fails. FNs help relay data between clusters, and PUs are licensed spectrum holders. The network can face threats from outside attackers, who may eavesdrop, inject fake messages, or replay captured packets, and from internal malicious nodes—legitimate cluster members that could manipulate spectrum sensing, falsify CH selection metrics, drop packets, or even try to take over the CH or SCH roles. These attacks can happen at different stages: during beacon transmission, false or altered signals can break cluster formation; during spectrum sensing, false PU detection may cause wrong channel choices; during neighbor discovery, fake messages can mislead nodes; and during data transmission, malicious nodes can misuse mini-slots or drop packets. To defend against these threats, cognitive uses encryption and digital signatures to protect messages, timestamps and nonces to prevent replays, secure key exchange for private communication, and backup CHs and FNs to ensure the network stays functional. Additionally, spectrum-aware trust checks make sure clusters and channel assignments rely only on genuine spectrum availability, reducing the impact of malicious nodes.To defend against these threats, the proposed protocol incorporates multiple security mechanisms, summarized in Table 3.2.

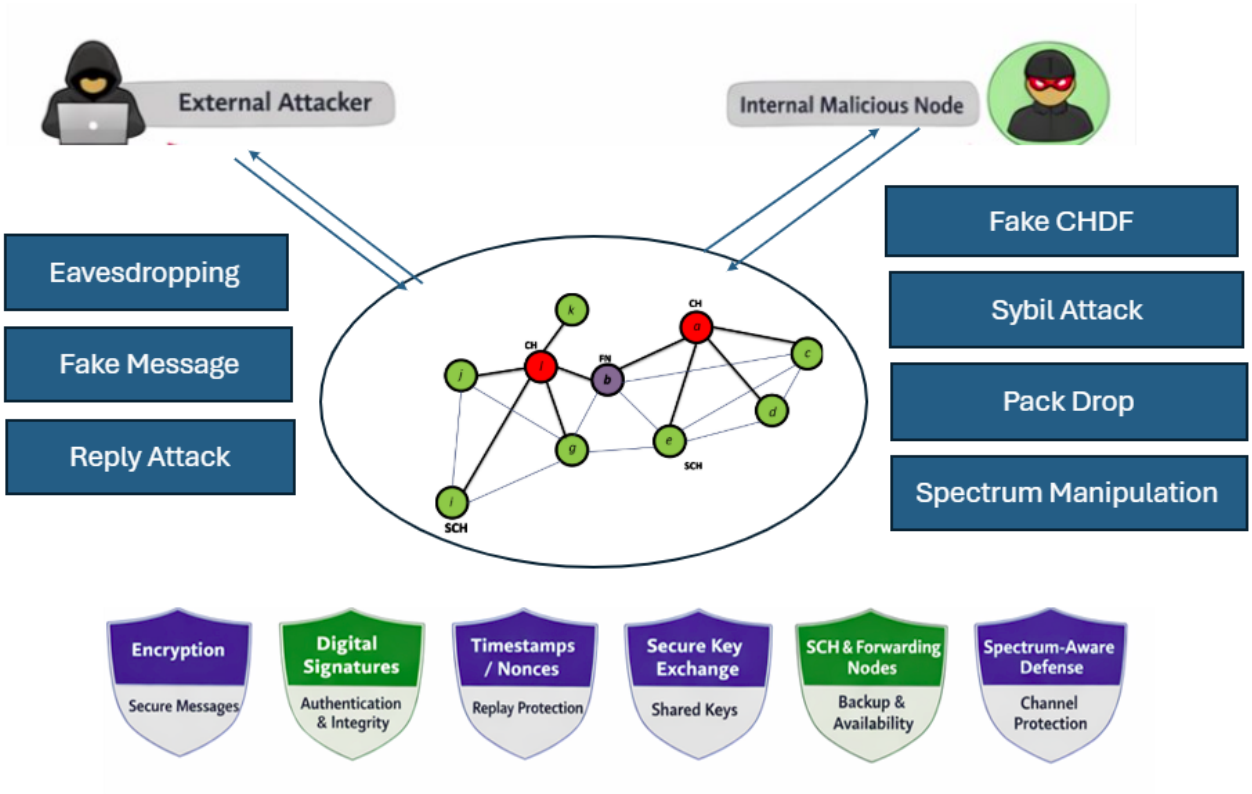


Figure 3.6: Secure CHDF Clustering Protocols threat model diagram

Table 3.2: Security Validation of the Proposed Secure CHDF Clustering Protocols

Attack Type	**Target Phase**	**Defense Mechanism**	**Security Property**	**Residual Risk**
Eavesdropping	Beacon, CHDF Exchange, Data Period	Symmetric Encryption via Shared Key	Confidentiality	Very Low
Fake Message Injection	Beacon, CHDF, Control	Digital Signature and Public Key Verification	Integrity, Authentication	Very Low
Replay Attack	CHDF and Control Exchange	Timestamp/Nonce Validation	Freshness	Very Low
Fake CHDF / CH Takeover	Cluster Formation	Signed CHDF + Neighbor Verification + Graph-Based CHDF Computation	Secure Leader Election	Low
Sybil Attack	Cluster Formation	Unique Public/Private Key per Node	Identity Assurance	Low
Spectrum Sensing Data Falsification	Spectrum Sensing Period	Synchronized Sensing + Aggregated Decision at CH + Channel Hopping	Spectrum Integrity	Medium
Packet Dropping	Contention-Free Period	Hierarchical Monitoring (CH/SCH) + Reclustering	Availability	Medium

1. **Eavesdropping**

   Description: Unauthorized nodes intercept network communications to obtain sensitive information such as CHDF values, spectrum occupancy data, or user traffic.

   Threat: Information leakage may enable further attacks, including fake message injection or network topology mapping.

   Defense Mechanism: Symmetric encryption using shared session keys ensures confidentiality of all transmitted control and data messages.

   Residual Risk: Very Low.

2. **Fake Message Injection**

   Description: Malicious nodes inject forged control or beacon messages into the network.

   Threat: Fake control messages may disrupt cluster formation, CH/SCH election, or spectrum allocation decisions.

Defense Mechanism: Digital signatures combined with public key verification ensure message authenticity and integrity.

Residual Risk: Very Low.

3. **Replay Attack**

   Description: Previously captured valid messages are retransmitted by an attacker.

   Threat: Replay of outdated CHDF or control messages may cause incorrect channel selection or repeated leader elections.

   Defense Mechanism: Timestamps and nonces are included in each control message to guarantee freshness and uniqueness.

   Residual Risk: Very Low.

4. **Fake CHDF / Cluster Head Takeover**

   Description: A malicious node attempts to manipulate CHDF values or impersonate a Cluster Head (CH).

   Threat: A compromised or fake CH may misroute packets, manipulate spectrum allocation, or disrupt cluster communication.

   Defense Mechanism: Signed CHDF messages, neighbor-based verification, and graph-based CHDF computation ensure secure and verifiable leader election.

   Residual Risk: Low.

5. **Sybil Attack**

   Description: A malicious node creates multiple fake identities to influence cluster decisions.

   Threat: Multiple fake identities may manipulate CH selection or distort cooperative spectrum sensing results.

   Defense Mechanism: Each node is assigned a unique public/private key pair, enforcing one legitimate cryptographic identity per physical node.

   Residual Risk: Low.

6. **Spectrum Sensing Data Falsification**

   Description: Malicious nodes intentionally report incorrect Primary User (PU) activity or spectrum availability.

   Threat: Incorrect sensing reports may cause selection of busy channels, reduced throughput, or interference with licensed users.

Defense Mechanism: Synchronized sensing, aggregated decision-making at the CH, and periodic channel hopping improve spectrum integrity and reduce the impact of falsified reports.

Residual Risk: Medium.

7. **Packet Dropping**

Description: Nodes deliberately drop or refuse to forward packets during scheduled transmissions.

Threat: Persistent packet dropping may lead to communication blackouts, reduced reliability, or denial of service.

Defense Mechanism: Hierarchical monitoring by CH and SCH nodes, combined with dynamic reclustering, enables detection and isolation of misbehaving nodes.

Residual Risk: Medium.

3.0.6 Time Complexity Analysis of Secure Cluster Formation (Algorithm 3.1)

The proposed secure cluster formation algorithm consists of three major phases. Below, we analyze the time complexity of each phase.

Graph Construction Phase

Each node CR_i constructs a bipartite graph $G_{pi}(A_i, B_i, E_i)$ using its neighbor list N_i and access control list ACL_i. The graph has vertices $|A_i| = |N_i|$ and $|B_i| = |ACL_i|$, with edges existing between neighbors that share a channel. The time complexity of this step is $O(n + e)$, where e is the number of edges. In sparse networks, where $e \propto n$, this simplifies to $O(n)$.

From the bipartite graph, the maximum edge biclique graph G_{ci} is derived to determine shared channels among neighbors. Processing the edges of G_{pi} to compute the biclique per node has a complexity of $O(n)$ when using heuristic algorithms.

CHDF Computation Phase

Each node calculates its Cluster Head Decision Factor (CHDF) in Equation 3.1 where C_i is the number of free channels and N_i is the number of neighboring nodes in the maximum edge biclique graph. Iterating over neighbors and shared channels for this computation results in a time complexity of $O(n)$.

Secure Communication Phase

Nodes generate a digital signature for their CHDF value, which depends on the key size k and has complexity $O(k)$. Secure key exchange with neighbors occurs in constant time per

node, $O(1)$. Encryption and transmission of the CHDF value involve $O(k)$ for encryption and $O(n)$ for sending to N_i neighbors. Signature verification and decryption by each receiving node take $O(k)$ per operation.

Cluster Head (CH) Selection and Cluster Formation

Nodes compare CHDF values to their neighbors to select cluster heads or join as cluster members. CH selection per node has complexity $O(n)$, while secondary CH (SCH) selection per cluster requires $O(n)$. Overall, cluster formation completes in $O(n)$ rounds per node.

Overall Time Complexity

Table 3.3 summarizes the time complexity for each phase of the secure cluster formation algorithm. The total per node is $O(n + k)$, which approximates $O(n)$ in large networks where $n \gg k$.

Phase	**Complexity**
Graph Construction	$O(n)$
CHDF Computation	$O(n)$
Cryptographic Operations	$O(k)$
Cluster Formation & CH/SCH Selection	$O(n)$
Total (per node)	$O(n + k) \approx O(n)$

Table 3.3: Time complexity of the secure cluster formation algorithm.

The proposed secure cluster formation algorithm is scalable, with linear time complexity per node, $O(n)$. The dominant factor is node-level operations, including graph construction, CHDF computation, and neighbor comparisons. Cryptographic operations introduce only minor computational overhead. Figures 3.2(a–d) illustrate the process, from bipartite graph construction to maximum edge biclique computation, CHDF evaluation, and final cluster formation.

Time Complexity Analysis of Cluster Join and CH Selection Process (Algorithm 3.2)

Let:

- n = number of nodes in the network
- s = number of spectrum channels to sense
- d = number of one-hop neighbors ($d \leq n$)
- k = cryptographic key/data size

Spectrum Sensing Phase

The joining node CR_j:

- Identifies available channels
- Sequentially scans s channels to detect CH beacons

Complexity:

$$O(s)$$

The sensing period lasts longer than a super-frame but remains linear in the number of channels.

Neighbor Discovery and ACL Exchange

CR_j broadcasts its neighbor and channel lists. Neighboring nodes reciprocate by broadcasting their ACLs.

Broadcasting and receiving from d neighbors:

$$O(d)$$

Since $d \leq n$:

$$O(n)$$

Graph Construction

After collecting neighbor information, CR_j:

- Constructs bipartite graph G_{pj}
- Derives maximum edge biclique graph G_{cj}

Each node and edge is processed once.

$$O(n + e)$$

For sparse CRAHNs where $e \propto n$:

$$O(n)$$

CHDF Computation

CHDF is calculated using neighbor and shared channel information.

Since it processes neighbor-level data:

$$O(d) \approx O(n)$$

Secure Communication Operations

Includes:

- Encryption of CHDF
- Decryption
- Signature verification
- Secure join and role-switch messages

Each cryptographic operation depends on key size k:

$$\text{Cryptographic cost: } O(k)$$

Since message size is small and k is fixed:

$$O(1) \quad \text{in practice}$$

Cluster Join and CH Selection Decision

Operations include:

- ACL intersection
- CHDF comparison
- Selecting highest CHDF
- Tie-breaking using node ID
- Possible CHDF recalculation

Each requires scanning neighbor sets.

$$O(d) \approx O(n)$$

Even in rejection cases, the algorithm attempts joining other clusters in bounded linear time.

Overall Time Complexity

Combining all phases:

$$O(s) + O(n) + O(n) + O(n) + O(k)$$

Since typically:

$$s \leq n$$

$$k \text{ is constant}$$

The dominant term becomes:

$$\boxed{\text{Overall Time Complexity: } O(n)}$$

The Cluster Join and CH Selection Process operates in linear time complexity with respect to the number of nodes in the network.

Time Complexity Analysis of Node Move-Out Algorithm(Algorithm 3.3)

The Node Move-Out Algorithm ensures secure and stable cluster maintenance when a node CR_k leaves the cluster. The departing node may be a CM, FN, SCH, or CH. The procedure includes secure notification, role reassignment, and cryptographic key updates.

Let:

- n = number of cluster members or neighboring nodes
- d = number of one-hop neighbors ($d \leq n$)
- k = cryptographic key size (constant)

Secure Leave Notification

The departing node:

- Generates a session key
- Broadcasts a secure leave message to neighboring nodes

Broadcasting to all neighbors requires:

$$O(d) \approx O(n)$$

Cryptographic operations (encryption, signing, key exchange):

$$O(k)$$

Since k is fixed, it contributes constant overhead.

Forwarding Node (FN) Replacement

If the departing node is an FN:

- The Cluster Head scans cluster members
- Selects a new FN based on highest CHDF
- Establishes secure key exchange

Selection among members:

$$O(n)$$

Secure communication:

$$O(k)$$

Cluster Head (CH) Departure

If the departing node is a CH:

- CH informs all cluster members
- SCH becomes new CH
- New SCH is selected based on highest CHDF

Broadcasting and member scanning:

$$O(n)$$

Key update within cluster:

$$O(n)$$

Cluster Member (CM) Departure

If a regular member leaves:

- CM notifies CH
- Time slot is deallocated
- If CM is SCH, a new SCH is selected

These require scanning cluster members:

$$O(n)$$

Inter-Cluster Link Maintenance

If the departing node connects multiple clusters:

- CH checks neighbor lists
- Selects replacement FN
- Performs secure key exchange

Operations remain:

$$O(n)$$

Overall Time Complexity

All operations are linear with respect to cluster size:

$$O(n) + O(k)$$

Since cryptographic key size k is constant:

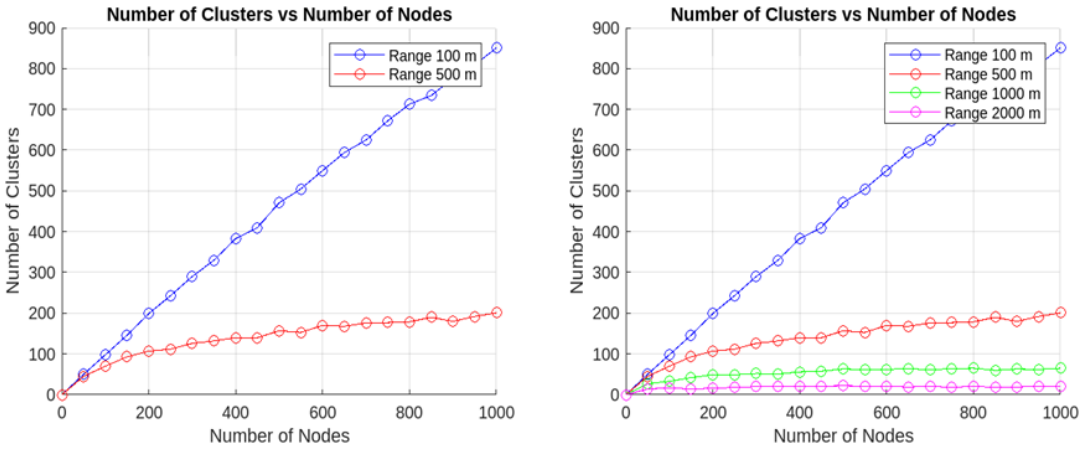
$$\boxed{\text{Overall Time Complexity: } O(n)}$$

The Secure Node Move-Out Procedure operates in linear time complexity relative to the number of cluster members or neighboring nodes. The dominant cost arises from broadcasting notifications, scanning members for role reassignment, and performing secure key updates.

Therefore, the algorithm efficiently supports dynamic topology changes while maintaining scalability in Cognitive Radio Ad Hoc Networks (CRAHNs).

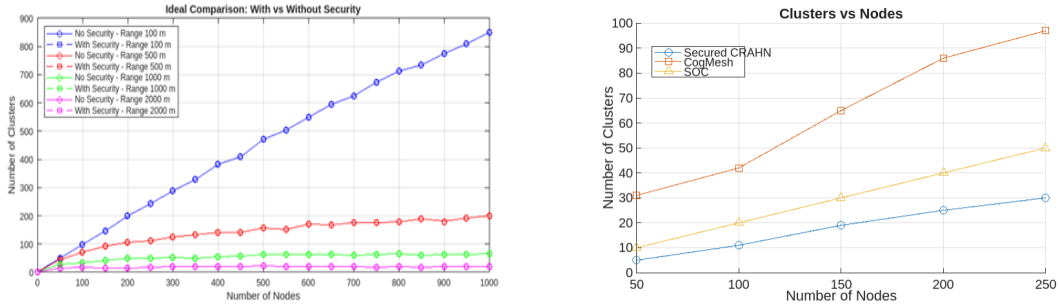
Chapter 4

Results and Discussion



(a) (b)

Figure 4.1: Comparison of Proposed Cluster Formation Performance: (a) Radio transmission 100m and 500m, (b) Radio transmission 100m, 500m, 1000m, and 2000m.



(a) (b)

Figure 4.2: Performance comparison of proposed cluster formation (a) with and without security (b)Secure Cluster formation with other approach.

The proposed clustering scheme is evaluated by measuring the total number of clusters in the network. This helps assess how well the cluster-based communication works in terms of security and efficiency for cognitive or sensor networks.The simulation is conducted in a

12 km² area, where cognitive nodes are placed randomly, simulating real-world conditions with unpredictable node placement. Each cognitive node has a communication range of 600 meters and can use one of 12 available communication channels.

Figure 4.1 depicts the performance of the proposed cluster formation method by examining the number of clusters formed and the impact of radio transmission range and network size on cluster formation. Two scenarios are considered: one with a transmission range of 500 meters and another with a range of 100 meters. The figure demonstrates that the proposed scheme results in fewer clusters when the radio transmission range is 500 meters, as opposed to 100 meters, across all network sizes. A similar pattern is observed in four different scenarios with transmission ranges of 2000 meters, 1000 meters, 500 meters, and 100 meters. This happens because an increase in a node's transmission range enlarges its coverage area. Thus, increasing the transmission range of cluster heads expands cluster coverage and reduces the total number of network clusters.

In Figure 4.2(a), we explored how clustering works in cognitive radio networks under ideal conditions, comparing networks with and without security mechanisms. Each node chooses its cluster head based on a decision factor that considers the number of idle channels and nearby nodes. In the "with security" scenario, security steps like digital signatures and encryption were included in the logic, but without adding any delays or extra energy costs. Interestingly, the results showed that the number and structure of clusters were exactly the same in both scenarios. This tells us that, in an idealized setting, security does not interfere with how clusters form. We also observed that larger transmission ranges led to fewer clusters, while more nodes naturally resulted in more clusters—patterns that held true regardless of security. Overall, this ideal comparison provides a clear baseline for understanding cluster formation and sets the stage for examining how real-world security overhead might affect network performance. Figure 4.2(b) illustrates the relationship between the number of SUs and the number of clusters for Secure CHDF, CogMesh, and SOC clustering schemes.

As the number of nodes increases, the cluster count rises across all approaches due to higher network density and clustering demand. The proposed Secure CHDF scheme consistently forms fewer clusters compared to CogMesh and SOC. At 250 nodes, Secure CHDF forms 30 clusters, while SOC and CogMesh form 50 and 97 clusters, respectively. The lower cluster count in Secure CHDF is attributed to its neighbor-aware CH selection mechanism combined with channel-overlap constraints, which prioritize nodes with more neighbors and sufficient common channels, enabling effective cluster merging while maintaining intra-cluster connectivity.

While existing protocols such as CogMesh and SOC focus primarily on throughput, energy efficiency, and cluster formation, they lack integrated security mechanisms and formal threat models. These gaps leave networks vulnerable to attacks including eavesdropping, Sybil attacks, fake message injection, CH takeover, spectrum sensing falsification, and packet dropping. Security assumptions are often implicit and reactive, with no clearly defined adversary capabilities, limiting the ability to proactively protect network commu-

nications. The proposed Secure CHDF addresses these gaps by integrating encryption and digital signatures for cluster formation and by incorporating a formal threat model that defines both insider and outsider attacks. This enables proactive mitigation of security threats while maintaining cluster formation efficiency and network performance.

Overall, the proposed Secure CHDF protocol demonstrates optimized and stable cluster formation, effectively balancing scalability, spectrum utilization, and security. It is particularly suitable for dense cognitive radio networks, where minimizing cluster overhead, maintaining reliable communication, and ensuring secure operation are critical.

Chapter 5

Conclusion

In this paper, we proposed a secure, spectrum-aware cross-layer MAC protocol for Cognitive Radio Ad Hoc Networks (CRAHNs) aimed at enhancing cluster formation efficiency while ensuring robust security. The protocol guarantees confidentiality, integrity, and authenticity by encrypting Cluster Head Decision Factor (CHDF) values during cluster formation and employing digital signatures to verify data authenticity. It maintains a stable number of common channels, dynamically adapts to spectrum availability, and mitigates re-clustering issues. Furthermore, it protects key exchanges from potential eavesdropping attacks, thereby improving overall cluster stability.

The protocol supports two critical operations: *Node-Move-In*, which securely integrates a new node into an existing cluster while safeguarding encryption keys, and *Node-Move-Out*, which ensures that departing nodes can no longer access secure communications. Pseudocode analysis of cluster formation, Node-Move-In, and Node-Move-Out procedures shows that these operations have linear time complexity, $O(n)$, ensuring scalability even in dense network environments.

Compared with existing schemes such as CogMesh and SOC, the proposed Secure CHDF protocol addresses key security limitations by incorporating formal threat modeling and proactive defense mechanisms against both insider and outsider attacks. By combining security mechanisms, neighbor-aware cluster head selection, and channel-overlap constraints, Secure CHDF forms fewer yet more stable clusters while optimizing spectrum utilization and network scalability.

For future work, we plan to reduce the time complexity of the Node-Move-In and Node-Move-Out operations to further enhance efficiency. Additionally, we aim to investigate improvements in data gathering, routing optimization, and energy management to enhance overall network performance, reliability, and applicability in dynamic CRAHN environments.Overall, the proposed Secure CHDF protocol achieves a balanced trade-off among security, scalability, and spectrum efficiency, making it a promising solution for secure and reliable cluster-based communication in cognitive radio networks.

References

[1] J. Mitola and G. Q. Maguire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[2] GSMA, "Introducing spectrum management," *Spectrum Primer Series*. [Online]. Available: https://www.gsma.com/spectrum/wp-content/uploads/2017/04/Introducing-Spectrum-Management.pdf

[3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, Apr. 2008.

[4] Y. Liao, L. Song, Z. Han, and Y. Li, "Full duplex cognitive radio: A new design paradigm for enhancing spectrum usage," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 138–145, Jan. 2015.

[5] Federal Communications Commission, "Notice of Proposed Rule Making and Order: Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies," document ET Docket No. 03-108, 2005, p. 73.

[6] J. Mitola III, "An integrated agent architecture for software-defined radio," KTH, Stockholm, Sweden, Tech. Rep., 2000.

[7] N. Mansoor, A. K. M. M. Islam, M. Zareei, S. Baharun, T. Wakabayashi, and S. Komaki, "Cognitive radio ad-hoc network architectures: A survey," *Wireless Personal Communications*, vol. 81, no. 3, pp. 1117–1142, Apr. 2015.

[8] M. Zareei, A. K. M. M. Islam, S. Baharun, C. Vargas-Rosales, L. Azpilicueta, and N. Mansoor, "Medium access control protocols for cognitive radio ad hoc networks: A survey," *Sensors*, vol. 17, no. 9, p. 2136, 2017.

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

[10] S. Feng, Z. Liang, and D. Zhao, "Providing telemedicine services in an infrastructure-based cognitive radio network," *IEEE Wireless Communications*, vol. 17, no. 3, pp. 12–20, Jun. 2010.

[11] M. V. Nguyen and H. S. Lee, "Effective scheduling in infrastructure-based cognitive radio networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 6, pp. 853–867, Jun. 2011.

[12] G. P. Joshi and S. W. Kim, "A survey on node clustering in cognitive radio wireless sensor networks," *Sensors*, vol. 16, no. 9, p. 1465, 2016. [Online]. Available: http://www.mdpi.com/1424-8220/16/9/1465

[13] N. Mansoor, A. K. M. M. Islam, M. Zareei, S. Baharun, and S. Komaki, "A stable cluster-based architecture for cognitive radio ad-hoc networks," in *Proc. IEEE Region 10 Conf. (TENCON)*, Oct. 2014, pp. 1–6.

[14] N. Mansoor, A. K. M. M. Islam, M. Zareei, S. Baharun, and S. Komaki, "A novel on-demand routing protocol for cluster-based cognitive radio ad-hoc networks," in *Proc. IEEE Region 10 Conf. (TENCON)*, Nov. 2016, pp. 632–636.

[15] N. Mansoor, A. K. M. M. Islam, M. Zareei, and C. Vargas-Rosales, "RARE: A spectrum aware cross-layer MAC protocol for cognitive radio ad-hoc networks," *IEEE Access*, vol. 6, pp. 22210–22227, 2018. doi: 10.1109/ACCESS.2018.2807781.

[16] F. G. Cocetti, J. S. Gonzalez, and I. Stojmenovic, "Connectivity-based k-hop clustering in wireless networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 205–220, 2003.

[17] S. Basagni, "Distributed clustering for ad hoc networks," in *Proc. Int. Symp. Parallel Architectures, Algorithms, and Networks*, pp. 310–315, 1999.

[18] D. Dubashi, A. Panconesi, J. Radhakrishnan, and A. Srinivasan, "Fast distributed algorithms for (weakly) connected dominating sets and linear-size skeletons," in *Proc. 14th Annu. ACM-SIAM Symp. Discrete Algorithms*, pp. 717–724, 2003.

[19] Q. Zhao, S. Qin, and Z. Wu, "Self-organize network architecture for multi-agent cognitive radio systems," in *Proc. Int. Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery*, Beijing, China, 2011, pp. 515–518. doi: 10.1109/CyberC.2011.88.

[20] X. Li, F. Hu, H. Zhang, and X. Zhang, "A cluster-based MAC protocol for cognitive radio ad hoc networks," *Wireless Personal Communications*, vol. 69, no. 3, pp. 937–955, Mar. 2013.

[21] Q. Zhao, S. Qin, and Z. Wu, "Self-organize network architecture for multi-agent cognitive radio systems," in *Proc. Int. Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery*, 2011, pp. 515–518.

[22] L. Lazos, S. Liu, and M. Krunz, "Spectrum opportunity-based control channel assignment in cognitive radio networks," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh and Ad Hoc Commun. and Networks*, Rome, Italy, 2009.

[23] K. E. Baddour, O. Üreten, and T. J. Willink, "A distributed message-passing approach for clustering cognitive radio networks," *Wireless Personal Communications*, vol. 57, no. 1, pp. 119–133, 2011.

[24] J.-Z. Zhang, F. Wang, F.-Q. Yao, H.-S. Zhao, and Y.-S. Li, "Cluster-based distributed topology management in cognitive radio ad hoc networks," in *Proc. Int. Conf. Computer Applications and Systems Modeling (ICCASM)*, 2010, pp. 544–548.

[25] A. Asterjadhi, N. Baldo, and M. Zorzi, "A cluster formation protocol for cognitive radio ad hoc networks," in *Proc. Eur. Wireless Conf. (EW)*, 2010, pp. 955–961.

[26] C.-C. Tang, K.-F. Ssu, and C.-H. Yang, "A cluster-based link recovery mechanism for spectrum aware on-demand routing in cognitive radio ad hoc networks," in *Advances in Intelligent Systems and Applications, vol. 1*, Springer, 2013, pp. 601–610.

[27] A. C. Talay and D. T. Altilar, "United nodes: Cluster-based routing protocol for mobile cognitive radio networks," *IET Communications*, vol. 5, no. 15, pp. 2097–2105, Oct. 2011.

[28] T. Chen, H. Zhang, G. M. Maggio, and I. Chlamtac, "CogMesh: A cluster-based cognitive radio network," in *Proc. 2nd IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Networks*, vol. 1, Apr. 2007, pp. 168–178.

[29] X. Li, F. Hu, H. Zhang, and X. Zhang, "A cluster-based MAC protocol for cognitive radio ad hoc networks," *Wireless Personal Communications*, vol. 69, no. 2, pp. 937–955, Mar. 2013.

[30] V. Shakhov and I. Koo, "An efficient clustering protocol for cognitive radio sensor networks," *Electronics*, vol. 10, no. 1, pp. 1–15, 2021.

[31] S. Kumar and A. K. Singh, "A localized algorithm for clustering in cognitive radio networks," *J. King Saud Univ. - Comput. and Inf. Sci.*, vol. 33, no. 5, pp. 600–607, 2021.

[32] L. Yang, Y. Lu, S. X. Yang, Y. Zhong, T. Guo, and Z. Liang, "An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks," *IEEE Sensors Journal*, vol. 21, no. 12, pp. 13935–13947, 2021.

[33] J. Wang and C. Liu, "An imperfect spectrum sensing-based multi-hop clustering routing protocol for cognitive radio sensor networks," *Scientific Reports*, vol. 13, no. 4853, pp. 1–13, 2023.

[34] M. Zheng, C. Wang, M. Song, W. Liang, and H. Yu, "SACR: A stability-aware cluster-based routing protocol for cognitive radio sensor networks," *IEEE Sensors Journal*, vol. 21, no. 15, pp. 17350–17359, Aug. 2021.

[35] H. Zhang, N. Xu, F. Xu, and Z. Wang, "GSM: Gateway selection mechanism for strengthening inter-cluster coordination in cognitive radio ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, 2013, Article 171.