Cross Layered Neighbor Route Discovery Protocol in Cognitive Radio Networks

M. Uma Suseela[1](✉), V. Hima Bindu[2], N. Durga Naga Lakshmi[1], and Vardhanapu Praveena[1]

[1] Vishnu Institute of Technology, Andhra Pradesh, India
umasuseela.m@vishnu.edu.in
[2] Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India

Abstract. New wireless services and applications have increased demand for spectrum. Communication between services and apps needs wireless spectrum. Cross-layer architecture connects the protocol layers to increase system efficiency. Not all layer functions are dumped into a network by cross-layer setup. Cross-layer architecture reduces network vulnerabilities to enhance communication. A self-determined time slot-based Cross-Layered Neighbor Route Discovery (C-LNRD) technique was developed to improve communication efficiency. Agents gather the data. The monitoring agent keeps track of the topology, time, and traffic of each neighbor at each level. The agent maintains a separate database for the data from each layer. Data is gathered at the physical, MAC, and network layers. Based on gathered metrics and updated routes, each node calculates its trust. PR ATTACK has no RTS, CTS, or RREQ in order to decrease false positives. Spectrum allocation that is adaptable and intelligent is made possible by cognitive radio and learning technology. Artificial Intelligence, Genetic Algorithm, Fuzzy Logic, and Game Theory are used to create Adaptive Cognitive Radio Networks (ACRN). High bandwidth is available from multi-hop cognitive radio networks (MCRNs) with DSA. The goal of this study is to develop MCRNs that reduce overhead, latency in routing, and spectral efficiency. The offered solution by Multi-hop CRN takes into account spectrum awareness, quality route establishment, and route maintenance in case of connection failure because of unavailability of the spectrum and node mobility. New methods enhance the cross-layer network layer protocols of MCRN. Spectrum awareness is enhanced through models. Routers and layered sensors communicate. The suggested routing method enhances performance and spectrum utilization.

Keywords: Cognitive radio · Cross layer protocol · WSN · edge based nodes · WSN

1 Introduction

In a WSN, sensors are spread hazards over a large or confined area. Sensor's role is to collect environmental data and deliver it to a sink; The objective of this technique is to create application-specific WSNs [1]. Cognitive radio maintains track of the available

P. Pareek et al. (Eds.): IC4S 2024, LNICST 598, pp. 102–110, 2025.
https://doi.org/10.1007/978-3-031-77078-4_9

spectrum bands throughout a cycle and logs the information it learns. The characteristics of the measured spectrum spaces are estimated during spectrum sensing Figure 2 depicts the Cognitive Radio Cycle (CRC) in diagrammatic form [2]. The cognitive cycle is crucial in figuring out the best order to carry out the transmission acts while taking the findings of the spectral sensing analysis into account. Radio transceiver settings for cognitive radio are based on knowledge of available spectrum bands and spectrum opportunities. In Multiple Input Multiple Output (MIMO) systems, among other things, the maximum transmission power, modulation rate, spread spectrum hopping mechanism, angle of arrival for directional broadcasts, identify the number of antennas to be used [3].

The first technique developed in this work to increase communication effectiveness in a WSN environment is called Cross Layered Neighbor Route Discovery (C-LNRD). Beginning with MAC sub-layers based on Dynamic Source Routing (DSR), the sensor network is investigated. Another feature of the MAC layer is a "dynamic route neighbor discovery table." The cross-layered sensor system is subjected to the "Broad Route Distributed Time slot Assignment" method following the discovery of the packet transmission route [4–7]. It's also important to note that the time slots are known as "Broad-Route" due to the significant differences in route length. When transmitting packets, the traffic rate is controlled by modifying the amount of data that is delivered depending on various periods with changing ranges. A "Rayleigh Fading model" is used in the C-LNRD technique to assess the communication performance of the sensor network. The imposed model can determine the proper power level for the MAC sub-layer. WSNs have a lot of cross-layer communication problems to solve. The cross-layer technique guarantees QoS while also allowing for the interchange of information between tiers. Based on this shared knowledge, the MAC protocol effectively chooses the best path over WSN settings. Consideration must be given to cross-layer time for neighbor route selection and time-slot assignment [8].

2 Background

In the Ad-hoc Cognitive radio network architecture, secondary user nodes communicate control information with their neighbors for data transfer. The development of various data structures that make use of these control messages, such as topology and neighbor node tables supports route formation between the source and destination. There are two different categories of communication channels: CCCs and DCCs. CCC are fixed channels used for the transmission of control information. To predict the status of the principal user, the prediction model includes all secondary nodes. As a result of the prediction model, channels are arranged in accordance with the next nearest channel concept. In accordance with the anticipated open spectrum bands, each node chooses an appropriate channel for communication. Figure 3 shows the spectrum sensing of the ad-hoc architecture. In order to combine the benefits of both technologies, predictor model spectrum sensing is given utilizing neural networks and genetic algorithms [9]. The prediction model can help secondary users in the sensing phase anticipate the spectrum holes before they start sensing. Even if the availability is dynamic, secondary consumers can benefit from this ideality.

For each node in the system, monitoring agents (MA) and data collection agents (DCAs) are employed. The data collection agent receives data regarding time, traffic, and topology whenever a new layer is added, and a monitoring agent keeps track of all the levels beneath it. Each level of data collection is represented by a separate table [10]. The data collecting agent makes use of the network, MAC (Media access control), and physical layers to collect data.

Using the data gathered from the various levels, each node then determines a trust value. After the routing database has been updated, only nodes that have been confirmed to be reliable can take part in routing. The metrics No RTS, No CTS, and No RREQ were used to calculate the likelihood of a real assault. Here, the integer No RTS stands for the number of RTS (Request to send) messages sent by a certain NoDE (Node) to all nearby NoDEs (Ni). The value No CTS [11] represents neighbor nodes' answers to Ni's CTS(Clear-to-send) messages. If the node Ni has broadcast any route request (RREQ) messages, then the Boolean value No RREQ is true; otherwise, it is false. Figure 1 depicts a flowchart for the complete procedure.

Selecting a DCC channel should be done fast because it takes time to discover the busy channels. A novel cross-layer cluster-based routing (CCBR) protocol called cross-layer autonomous route recovery (CLARR) mechanism [12]. By introducing a new mechanism, an enhanced CLCR (ECLCR) with IEEE 802.11p has been proposed. First, a packet's mobility parameter is added to the packet header, which can store the total network NSR for each route request packet to reduce delay. Next, the appropriate relay nodes are selected by calculating neighbor set ratio (NSR) using neighborhood knowledge to acquire more robust route for successful packet dissemination [13]. Numerous security methodologies for network-wide security, security flaws in the SDN's levels, and the security frameworks guarding each layer were all examined [14]. The main goal is to establish stable clusters for better multimedia data dissemination and to lengthen the routing path lifespan by reducing connection breakage. To do this, the mobility metric is used to introduce the clustering concept into the current CLARR. Reliability relay vehicles are then found by assessing the relative distances between them to the destination.

Spectrum prediction techniques are used to increase efficiency even more and forecast channel utilization in the future. In this regard, a back propagation training neural network-based spectrum prediction model has been suggested. A genetic algorithm is used to minimize aggressive weight patterns and optimize the neural network's topology. With the use of crossover, mutation, and selection functions, this algorithm increases unpredictability, avoiding local optima's convergence and raising the possibility of discovering the globally optimal solution [15]. Hybrid optimization is a new class of optimization heuristics that is applied. By doing this, multiple algorithms for the same optimization will be implemented. An innovative supervised learning approach for forecasting spectrum patterns in cognitive radio networks, called Genetic approach together with Particle Swarm Optimization (GAPSO), is presented in conjunction with a Back-Propagation Neural Network (BPNN) [16].

To lessen this malicious activity, a cognitive trust management system is suggested. It does this by preserving an appliance's trust and controlling Quality of Service (QoS) and service level belief. In computing networks at the edge, enhanced packet delivery ratio and jitter in cognitive trust management systems based on QoS metrics show promise for identifying potentially dangerous edge nodes [17].

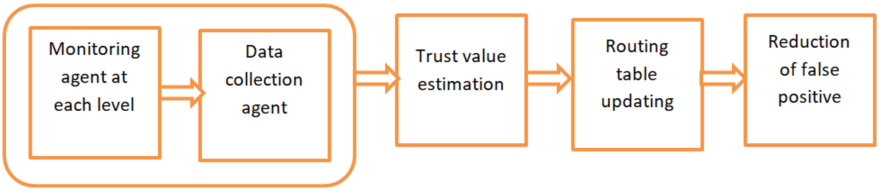

Fig. 1. Block diagram for Monitoring agent

3 Background

A full duplex wireless transceiver, with a maximum range of between 10 and 80 meters, is what the nodes in the network typically use to transmit or receive data within the local WSN scope. The nodes can also perform signal processing tasks and simple protocols. Finally, the nodes can obtain a strong, unique wired ID. Additionally, nodes with clocks are in sync [18]. Additionally, it is standard procedure for every node to make use of an internal GPS or localization algorithm. An effective communication protocol can then be created using the location information. The position data only has to be gathered once after the first network detection stage is finished because the MS and network nodes stay stationary. It's important to remember that the MS will likely be a highly capable node with improved processing, storage, and power capabilities. However, this can reach every node in the network if a high-gain antenna is used. As a result, it serves as a WSN interface and is a location for data collecting in big networks.

The processing steps of the proposed FABC-MACRD protocol are described in this section [19]. The three main phases of the FABC-MACRD protocol's functioning are Network-Assembly, Nearest-Node-Detection, and Consistent-State (Fig. 2). The following is a breakdown of its features as well. After the network has been successfully certified, it is possible to identify an effective path between two nodes for the transmission of data packets from a source node to any destination. The decision to take this route is influenced by the journey's hop count and trust value. In Fig. 6, data delivery from source node S to destination node D is being attempted. It determines the optimum way by sending the RREQ message to each of its intermediary nodes. The node that is able to respond returns the RREP message.

4 Results

Because of its open-source design and ease of use, the simulator has been utilized in several CRN applications, such as spectrum management approaches, MAC protocols, and the investigation of radio contact interference in difficult situations. Two novel MAC protocols that were expansions of the core CR MAC module were validated by these testing. Three functional levels—the application layer, the CR MAC layer, and the physical layer—that mimic transceivers and specific transmission channels make up this structure. It is the whole CRN simulator suite. Figure 3 shows the node topology that CR Simulator introduced.

Simulating the Cross-layer Architecture for Secure Multipath Routing (CASMR) protocol is achievable through NS2. In Mobile Ad-Hoc Networks (MANETs), the MAC

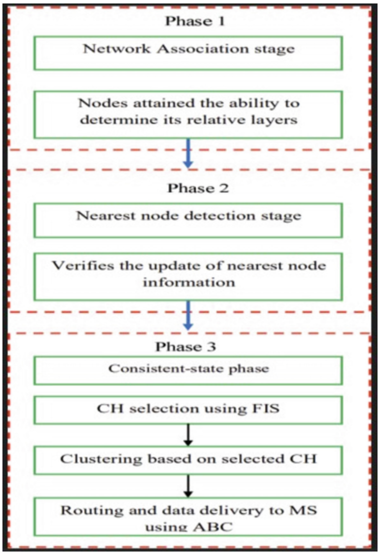

Fig. 2. Flowchart for 3 phase architecture

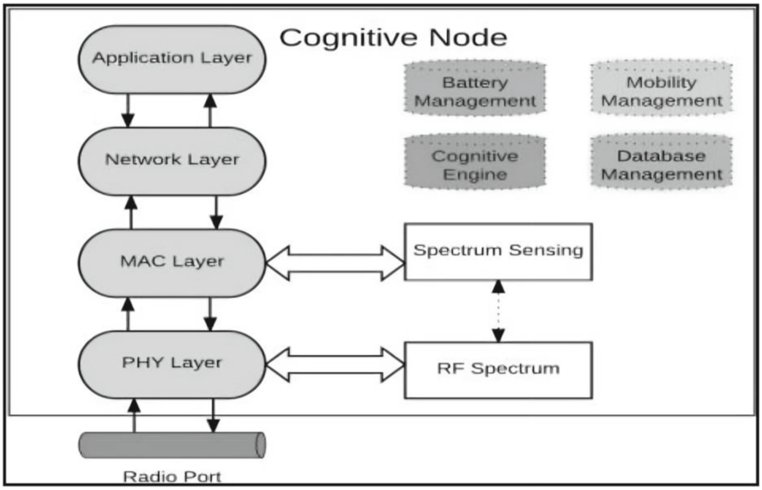

Fig. 3. Flowchart for 3 phase architecture

layer protocol employed is IEEE 802.11, which can inform the network layer of a link breakage. For this particular scenario, packet sending rates of 10, 30, 50, 70, and 90 Kb are utilized. The findings in the Fig. 4 show that CASMR has high performance i.e. low delay in comparison with the existing conventional AOTMDV protocol.

When developing Multi-hop Cognitive Radio Networks (MCRNs), a number of factors need to be considered, such as throughput, overhead, routing latency, and spectrum

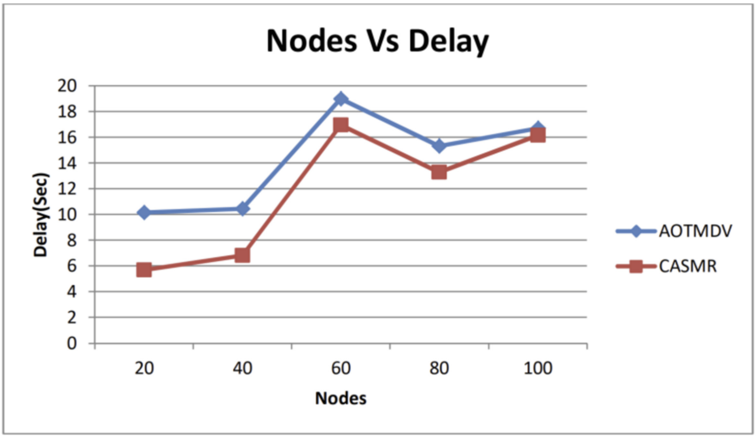

Fig. 4. Node Vs Delay

consumption. Here are some general notions and equations related to these regions, while specific equations may vary depending on the protocols and algorithms chosen:

- Utilization of Spectrum

The ratio of the bandwidth that is in use to the total bandwidth that is available is known as spectrum utilization (SU).

$$Spectrum\,utilization = \frac{\text{Total bandwidth utilized}}{\text{Total Data Transfer Capacity}} \tag{1}$$

- Throughput

Think about the total throughput for a multi-hop network, including all of the nodes in the path. The formula can be used to compute throughput (T).

$$Throughput = \frac{\text{The amount of bits were successfully transmitted}}{\text{Timing of data transfer}} \tag{2}$$

A range of between 2–10 malicious nodes is used to plot the throughput of all schemes. The improvement in number of malicious nodes lowers throughput of all schemes. Throughput can be represented by the unit of (kbps).

- Overhead

Overhead in a network can take many forms, including protocol-specific overhead, control message overhead, and signaling overhead. It is quantifiable as a proportion of the overall data supplied.

$$Overhead = \frac{Data\ size\ for\ overhead}{quantity\ of\ data\ transmitted\ overall} \tag{3}$$

- Energy Consumption

Efficient routing takes energy usage € into account.

$$E = Ptx \times Droute + \Pr x \times N \quad (4)$$

The particular algorithms, protocols, and features of the MCRN in question may necessitate adjustments to these simplified equations. In order to account for the ever-changing nature of cognitive radio networks, simulation and modeling methods are frequently used in the design and assessment of MCRNs.

NS2 is used to emulate the Cross-layer Architecture for Secure Multipath Routing (CSMR) protocol. IEEE 802.11 serves as the MAC layer protocol in MANETs. It can alert the network layer in the event of a network link failure. In our example, packet sending rates of 10, 30, 50, 70, and 90 Kb are used.

The simulation lasts for 50 s and covers a square area of 1000 m by 1000 m. This traffic has a constant bit rate (CBR). In our initial trial, CBR traffic is carried by 20 to 100 nodes. Figure 8 displays the outcomes for the CBR traffic after changing the number of nodes from 20 to 100 and contrasting the procedures. The performance of the two protocols can be compared by increasing the number of nodes from 20 to 100, as illustrated in Figure 5.

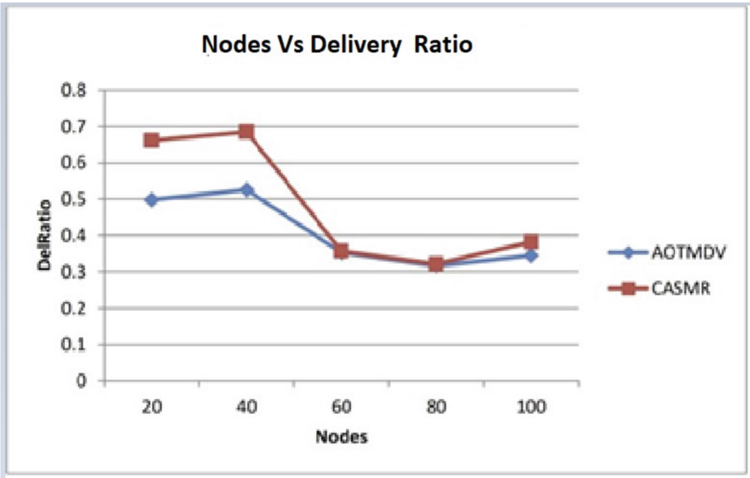

Fig. 5. Node Vs Delivery Ratio

The proposed approach uses 10 channels at a rate of 95%, compared to 90% for the traditional approaches. The suggested and existing approaches both achieve 90% and 85% channel utilization for 20 channels, respectively. For 30 channels, the channel is 85% and 80%, respectively, using the suggested and existing approaches. The standard method only utilizes 70% of the 40 channels, compared to the suggested technique's 75% channel utilization value. Using the suggested and existing approaches, 50 channels might be used at 70% and 66% of capacity, respectively. The new strategy is therefore more able to use the channel than the previous one. The suggested solution clearly beats the current in terms of latency, delivery ratio, packet loss, throughput, and channel utilization in light of the aforementioned.

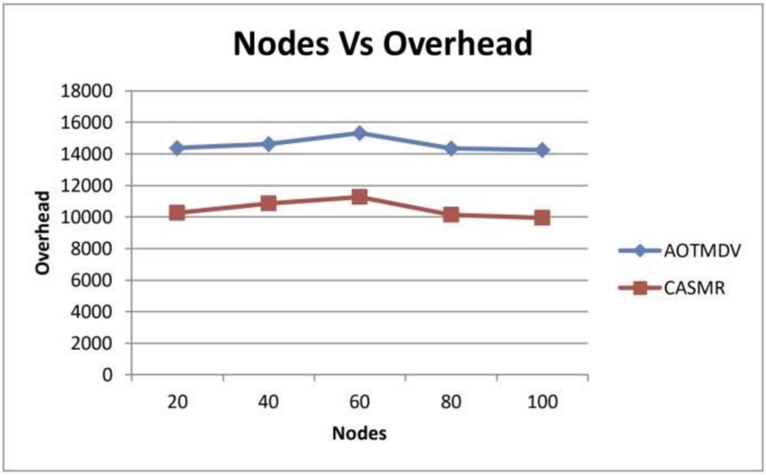

Fig. 6. Node Vs Overhead

5 Conclusion

This study's main objectives were the defense against selfish attacks in mobile ad hoc networks and secure multipath routing. The monitoring agent generates traffic and topology statistics for each neighbor it is tracking and delivers them to the data collection agent. Each level of information that is gathered has its own table. This data collection covers both the MAC and physical levels of the network. Using the data gathered from the various levels, each node then determines a trust value. After that, the routing database is changed to get ready for routing. To reduce the number of false positives, PR ATTACK is generated based on the parameters of No RTS, No CTS, and No RREQ. An optimal link state routing protocol and a multi-hop network based on cognitive radio have been developed. Modifying the ideal link-state routing protocol is necessary for choosing the optimum node. The suggested strategy is already in use on the NS2 platform. The performance of the suggested solution is evaluated using a variety of measures, including channel utilization, drop, and latency, throughput, and delivery ratio. By altering the network's node count, performance is evaluated. When compared to the current methodology, the proposed solution reduces overall delay and packet drop while enhancing channel utilization, throughput, and delivery ratio.

References

1. Caiazzo, B., Lui, D.G., Petrillo, A., Santini, S.: Distributed double-layer control for coordination of multiplatoons approaching road restriction in the presence of IoV communication delays. IEEE Internet Things J. **9**(6), 4090–4109 (2021)
2. Safaei, B., Monazzah, A.M.H., Ejlali, A.: ELITE: An elaborated cross-layer RPL objective function to achieve energy efficiency in Internet-of-Things devices. IEEE Internet Things J. **8**(2), 1169–1182 (2020)

3. Kafetzis, D., Vassilaras, S., Vardoulias, G., Koutsopoulos, I.: Software-defined networking meets software-defined radio in mobile ad hoc networks: state of the art and future directions. IEEE Access **10**, 9989–10014 (2022)
4. Valentini, R., Di Marco, P., Alesii, R., Santucci, F.: Cross-layer analysis of multi-static RFID systems exploiting capture diversity. IEEE Trans. Commun. **69**(10), 6620–6632 (2021)
5. Lee, Y., Yoon, J., Choi, J., Hwang, E.: A novel cross-layer authentication protocol for the Internet of Things. IEEE Access **8**, 196135–196150 (2020)
6. Iqbal, N., Al-Dharrab, S.I., Muqaibel, A.H., Mesbah, W., Stüber, G.L.: Cross-layer design and analysis of wireless geophone networks utilizing TV white space. IEEE Access **8**, 118542–118558 (2020)
7. Kakkavas, G., Tsitseklis, K., Karyotis, V., Papavassiliou, S.: A software defined radio cross-layer resource allocation approach for cognitive radio networks: from theory to practice. IEEE Trans. Cogn. Commun. Netw. **6**(2), 740–755 (2020)
8. Kim, J., Astillo, P.V., You, I.: DMM-SEP: secure and efficient protocol for distributed mobility management based on 5G networks. IEEE Access **8**, 76028–76042 (2020)
9. Shi, P., Gu, C., Ge, C., Jing, Z.: QoS aware routing protocol through cross-layer approach in asynchronous duty-cycled WSNs. IEEE Access **7**, 57574–57591 (2019)
10. Monica, R., Davoli, L., Ferrari, G.: A wave-based request-response protocol for latency minimization in WSNs. IEEE Internet Things J. **6**(5), 7971–7979 (2019)
11. Abd El-atty, S.M., Tolba, A.: A cross-layer approach for optimization of molcom systems toward the internet of bio-nanothings. IEEE Syst. J. **13**(3), 2751–2762 (2018)
12. Shafi, S., Venkata Ratnam, D.: A cross layer cluster based routing approach for efficient multimedia data dissemination with improved reliability in VANETs. Wirel. Pers. Commun. **107**(4), 2173–2190 (2019)
13. Shaik, S., Venkata Ratnam, D., Bhandari, B.N.: An efficient cross layer routing protocol for safety message dissemination in VANETS with reduced routing cost and delay using IEEE 802.11 p. Wirel. Pers. Commun. **100**(4), 1765–1774 (2018)
14. Goud, K.S., Gidituri, S.R.: Security challenges and related solutions in software defined networks: a survey. Int. J. Comput. Netw. Appl. (IJCNA) **9**(1), 22–37 (2022)
15. Supraja, P., Gayathri, V.M., Pitchai, R.: Optimized neural network for spectrum prediction using genetic algorithm in cognitive radio networks. Clust. Comput. **22**, 157–163 (2019)
16. Supraja, P., Pitchai, R., Raja: Spectrum prediction in cognitive radio with hybrid optimized neural network. Mob. Netw. Appl. **24**, 357–364 (2019)
17. Ganesh, D., Suresh, K., Kumar, M. S., Balaji, K., & Burada, S. (2022, October). Improving security in edge computing by using cognitive trust management model. In *2022 International Conference on Edge Computing and Applications (ICECAA)* (pp. 524–531). IEEE
18. Ngo, M.V., La, Q.D., Leong, D., Quek, T.Q., Shin, H.: User behavior driven mac scheduling for body sensor networks: a cross-layer approach. IEEE Sens. J. **19**(17), 7755–7765 (2019)
19. Marzi, Z., Madhow, U.: Interference management and capacity analysis for mm-wave picocells in urban canyons. IEEE J. Sel. Areas Commun. **37**(12), 2715–2726 (2019)