IEEE Open Journal of
Vehicular Technology

Received 1 February 2023; accepted 19 March 2023. Date of publication 7 April 2023;
date of current version 24 April 2023. The review of this article was coordinated by Editor Rongxing Lu.

Digital Object Identifier 10.1109/OJVT.2023.3263804

Reputation-Aware Relay Selection With Opportunistic Spectrum Access: A Blockchain Approach

ESRAA M. GHOURAB[1] (Student Member, IEEE), LINA BARIAH[2] (Senior Member, IEEE), SAMI MUHAIDAT[3,4] (Senior Member, IEEE), PASCHALIS C. SOFOTASIOS[5,6] (Senior Member, IEEE), MAHMOUD AL-QUTAYRI[7] (Senior Member, IEEE), AND ERNESTO DAMIANI[1] (Senior Member, IEEE)

[1]KU Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi 127788, UAE
[2]Technology Innovation Institute, Abu Dhabi , UAE
[3]KU Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi 127788, UAE
[4]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada
[5]Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi 127788, UAE
[6]Department of Electrical Engineering, Tampere University, 33014 Tampere, Finland
[7]Systems-on-Chip (SoC) Center, Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi 127788, UAE

CORRESPONDING AUTHOR: LINA BARIAH (e-mail: lina.bariah@ieee.org)

ABSTRACT The highly dynamic nature of cognitive radio (CR) systems and their stringent latency requirements pose a significant challenge in the realization of efficient intelligent transport systems (ITS). In this paper, we investigate relay selection and opportunistic spectrum access in conjunction with blockchain technology in a secure manner. Specifically, we propose a cross-layer method for secure relay selection, where secondary relays (SRs) are granted access to available spectrum bands based on the balance of their respective virtual wallets. These virtual wallets, which are built based on the SRs' secrecy capacity and their behavior in the network, are the predominant factors that allow SRs to participate in an auction model. To quantify the trustworthiness of the SRs, we formulate a mathematical framework to evaluate the trust value of each SR, which is then leveraged for rewarding or penalizing the SR. Also, we develop an offline blockchain framework to store the information of participating relays and make it available for future operations, to detect reputable and non-reputable relays in the presence of multiple eavesdroppers. The stored reputations of the participating relays are used to develop a self-learning algorithm to exclude the non-reputable relays from the selection group. Finally, we present thorough numerical results to demonstrate the superiority of the proposed system in terms of security, credibility, and integrity.

INDEX TERMS Blockchain, channel secrecy capacity, intercept probability, relay selection, security, spectrum sharing, vehicular network.

I. INTRODUCTION

The speculative vision of future sixth-generation (6G) wireless networks is expected to pave the way for provisioning secure connectivity on a large scale, enabling various applications including augmented reality, haptics, flying vehicles, and telepresence, to name a few [1]. Such applications impose new, stringent connectivity requirements as the number of connected, data-hungry devices grows exponentially. Given the scarcity of spectrum, the rapid proliferation of these new applications poses a major challenge for 6G networks, which necessitates the development of efficient spectrum-sharing mechanisms with controlled multi-user interference. This stimulated a renewed interest in cognitive radio (CR) systems, which allow unlicensed nodes to share spectrum with licensed devices while maintaining a controlled level of interference and a desired quality of service (QoS) [2]. In opportunistic spectrum access, unlicensed nodes continuously sense the spectrum to opportunistically access the spectrum to enable transmissions at higher data rates [2], [3]. On the flip side, the dynamic nature of vehicular networks

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

exposes them to potential security attacks. It is important to emphasize that security is one of the key challenges for future 6G networks. In conventional opportunistic CR networks, decentralized schemes are exploited to select trusted secondary users and allow them to transmit [4], [5].

In general, CR networks are considered a viable scheme for vehicular networks in which objects equipped with cognition make intelligent decisions by understanding both the social and physical worlds [6]. However, spectrum availability as well as data sharing and transferring among vehicles are critical for improving services and driving safety metrics, where the presence of malicious devices (MDs) further degrades network performance. Therefore, with the deployment of CR systems for vehicular networks, additional security-related issues arise, such as protecting the privacy of cooperating vehicles and identifying malicious CR-enabled vehicles that broadcast false spectrum sensing reports while driving [7]. Solving security problems in CR-VANETs is challenging because neighboring vehicles can change over time. In particular, it is difficult to detect a malicious vehicle while driving, which might send fake spectrum sensing reports, which requires rapid detection and correction. In doing so, blockchain technology has been introduced in CRN-based vehicle networks to prevent data alteration by these MDs and allow vehicles to track both legal and illegal activities in the network [8]. In particular, blockchain can provide strong security in CR networks by enabling secure dynamic access to the available spectrum and calculating the trustworthiness of participating users to effectively identify malicious users (MU) [9]. In addition, the decentralization feature of blockchain increases the security level more than traditional methods by guaranteeing that all CR network participants have a copy of the ledger to ensure complete transparency [10], [11], [12]. Thus, the problem of single-point-of-failure is prevented in a highly dynamic network, such as a CR-enabled vehicular network [13].

Because of the above characteristics, blockchain technology enables highly secure transactions, which is exactly what is missing in the current CR-based vehicular networks.

To the best of our knowledge, a framework that integrates the blockchain with other network layers, including the physical layer, in a CR scenario has not been studied in the open literature. It should be noted that the integration of the physical layer adds a new perspective to the design from the angles of complexity and reliability. Therefore, in our framework, we propose a novel cross-layer system design by integrating blockchain technology as an offline higher-level verification protocol for decentralized trust management, where we classify secondary users into reputable and non-reputable relays and use reputable ones as trusted reliable relays. The classification is based on the historical behavior of secondary users, which is quantified by the physical layer parameters in an opportunistic spectrum-sharing scenario. In particular, we introduce a payment-based algorithm via virtual wallets to grant spectrum access to unlicensed users. The auction model, where a given node is selected to leverage the available spectrum on a first-come-first-out (FIFO) basis, relies on the advertised price of each spectrum to grant unlicensed access. Transactions between licensed and unlicensed users, as well as all the information collected about the behavior of unlicensed nodes, are stored in blockchain ledgers. Therefore, the blockchain is responsible for validating and updating the virtual wallet of each node according to its historical behavior.

A. RELATED WORK

In this section, we highlight the state of the art in securing CR-based vehicular networks using conventional relay selection methods and a blockchain-based relay selection method to present the motivation for this work.

1) RELAY SELECTION IN VEHICULAR CR NETWORKS

Due to the inherently dynamic nature of vehicular networks, extensive research efforts have been devoted to developing relay selection mechanisms for CR vehicular networks [14]. In [15], the authors propose a buffer state-based relay selection procedure for cooperative cognitive radio networks (CRNs). The model proposed in [15] reduces the internetwork interference in the secondary (unlicensed) network. From a different perspective, the authors in [16] have presented an efficient relay selection scheme to enhance security in V2V wireless communications. The main objective in [16] is to increase the channel security and decrease the intercept probability.

In [17], the authors address the security of data transmission between the transmitter and receiver of a SU via a relay in a CRN when there are eavesdroppers. Their proposed method selects the best decode and forward (DF) relay among different relays to support the transmitter and maximize the achievable secrecy rate without compromising the PU. The authors in [18] presented an optimal scheme for power allocation and relay selection in a CRN to improve the transmission rate of SU transceivers over two-way relays. Their proposed scheme maximizes system throughput. They have demonstrated the efficiency of the model through numerical simulations and comparisons of performance under different operating conditions. The authors in [19] proposed an optimal power allocation scheme between the secondary transmitter (ST) and the secondary relay (SR) with the best relay selection for a two-hop cognitive DF relay network. They presented an optimal power allocation and relay selection considering the quality of service (QoS) of PU according to the joint consideration of the interference of ST and SR with PU. In [20], a trust-preserving relay selection scheme based on Dirichlet distribution was proposed to ensure that only trusted vehicles are selected as relays. The proposed scheme guarantees the confidentiality of the locations of the participating vehicles. It also uses pseudonyms and trust level criteria instead of explicit reputation values. In [21], the authors present a cognitive user emulation attack in a CRN that can be exploited by intruders during spectrum handover. They proposed a secure handover mechanism that can successfully

defend the CR network by introducing a controlling cognitive user that calculates the trust level of each cognitive user based on its behavioral characteristics.

On the other hand, a spatiotemporal diversity-based mechanism has been evaluated to confuse eavesdroppers by sending fake data over relays/vehicles traveling on a multi-lane road through dynamic paths. Moreover, in [22], the authors presented a novel MTD framework to improve the channel secrecy capacity in a two-phase DF network. The approach to MTD proposed in [22] enables multi-dimensional spatiotemporal diversification of user traffic in a cooperative wireless network, preventing attackers from tracing the signal transmission pattern.

2) RELAY SELECTION SCHEMES BASED ON BLOCKCHAIN AND SPECTRUM SHARING IN VEHICULAR NETWORKS

In [8], [9], the authors propose a blockchain protocol that provides secure and dynamic access to the available spectrum. The system relies on a virtual currency, Specoins, as a metric to quantify the trustworthiness of participating nodes. The goal of the presented protocol is to prevent malicious users from accessing the licensed spectrum without paying for it. Specoins are used in the transactions to either reward miners for updating the blockchain or allow unlicensed users to lease the available spectrum. In [12], the authors presented a blockchain-based protocol for detecting spectrum in CR networks where malicious attacks are taking place. They proposed an accurate recognition strategy to distinguish authorized users from malicious ones. In particular, they exploited the digital signatures of all the nodes involved to identify reputable users. Moreover, in [23], the authors presented a new approach for secure spectrum management in CR networks using machine learning (ML) and blockchain algorithms. The proposed framework consists of three steps. First, spectrum discovery using the ML-based extreme learning machine (ELM) method. Second, using blockchain to securely allocate spectrum between unlicensed users. Finally, malicious users are identified and prevented from accessing the available spectrum resources. Moreover, blockchain technology has been used in [24] to validate the certificates required for vehicle authentication. In particular, a fully distributed vehicle admission/revocation scheme was proposed to improve network security via digital certificates. The proposed system performed vehicle registration, admission, and revocation in a decentralized manner using blockchain. The authors in [25] proposed a blockchain architecture for radio access networks to coordinate network access in a secure and decentralized manner. The results reported in [25] show that the proposed model is able to handle the rapid network variations and QoS requirements of users. In [26], the authors model a spectrum access coordination process as a call admission control optimization problem using a continuous-time Markov decision process (CTMDP). Spectrum access requests from opportunistic SUs are queued using a blockchain before they can access an idle spectrum. The parameters of CTMDP were applied to a feed-forward neural network to derive the optimal strategy for maximizing the rewards of the threshold policy for accepting SUs. In [27], the authors proposed a blockchain-based framework for dynamic spectrum access sensing. The proposed framework uses unlicensed users as miners to sense the spectrum. In particular, the authors assumed that the unlicensed users are responsible for mining and updating the idle spectrum. In [28], the authors proposed a cross-layer approach that optimizes the selection process for the best relay in a cooperative DF network, allowing only trusted relays to participate in data transmission. They used blockchain to store real-time information about participating users and their channels. They used throughput and bit error rate (BER) as evaluation metrics to demonstrate the effectiveness and efficiency of the presented approach. Finally, in [29], the authors presented a system for validating the exchanged messages in vehicular networks using the Bayesian inference model. Based on blockchain technology and roadside units (RSUs), each vehicle in the network is assigned a trust value based on the validation process of the miners and then stored in the chain. By implementing the proposed system, vehicles can evaluate the credibility of the received messages. However, the proposed solution assumes that all decisions are made online in real-time, which results in a high delay until the decision process is completed. These decisions are generated with a significant delay due to the dynamic message exchange protocol. Such delays have a negative impact on the performance of the wireless network. Authors in [30] proposed a token-based dynamic spectrum-sharing platform with blockchains and smart contracts. Their proposed platform improves efficient spectrum usage while enabling advertisement- and sensing-based dynamic spectrum sharing by primary users (PUs) and secondary users (SUs). They demonstrated the utility and performance of the proposed platform by developing it using the Ethereum blockchain and a set of wireless devices. Moreover, the authors in [31] have proposed a blockchain-based spectrum access mechanism for unlicensed spectrum in semi-decentralized wireless networks. Due to some access delay, their proposed spectrum access mechanism can be used for non-real-time data transmission and processing in cyber-physical-social systems (CPSSs). They also used mining on blockchains to solve spectrum conflicts. Finally, they proposed a blockchain-based KM protocol, which is a private chain, to achieve spectrum allocation and transaction recording on a network.

The above discussions are implemented entirely based on higher-level operations. In particular, lower levels are assumed to automatically adapt to changes offered by higher layers. Implementing these schemes in practical scenarios results in a significant overhead for the lower layers to recognize and support the decisions of the higher layers. Due to the lack of coordination between these layers, the research contributions discussed so far have not provided a comprehensive evaluation of network performance considering the

TABLE 1. Comparative Analysis of Related Work

Ref	System Model	Objective	Approach Followed	Findings
[12]	BC-based CRN + Multiple PUs & SUs. + Malicious user.	Max. CRN security during spectrum sensing.	A blockchain-based method was used to detect MU through cryptographic keys.	The method complexity, in contrast to prevailing models, was very low. + storage of a large number of blocks, which drives up the energy consumption.
[8], [9]	BC-based CRN + PUs with HD & SUs. + Auction mechanism.	Max. spectrum leasing security.	A blockchain-based verification method for secure spectrum sharing using Specoins, to rent the spectrum.	The proposed model is compared to ALOHA. They have not considered the multipoint attacks nor studied the impact of other parameters of wireless channel. The system is not suitable for devices with limited power consumption.
[23]	BC-based CRN + PUs with HD & SUs. + Auction mechanism.	Max. Detection rate + Min.Error rate.	Leveraging ML and BC algorithms to enable secured spectrum management.	The SNR range is very limited, and they didn't consider the delay of the presented model space. The system is not suitable for power constrained devices.
[27]	BC-base DSA framework.	Max. Avg. transmission rate + Max. system energy efficiency.	Cooperative spectrum sensing scheme for CRN.	Laking many aspects of spectrum management applications, such as spectrum trading and secure database & policy inforcement. An additional power consumption is experienced at SUs.
[28]	Cooperative vehicular Net.	Max. Throughput.	A cross-layer framework.	Although the proposed framework has improved the performance of the vehicular network, security analysis is lacking given the existence of Eav. Adaptive routing selection has not been considered.
[29]	Blockchain-based decentralized trust management in vehicular network.	Max. credibility.	A blockchain-based system to validate received messages using Bayesian inference model.+ Develop joint PoW and PoS consensus mechanism.	A real-time trust value calculation that relies on the offset of vehicles in the chain. Hence, the resulting delays significantly degrade the QoS.
[26]	BC-base CRN.	Opt. SUs arriving + Max. total discounted reward.	Designing optimal CRN by establishing a CTMDP Process.	Laking many aspects of spectrum management applications, such as spectrum trading, secure database & policy inforcement, and spectrum sensing.

parameters of multiple layers. Moreover, the interaction of higher and lower layers with the leverage of blockchain in CR networks has not been studied in the literature yet.

In this work, we tackle some of the shortcomings in the literature and provide a system configuration that guarantees trustworthiness in a CR vehicular network. Table 1 shows a comparative analysis of the researched literature indicating the main advantages and limitations in order to emphasize the main contribution of our work.

In particular, we develop a cross-layer design in order to realize secure CR networks. Such a design has not been proposed in the literature yet. Specifically, we integrate blockchain technology as an offline higher-level verification protocol for decentralized trust management, where we classify secondary users into reputable and non-reputable relays and use reputable ones as trusted reliable relays. The classification is based on the historical behavior of secondary users, which is quantified using the physical layer parameters in an opportunistic spectrum-sharing scenario. The cross-layer approach aims to handle computationally intensive transactions at the network layer without compromising the communication quality. To enable a self-learning system, the framework allows the non-reputable relays to improve their participation quality by sending them alerts. This procedure guarantees the trustworthiness of each relay in the network. Only the SR, whose trust value is above a certain threshold, is allowed to play the role of an active relay in the network.

B. CONTRIBUTION

In this paper, we propose a novel framework for reliable relay selection in CR vehicular networks. The proposed selection scheme enables real-time interaction between the physical and network layers by integrating a blockchain algorithm. The main contributions of the paper can be summarized as follows.

- Propose a solid cross-layer design, that is developed in order to realize secure CR networks, where we incorporate key performance indicators (KPIs) pertaining to the physical layer, network layer, and the cloud.
- Develop a relay selection mechanism based on the available balance of SRs' virtual wallets, which in turn depends on the channel secrecy capacity and the behavior of SR in the network.
- Implement an efficient auction model to identify reputable and non-reputable relays depending on the result of the historical behavior in the blockchain ledgers.
- Develop a self-optimized rewarding/penalizing scheme, to avoid internal attacks by revoking the non-reputable nodes.

The rest of the paper is organized as follows. The detailed system model is presented in Section II. Section III. presents the traditional CR model characteristics. Section IV. presents the proposed blockchain framework to secure the CR network. Section V. illustrates the mathematical model supporting the best relay selection and trust values calculation. Section VI. presents simulation results and the paper is concluded in Section VII.

TABLE 2. List of Symbols

Notation	Definition
$\hat{H_{IXJ}}$	Determined state of the spectrum
C_s	Channel Secrecy Capacity
P_{int}	Intercept Probability
n	AWGN
γ	signal to noise ratio
N	Total Sensing time Slots
J	Number of Channels Available
K	Number of involved relays
L	Number of eavesdroppers
W_i^k	Relay's Wallets
max(.)	Maximum function
min(.)	Minimum function
g_1	High-reputation responses
g_2	Low-reputation responses
$Trust_{min}$	Threshold trust value

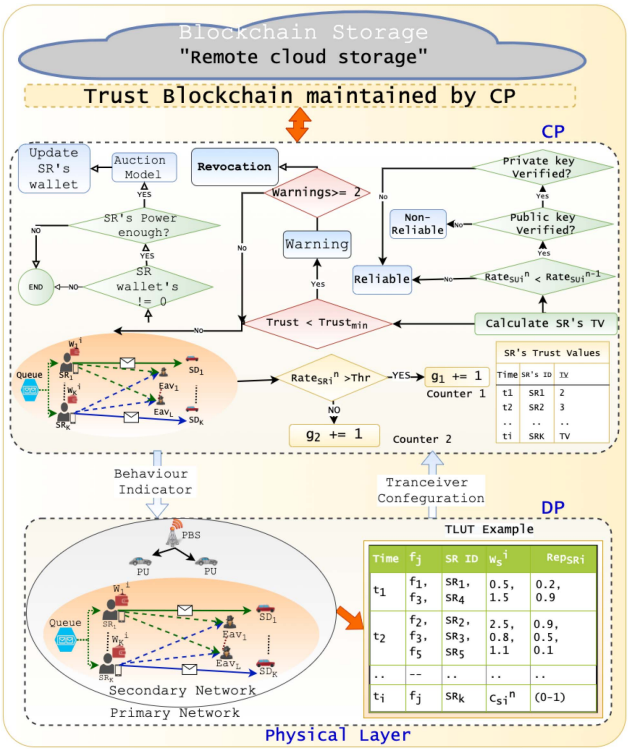

FIGURE 1. System Model of trust management in the Cognitive Radio network.

Throughout the paper, the used notations are summarized in Table 2.

II. SYSTEM MODEL

In this work, a blockchain-enabled cognitive radio (CR) vehicular network is adopted, as shown in Fig. 1. In particular, blockchain is used to improve the security of CR networks, where reputation-aware transmission is guaranteed while maintaining high-quality data transmission for primary networks. The proposed system is based on selecting reliable relays and allowing them to access the spectrum securely according to the framework shown in Fig. 1. This can be achieved by quantifying the confidentiality level of all relays and then using it as a criterion to decide whether each participating node should be rewarded or penalized. This approach is presented in two interrelated planes, namely the data plane (DP) and the controller plane (CP).

A. DP

The data plane is part of a network responsible for data transmission. It includes a primary vehicular network, a secondary vehicular network, and L eavesdroppers. The primary network consists of a primary base station (PBS) and N_P primary users (PUs). The PUs exploit the licensed spectrum to communicate with their corresponding PBS. The secondary network, on the other hand, consists of K secondary relays (SRs) and K secondary destinations (SDs). The SRs opportunistically access the licensed spectrum with the PUs. Each SR is equipped with computing and sensing devices. Due to the broadcast nature of wireless networks, eavesdroppers might be able to overhear exchanged messages between nodes. Therefore, the proposed model examines the worst-case impact of L eavesdroppers on the reputation of the secondary relays.

Owing to the heterogeneity of the network, SRs are divided into two categories, namely, reputable and non-reputable relays. Specifically, if particular SRs are in the same range, they receive the same channel status information (CSI). If the signal received by a particular relay is different from that of its peers, that relay may be classified as non-reputable.

The operation of DP is illustrated in Fig. 2 in detail. It is worth noting that each relay (vehicle) in the CR network has a unique identity number (ID), which can be its MAC address. This ID contains the public and private keys of the corresponding relay, which are used for digital signatures and encryption methods. Based on Fig. 2 and Algorithm 1, we explain the main architecture of DP and the classification of relays below:

- At each time instant, when there is a vacant spectrum, a transient lookup table (TLUT) is populated with data about the relays involved. This TLUT consists of the IDs of the relays, the available spectrum, and the reputation of each SR.
- Each relay is associated with a virtual wallet that reflects its behavior on the network. Initially, these wallets are initialized based on the channel secrecy capacity of each SR [32]. Then, the values of the wallets increase or decrease according to the auction results, which is the basic step to determining the reputation of SRs. The auction model is explained in detail in Section IV-B.
- The wallets allow relays to participate in the auction algorithm. In particular, a relay with the highest balance in the wallet can rent the available spectrum.
- Determine the reputations of the winning relays based on their intercept probabilities. These reputations are

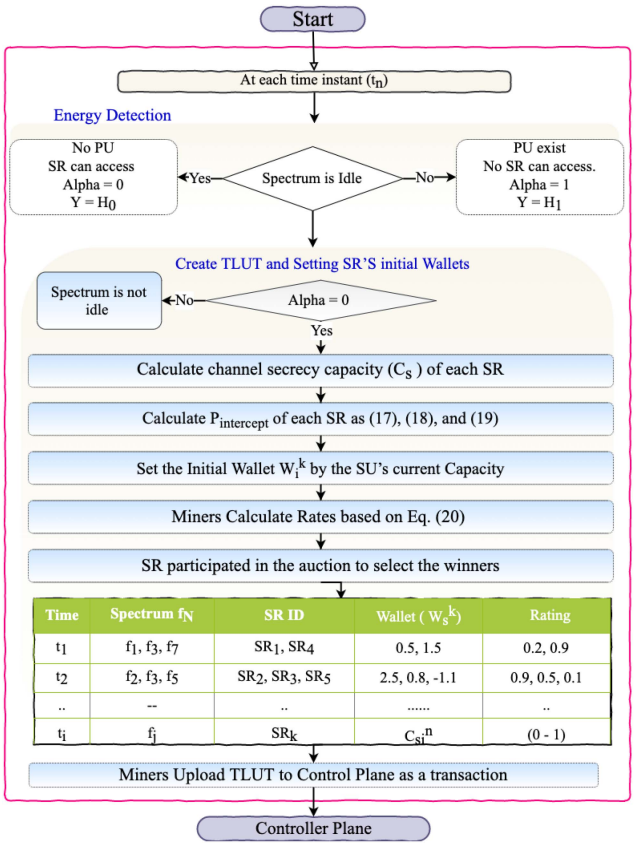

FIGURE 2. Flow Chart representation of Data-Plane mechanism for proceeding the SR's reputation and uploading them for the second phase based on the cognitive networks blockchain trust management.

compared with a certain threshold to be classified as high reputation (g_1) and low reputation (g_2).

- To evaluate the trustworthiness of SRs based on their historical behavior, the weighted accumulation approach is used as explained in Section V-C. However, the participating relays are rewarded or penalized for their participation in the mining process. The aforementioned information is stored in the communication awareness table (CAT), as explained in Section II-B.
- As a self-learning approach, the proposed model revokes the non-reputable relays after comparing their trust values with thresholds and sending them several warnings.
- Finally, all this information is uploaded to the CP and stored in blockchain ledgers to be ready for the following operation on the CP.

B. CP

The CP is responsible for managing trust values and detecting non-reputable relays. The CP consists of several control users (miners); a minor can be any relay of the available SRs or any other trusted node connected to the network. The mining operation begins by processing the TLUT data, which includes SRs IDs, digital signatures, and reputations. The miners are responsible for:

Algorithm 1: Data Plane Algorithm to Generate TLUT and SR's wallets.

Result: Transient Lookup Table (TLUT) and SRS initial Wallets

Initialization;

At each time instant t_i;

while *Spectrum is Idle* **do**

  Calculate channel secrecy capacity (C_s) of each SR;

  Miners Calculate Reputations based on P_{int};

  Set the initial wallets values (W_i^k) by the SRs current reputations;

  The winning SR is selected based on these reputations;

  Miners upload the TLUT to CP;

end

TABLE 3. Transient Lookup Table for All Available Relays' Reputations

Time	Spectrum (f_j)	SR ID	Reputation
t_1	f_1,f_2,f_5	SR_1, SR_4	0.2, 0.9
t_2	f_3,f_4,f_5	SR_2, SR_3, SR_4	0.5, 0.7, 0.1
..	....	....	....
t_n	f_j	SR_K	(0-1)

TABLE 4. Communication Awareness Table for All Available Relays Trust Values

SR's ID	Auction	Mining Activity	Trust Value T_n
SR_1	✓	✓	$T_{n-1}+2$
SR_2	X	✓	$T_{n-1}+1$
SR_3	X	X	$T_{n-1}-2$
...	..	..	...

1) Verify the data received from DP and allow SRs to participate in the auction process according to their wallets. The auction process is defined as a competition between SRs to lease the available spectrum from the PU. The winning relay is selected according to Algorithm 2.
2) Update the reputation values of the relays in TLUT based on the auction process.
3) Increase or decrease the wallets of the SRs according to their behavior in the auction process and tabulate the new values in the CAT as presented in Table 4.
4) Transfer the data from the CAT to the blockchain to make it available for future use. Specifically, miners calculate the trust values of SRs by determining and analyzing their reputations, as explained in Section V-C.

Fig. 3 and Algorithm 2 illustrate the CP operation in detail, including trust value calculation and trust reputation management. These operations are described as follows.

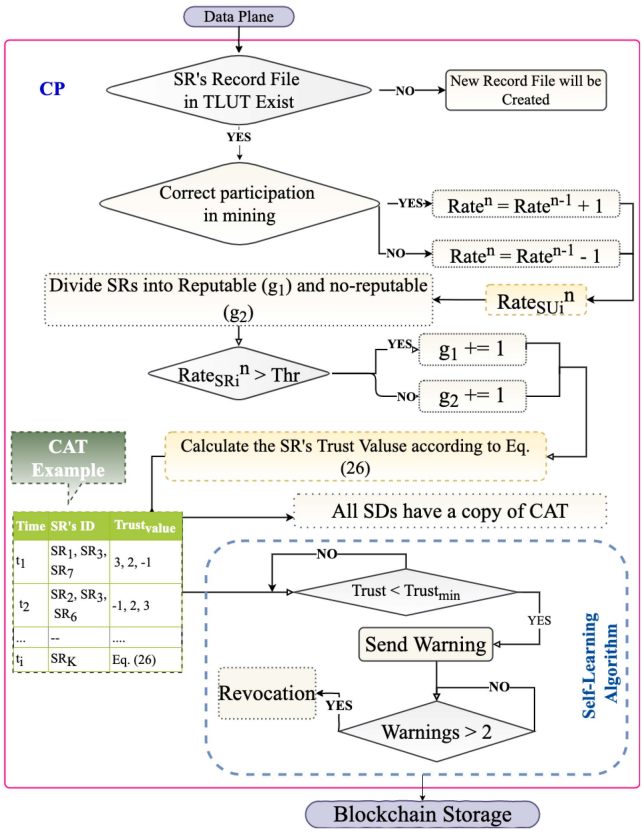

FIGURE 3. Flow Chart representation of CP mechanism for proceeding the SR's trust values and uploading them for the blockchain storage in cognitive networks.

Algorithm 2: Secure Spectrum Allocation.

Result: Secondary Relay S_i^k access to available spectrum f_j owned by a primary user PU_{N_P}
initialization;
while f_j *is not used* **do**
  advertise f_j as available spectrum;
  if $W_i^k > Cost(f_j)$ **then**
    $S_i^k \longleftarrow f_j$ request to update the blockchain by the new transaction on the $t+1$ itteration as $B_t \longleftarrow B_{t+1}$;
    Remove f_j from the available spectrum pool;
  else
    Remove S_i^k from the bidding pool;
  end
end

1) TRUST VALUE CALCULATION

The proposed framework assumes that only miners are authorized to evaluate the trust value (TV) of SRs and identify the trusted relays. The trust value is determined using the auction model in the DP plane and the aggregated reputation, which represents the historical trustworthiness and credibility of the transmitted messages of each SR.

2) TRUST REPUTATION MANEGMENT

In the proposed model, miners calculate the reputation of SRs based on their channel secrecy rate and intercept probabilities. The SD has a database register that stores a copy of the information about SRs that existed in the TLUT. However, the limited computational capacity onboard prevents the SDs from collecting a sufficient amount of data on each relay. Therefore, this data will be stored in a shared blockchain ledger, and the CP will adjust the TLUT with real-time updates based on the content of the chain.

Table 4 represents the communication awareness table (CAT) for evaluating the trust values of all available relays. In particular, we have developed a reward-based system that helps to identify reputable and non-reputable relays. This approach allows the network controller to select the optimal relay for transmission and to maximize the security of the entire system. Without loss of generality and for simplicity, we consider the following reward mechanism in our model: if an SR successfully completes the mining process, that particular relay is rewarded with one point, and if it passes the auction model, it is rewarded with an additional point. On the other hand, if a relay fails to complete any of these tasks, one point is deducted for each failure. Note that this scheme can be generalized to any number of points, but an appropriate threshold value should be chosen depending on the scheme under consideration.

III. CR MODEL

CR networks allow spectrum sharing between licensed and unlicensed nodes. In conventional CR networks, SUs sense the spectrum to determine the status of PUs. In the Interwave CR network, when a PU is active/transmitting data, SUs are not allowed to access the spectrum until at least one channel becomes idle to avoid interference between channels. On the other hand, if a spectrum is not occupied by a PU, the SU can transmit.

Let $\hat{H}$ denote the status of the sensed spectrum, then a null hypothesis $H_0 : \hat{H} = 0$ and an alternative hypothesis $H_1 : \hat{H} \neq 0$ represents the idle and occupied spectrum, receptively. In particular, according to Algorithm 4, H_0 considers the case where the spectrum is detected as unoccupied, while H_1 denotes an occupied spectrum. In our framework, we assume that the available spectrum set is f_j Hz, $\{j = 1, 2, \ldots, J\}$, and the time of the received signal is T. We define a random variable α as:

$$\alpha = \begin{cases} 0, & H_1|H_0 \\ 1, & H_1|H_1 \end{cases} \tag{1}$$

where α defines the interference of PUs and SUs that occurs due to the false alarm probability (FAP). In particular, the licensed spectrum f_j is assumed to be unoccupied by the PBS when $\alpha = 0$; therefore, the relay can access the spectrum, $\hat{H} = H_0$. On the other hand, the relay cannot access the spectrum if it is occupied by the PBS, i.e., $\hat{H} = H_1$, and $\alpha = 1$.

Algorithm 3: Spectrum Sensing Through Energy Detection.

Data: A set of K SR nodes participating in sensing the PU's spectrum, adopting two hypothesis, H_0 for idle channel and H_1 for busy channel
Result: Variable Y, representing the detected energy level.
Sense variable α:
if $\alpha = 0$ **then**
  $Y = H_0$;
else
  $Y = H_1$;
end

The probability of detection, $(P_d) = \Pr(\hat{H} = H_1|H_1)$, and the associated False Alarm Probability is $P_f = \Pr(\hat{H} = H_1|H_0)$.

A. SIGNAL MODEL

1) SINGLE EAVESDROPPER ACCESS POINT

According to the presented model in [33], when the spectrum is idle ($\alpha = 0$), the relay transmits signal x_s with power P_s. Without loss of generality, we assume that $E(|x_s|^2) = 1$. Consequently, the received signal at the SD can be represented as follows

$$y_d = h_{sd}\sqrt{P_s}x_s + h_{pd}\sqrt{\alpha P_p}x_p + n_d, \tag{2}$$

where, h_{sd} and h_{pd} represent the channel fading coefficients between the SR-SD link and between the PBS-SD link, respectively. Note that h_{sd} and h_{pd} are assumed to follow the Rayleigh distribution. Also, the additive white Gaussian noise (AWGN) at the destination is denoted by n_d, with zero mean and variance $\sigma_n^2 = N_0/2$.

Owing to the broadcast nature of wireless channels, an eavesdropper (E) could listen to the signal transmitted by the relays. Therefore, the received signal at E can be written as follows.

$$y_e = h_{se}\sqrt{P_s}x_s + h_{pe}\sqrt{\alpha P_p}x_p + n_e, \tag{3}$$

where the wireless links SR-E and PBS-E are given by h_{se} and h_{pe}, respectively, which are modeled as Rayleigh fading channels. Moreover, the AWGN at E is given by n_e, with zero mean and variance $\sigma_n^2 = N_0/2$.

2) MULTIPLE EAVESDROPPER ACCESS POINT

Assume x_p, x_{si} and $x_{s(i+1)}$ denote the random symbols transmitted by the PU and different SU, $(SU_i|i = 1, 2, \ldots, K)$, respectively at a particular time instance. Without loss of generality, we assume $E[|x_p|^2] = E[|x_{si}|^2] = E[|x_{s(i+1)}|^2] = 1$. Therefore, the received signals at D_i can be written as:

$$y_d = \sum_{\zeta=1}^{N}\sum_{i=1}^{K}\left(h_{sid_\zeta}\sqrt{P_{si}}\,x_{si} + \sum_{i=2}^{K} h_{sid(i+1)_\zeta}\sqrt{\alpha_\zeta P_{s_{i+1}}}\,x_{si+1}\right) + h_{Pd}\sqrt{\alpha P_p}x_P + n_{d_i} \tag{4}$$

Meanwhile, due to the wireless broadcast nature, eavesdroppers attempt to intercept the transmission from S_i to D_i. Firstly, we combine the received signals at E_j to obtain an enhanced version for the purpose of improving the possibility of successful eavesdropping attacks. Then, Considering the Maximum Ratio Combining (MRC), we obtain a combined version of the received signal at $(E_j|j = 1, 2, \ldots, L)$ as follows

$$y_{e_j} = \sum_{\zeta=1}^{N}\left(\sum_{j\in\Upsilon}\left[h_{sej_\zeta}(n)\sqrt{P_{sj}}x_{sj} + \sum_{m=1}^{K} h_{sem_\zeta}(n)\sqrt{\alpha_\zeta P_{sm}}x_{sm}\right) + h_{pej}(n)\sqrt{\alpha P_p}xp + n_{ej}\right] \tag{5}$$

B. CHANNEL SECRECY CAPACITY

The channel secrecy capacity (C_s) is an essential metric to quantify the security level of the nodes [34]. Accordingly, the legitimate channel capacity of SD can be written as follows using (2) and the Shannon capacity equation [35].

$$C_{sd} = \log_2\left(1 + \frac{|h_{sd}|^2\gamma_s}{\alpha|h_{pd}|^2\gamma_p + 1}\right) \tag{6}$$

$\gamma_s = P_s/\sigma_n^2$ and $\gamma_p = P_p/\sigma_n^2$. Likewise, the wiretap channel capacity can be evaluated as:

$$C_{se} = \log_2\left(1 + \frac{|h_{se}|^2\gamma_s}{\alpha|h_{pe}|^2\gamma_p + 1}\right) \tag{7}$$

Therefore, the channel secrecy capacity can be written as

$$C_s = \begin{cases} C_{sd} - C_{se}, & \gamma_s > \gamma_p \\ 0, & \gamma_s \le \gamma_p \end{cases} \tag{8}$$

IV. SECURE CR NETWORKS USING BLOCKCHAIN

Initially, the relays acquire the spectrum (f_j) based on energy detection, as in Algorithm 3, to determine the state of channel occupancy. The determined state of the spectrum is represented by $\hat{H}_{N\times J}$ (i.e., N represents the total sensing time slots, and J represents the number of available channels). The null hypothesis $H_0 : \hat{H}(i, j) = 0$ denotes the idle spectrum at time i, while the alternative hypothesis $H_1 : \hat{H}(i, j) \neq 0$ represents the case where the licensed spectrum j is occupied by the PBS at time i.

It is worth noting that the proposed model exploits the blockchain to improve the trustworthiness of participating relays and prevent non-reputable relays from accessing the

Algorithm 4: Detection of Non-Reputable Relays via Intercept Probability and Digital Signature Verification.

Data: A set of C_s^K signals are received from K users after performing energy detection.
Result: Classification of reputable and non-reputable relays.

```
for Decision C_s^i, i = 1 to K do
    if Rep_{SR_i}^n > Rep_{SR_i}^{n-1} then
        Reputable SR Detected;
    else
        if Public Key is verified then
            if Private Key is verified then
                Reputable SR Detected;
            else
                non-reputable SR Detected;
            end
        else
            non-reputable SR Detected;
        end
        non-reputable SR Detected;
    end
end
```

spectrum. The algorithm developed for this purpose is explained in the following subsections.

A. RELAYS CLASSIFICATION

After performing spectrum sensing, SRs are classified into reputable and non-reputable relays using the proposed mechanism shown in Algorithm 4. This mechanism ranks the participating relays based on two metrics, namely, cumulative intercept probability and digital signature verification; the latter is performed using public and private keys. The detection probabilities are explained below.

1) PROBABILITY OF DETECTING A REPUTABLE SR

The probability of detecting a reputable relay can be evaluated as

$$P_d = \frac{\theta_a}{\eta} \tag{9}$$

where θ_a denotes the number of detected reputable relays and η is the total number of iterations.

2) PROBABILITY OF DETECTING A NON-REPUTABLE SR

This metric specifies the probability of detecting a non-reputable SR, where, θ_m is the number of detecting non-reputable SR in η iterations, and it can be written as

$$P_{md} = \frac{\theta_m}{\eta} \tag{10}$$

3) PROBABILITY OF MISS DETECTION

The probability of miss-detection is defined as the probability that a reputable relay will be misclassified as non-reputable. This probability can be evaluated as follows:

$$P_m = \frac{\hat{\theta_a}}{\eta} = 1 - P_d \tag{11}$$

where $\hat{\theta_a}$ is the failed number of detecting a reputable relay given η number of iterations.

4) PROBABILITY OF FALSE ALARM

False alarm probability is the probability of detecting a non-reputable relay as reputable. The probability of a false alarm (P_f) is given by

$$P_f = \frac{\hat{\theta_m}}{\eta} = 1 - P_{md} \tag{12}$$

where $\hat{\theta_m}$ is the number of non-reputable SR detected incorrectly with η number iterations.

B. AUCTION MODEL

In this work, we consider a highly distributed network with different SRs. In particular, we use blockchain technology to ensure transparency and integrity. A detailed description of the auction process is provided below. The adopted auction process is performed as follows.

1) PUs set a price for the available spectrum resources.
2) A controller checks the wallet values of each SR, which are updated according to the physical layer parameters, as shown in Algorithm 2. If the balance of a particular relay is sufficient, the available spectrum is allocated to that relay. Otherwise, the relay remains in the queue.
3) The leased spectrum is removed from the pool of available spectrum, as shown in Algorithm 2.
4) The CP updates the blockchain by adding the new transaction to the ledger.
5) The blockchain operation in the auction model is performed as follows.

- The fastest user who computes the block hash (B_M) is responsible for creating the next block in the chain, (B_{M+1}), and is rewarded with the block cost, (Cost(B_{M+1})).
- All relays that participate in the hash calculation will calculate their channel capacity and upload it to the TLUT, as shown in Table 1.
- The auction winner's wallet is increased by the block cost, Cost(B_{M+1}).
- The wallet of PU is increased by the spectrum cost, Cost(f_j), while the wallet of SR is decreased by the same amount.

6) If a *SR* engages in untrustworthy behavior, and attempts to miscalculate the hash, it is excluded from the bidding pool [36].

V. PERFORMANCE ANALYSIS

A. INITIAL WALLETS VALUES EVALUATION

Due to the increasing number of attacks and the unpredictable nature of anonymous vehicles, the classification of relays'

reputations depends on their historical behavior. Therefore, the secrecy capacity of the channel and the reputation of relays are evaluated based on Algorithm 1 as follows.

1) *Single eavesdropper scenario:* The legitimate channel capacity of the ith SR is given in (15). where $n = 0, 1, 2, \ldots, I$ is the time instant. Moreover, $h_{s_{id_{i_\zeta}}}(n)$, $h_{s_{(i+1)d_{i_\zeta}}}(n)$ and $h_{p_d}(n)$ denote the fading channel coefficients at time instant n and frequency ζ of the links SR$_i$-SD, SR$_{i+1}$-SD and PBS-SD, respectively. Also, the AWGN at SR$_i$ is n_d, which has zero mean and variance $\sigma_n^2 = N_0/2$. Moreover, ith and $(i+1)$th signal-to-noise ratios are $\gamma_{s_i} = P_{s_i}/\sigma_n^2$ and $\gamma_{s_{(i+1)}} = P_{s_{(i+1)}}/\sigma_n^2$, respectively. The wiretap channel capacity at E is written as follows.

$$C_{se}(n) = \log_2\left(1 + \frac{\sum_{\iota=1}^{K}\sum_{\zeta=1}^{N}|h_{se_\zeta}|^2[\gamma_{s_i} + \gamma_{s_{(i+1)}}]}{\alpha|h_{pe}|^2\gamma_p + 1}\right). \tag{13}$$

The channel at time instant n and frequency ζ are given by $h_{se_\zeta}(n)$ and $h_{pe}(n)$, for SR$_i$-E, and PBS-E, respectively. Consequently, the ergodic channel secrecy capacity at the selected SR can be written as follows [37]:

$$C_s(n) = \begin{cases} C_{sr}(n) - C_{se}(n), & \gamma_{s_i} > \gamma_p \ |\zeta \in J \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

where, γ_{s_i} and γ_p denotes the signal-to-noise ratios (SNRs) at SR$_i$ and PBS, respectively.

2) *Multiple eavesdropper scenario:* For the worst-case scenario, we assume the existence of K relays and L eavesdroppers ($\Upsilon = \{E_j | j = 1, 2, \ldots\ldots, L\}$). The eavesdroppers independently intercept the transmitted data SR$_i - SD$. The winning SR can use the leased spectrum to transmit its data to a destination. For the case of L eavesdroppers, the channel capacity of ith SR is given in (15) shown at the bottom of this page. Similarly, the eavesdropper channel capacity of the E_j is provided by (16) shown at the bottom of this page. Within this context, the channel secrecy capacity at the destination can be written as follows

$$C_{si}(n) = \begin{cases} C_{sd_i}(n) - C_{se_i}(n), & \gamma_{s_i} > \gamma_p \ \ |\zeta \in J \\ 0, & \text{otherwise} \end{cases} \tag{17}$$

According to the calculated channel secrecy capacity, miners calculate the SRs' reputations. Initial relay wallets W_i^k will be calculated according to Algorithm 2 as

$$W_i^k = \begin{cases} C_{si}, & C_{si} > 0 \\ \text{Not available}, & \text{otherwise} \end{cases} \tag{18}$$

where the ith SR wallet becomes available only if the channel secrecy capacity is greater than zero, meaning that this SR can reliably participate in the auction model. Otherwise, if the channel secrecy capacity falls below zero, it means that this SR is exposed to possible attacks and therefore cannot participate in the transmission.

B. RELAYS REPUTATION

The overall reputation of each SR will increase or decrease according to the evaluated intercept probability, as follows.

1) *A Single eavesdropper scenario:* The intercept probability in the presence of a single eavesdropper can be written as

$$P_{int_n}^{Prop_1} = P_r(C_{se}(n) > R_d|\hat{H}_\zeta = H_0),\ \zeta \in J$$
$$= \prod_{\zeta\in J} e^{-\left(\frac{\Delta}{\sigma_{se_\zeta}^2}\right)}\left[\beta_0 + \beta_1\frac{\zeta}{\Lambda_{ps}\ \gamma_p\ \Delta\ +\ 1}\right] \tag{19}$$

where $\beta_0 = P_r(H_0|\hat{H}_\zeta = H_0)$ and $\beta_1 = P_r(H_1|\hat{H}_\zeta = H_0)$. Moreover, $\Gamma = \gamma_{s1} + \gamma_{s2}$; $\Delta = 2^{R_d} - 1/\Gamma$.

2) *Multiple eavesdropper scenario:* The intercept probability in the presence of L eavesdroppers is defined in (20) shown at the bottom of the next page. where, $\eta = (2^{R_d} - 1/\sum_{j\in\Upsilon}\gamma_{sj}) = (2^{R_d} - 1/\Upsilon\gamma_{sj})$.

3) *Benchmark model:* The conventional intercept probability can be written as [33]

$$P_{int_n}^{DT} = P_r(C_{se} > R_d|\hat{H} = H_0),$$
$$= e^{-\left(\frac{\delta}{\sigma_{se}^2}\right)}\left[\omega_0 + \omega_1\frac{1}{\Lambda_{ps}\ \gamma_p\ \delta\ +\ 1}\right] \tag{21}$$

where $\delta = \dfrac{2^{R_d} - 1}{\gamma_s}$. Moreover, $\omega_0 = P_r(H_0|\hat{H} = H_0)$ and $\omega_1 = P_r(H_1|\hat{H} = H_0)$.

Hence, the SRs reputations can be evaluated as follows

$$\text{Rep}_{SR_i}^n = \begin{cases} 1 - P_{int}^{\text{Prop}_1}, & \text{Single Eav} \\ 1 - P_{int}^{\text{Prop}_2}, & \text{Multi Eav} \\ 1 - P_{int}^{\text{DT}}, & \text{Otherwise} \end{cases} \tag{22}$$

$$C_{sdi}(n) = \log_2\left(1 + \frac{\sum_{i=1}^{K}\sum_{\zeta=1}^{J}|h_{s_id_i\zeta}(n)|^2\gamma_{s_i}}{\left[\sum_{\zeta=1}^{J}\sum_{i=2}^{K}\left(\alpha_\zeta|h_{s_id_{(i+1)\zeta}}(n)|^2\gamma_{s_{i+1}}\right) + |h_{pd_i}(n)|^2\gamma_P\right] + 1}\right) \tag{15}$$

$$C_{se_i}(n) = \log_2\left(1 + \frac{1/L\ \sum_{\zeta=1}^{J}\ \sum_{j\in\Upsilon}\ |h_{se_{j_\zeta}}|^2\gamma_{s_j}}{\sum_{j\in\Upsilon}\ \alpha_\zeta\ 1/L\ \left[\sum_{\zeta=1}^{J}\ \sum_{m=1}^{K}|h_{se_{m_\zeta}}|^2\ \gamma_{s_m}\ +\ |h_{pej}|^2\ \gamma_p\right]\ +\ 1}\right) \tag{16}$$

C. TRUST VALUES EVALUATIONS

Since the miners verify the performance of the relays based on their behavior in the network, the responses to a given signal may differ across multiple relays due to the different conditions of the participating relays. Therefore, the miners divide the responses into two categories: high-reputation responses (g_1) according to ($\sum Rep^n_{SR_i} > \text{Trust}_{min}$) and low-reputation responses (g_2) based on ($\sum Rep^n_{SR_i} < \text{Trust}_{min}$).

Note that any relay whose trust value is below the threshold (Trust_{min}) will receive an alert message. Consequently, the alerted relays must send a message with a high value to improve their trustworthiness and maintain their participation in the network. Otherwise, the miners will exclude these relays from the network and disqualify them from future participation. In our framework, trust values are calculated using the weighted accumulation approach as follows

$$\text{TV}_{SR_i}(n) = \begin{cases} \dfrac{\chi_1(n).g_1 - \chi_2(n).g_2}{g_1 + g_2}, & \text{New User} \\ \dfrac{\chi_1(n).g_1 - \chi_2(n).g_2}{g_1 + g_2} + 1, & W_i^k(n) \geq W_i^k(n-1) \\ \dfrac{\chi_1(n).g_1 - \chi_2(n).g_2}{g_1 + g_2} - 1, & \text{otherwise} \end{cases} \tag{23}$$

where $\text{TV}^n_{SR_i}$ is the trust value of the ith SR at time n. Also, the weights are χ_1 and χ_2, are given by.

$$\chi_1(n) = \max_{SR_i \in K \& n \in I} (\text{Rep}^n_{SR_i}, \text{Trust}_{\min}) \tag{24}$$

and

$$\chi_2(n) = \min_{SR_i \in K \& n \in I} (\text{Rep}^n_{SR_i}, \text{Trust}_{\min}) \tag{25}$$

D. NON-REPUTABLE RELAY DETECTION

Miners can identify the non-reputable relays based on the historical behavior involved, reputations, and trust values of all the relays. Therefore, miners check the public and private keys of a relay before deciding that it is a non-reputable one and excluding it from the network, as shown in Algorithm 4.

E. COMPLEXITY

In this section, we present the complexity of deploying the proposed CR-based cross-layer with a blockchain and the complexity of selecting the optimal relay after deploying the algorithm in order to evaluate the efficiency of the model.

1) TIME COMPLEXITY OF THE CROSS-LAYER ALGORITHM

Throughout the paper, there are two distinct modules: an *Off-Chain Module* and an *On-Chain Module.*

- *Step 1:* Off-Chain Module. The overall complexity of the first step depends on the classification of reputable and non-reputable users to select the optimal SU as a relay based on the intercept probability calculation and the auction algorithm. Therefore, the time complexity increases as the number of participating SRs increases. However, this complexity does not affect the real-time transmission since it is deployed off-chain (offline).
- *Step 2:* On-Chain Module. After a certain period, once the secondary users' data is stored on-chain when the PU wants to transmit data to its destination, a request will be sent to the chain in order to retrieve the trust values for all the involved SRs to select the maximum value. Since this operation is executed on the devices (i.e., in the data plane), there is no execution time; it is executed almost immediately.

2) RELAY SELECTION COMPLEXITY

Calculate the time complexity of selecting the optimal SR, it depends on the activated phase. For example,

1) During the Off-Chain module, we will ignore the delay as it is deployed off-chain
2) During the On-Chain module, selecting the optimal relay will occur almost in real-time.

F. BLOCKCHAIN SEQUENCE GENERATION

After the operations at the physical and network layer operations, the miners generate blockchain transactions that contain the CAT, which includes the SR IDs, trust values, public keys, and some useful historical data, such as the SR reputation. The miners must verify these transactions to be ready for the chain.

VI. NUMERICAL RESULTS

In this section, we investigate the performance of the proposed system in different scenarios. Unless otherwise stated, we consider the numerical parameters summarized in Table VI. We assume three SRs, i.e., SR_1, SR_2, SR_3, each of which has different channel conditions. Without loss of generality, we assume that SR_1 has the weakest average channel gain, while SR_3 has the strongest channel gain. In this section, we consider:

- **Scenario 1**, Single eavesdropper
- **Scenario 2**, Multiple eavesdroppers

In the following sections, we will explain the steps to compute the trust values using the proposed algorithms.

$$\begin{aligned} P^{Prop_2}_{int_n} &= P_r(C_{se_i}(n) > R_d | \hat{H}_\zeta = H_0), \\ &= \prod_{\zeta \in J} (1/L) \exp\left(-\sum_{j \in \Upsilon} \frac{\eta}{\sigma_{se_{i_\zeta}}} \left(\beta_0 + \beta_1 \frac{\Upsilon \zeta}{\sum_{\zeta=1}^{N} \sum_{j \in \Upsilon} [K \gamma_s \eta \Upsilon + \Lambda_{ps_{i_\zeta}} \eta \gamma_p + \Upsilon]}\right)\right. \end{aligned} \tag{20}$$

TABLE 5. Key-Parameters

Parameter	Value
No. of SRs (K)	15
No. of PUs (N_p)	8
Total number of users (N)	N = 23
No. of eavesdroppers (L)	7
Channel Type	Flat fading channel
Trust$_{min}$	0.6
Data Rate R_b	7.5 Mbps
γ	15 dB
σ^2_{sd}	0.5
$\sigma^2_{SR_1}$	0.6
$\sigma^2_{SR_2}$	0.9
$\sigma^2_{SR_3}$	1.2
Warning Threshold	0.5 - 1.5
Number of samples (n)	1e6

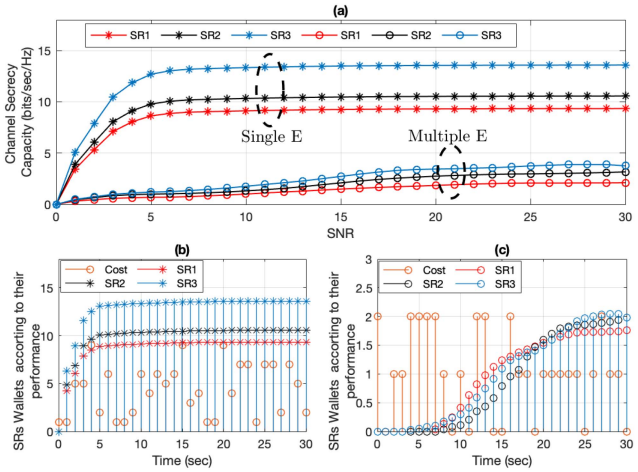

FIGURE 4. (a) The Channel Secrecy Capacity for the relays in case of single eavesdroppers and multiple eavesdroppers scenarios. (b) Relays wallet values in case of a single eavesdropper. (c) Relays wallet values in case of multiple eavesdroppers.

A. BENCHMARK

In order to validate the superiority of our framework, the distributed CR model for VANETs in [33] is selected as a benchmark model. In [33], similar to our work, the authors considered the intercept probability metric. The difference between the two models lies in the technique used to protect the network from eavesdroppers. In [33], a moving target defense (MtD) approach is used to prevent attacks, hence transmitting the data securely. Specifically, they proposed a queuing model to determine which SU can transmit data in each time slot over the available channel bands through spatiotemporal diversification. While in our framework, we follow a different approach to select the optimal SU by developing a cross-layer reliable relay selection scheme for vehicular CR networks based on blockchain and an auction model. This auction algorithm can rank participating relays as reputable or non-reputable. Specifically, we used blockchain as a trustworthy technique to increase the credibility of participating SRs by storing their trust values and revoking the SRs with low trust values, so, this technique helps to improve the overall network security.

B. CHANNEL SECRECY CAPACITY AND WALLETS

Fig. 4 shows the channel secrecy capacity of the three SRs and their associated wallets according to their performance using Scenario 1 and Scenario 2. From Fig. 4(a), it can be seen that SR_1 has the lowest secrecy capacity, while SR_3 has the highest performance for both scenarios. Such performance is to be expected given the assumed channel scenario. Fig. 4(b) reflects the values of the wallets of SR, corresponding to their channel secrecy capacity as well as their behavior in the network as in Scenario 1. It should be noted that these wallet values are provided in addition to the spectrum cost values based on the spectrum access mechanism. In particular, considering that SR_1, SR_2, and SR_3 participate in the auction model, their wallet values are compared to the available spectrum cost at each time instant. Then, the relay with a balance higher than the spectrum cost is granted access in a FIFO manner. Note that in our simulation environment, the available spectrum cost is randomly generated. For example, at $t = 4$ seconds, the cost of the spectrum is about 1.2 virtual currency (VC), and therefore, SR_2 and SR_3 can access the spectrum according to the FIFO queue, while SR_1 cannot rent the spectrum. In Fig. 4(b), it can also be observed that the behavior of the relays in the network allows them to increase their wallets over time. For example, in the figure, it can be seen that the initial value of SR_1's wallet is zero, while at time 30 seconds, it increases to 5 VC. The same observations can be seen in Fig. 4(c) for Scenario 2. However, it can be seen from Fig. 4(a) that the performance of the three relays in Scenario 2 is lower than in Scenario 1 over the entire SNR range, which justifies the results in Fig. 4(c), where it can be seen that during the first 10 seconds, all relays cannot access the spectrum because their wallet values are below the spectrum cost.

C. INTERCEPT PROBABILITIES AND SRS REPUTATIONS

Figs. 5 and 6 shows the intercept probability and the reputation of SRs according to their historical behavior in the physical layer. Note that the intercept probability is calculated according to (17) and (18). Since SR_3 has the lowest intercept probability, it can easily conclude that SR_3 has the highest reputation according to (20), as shown in Fig. 5 for the two interception scenarios. Although the intercept probability of SR_1 and SR_2 are close to each other, their reputations are different due to their different behaviors in the network. In Fig. 6, we see that although the reputation of the relays in both scenarios increases with time, SR_3 is the most reputable relay in the system. However, in the multiple eavesdropper scenarios, the reputation of SR_2 decreases after 5 seconds and reaches the reputation of SR_1 then increases again after 10

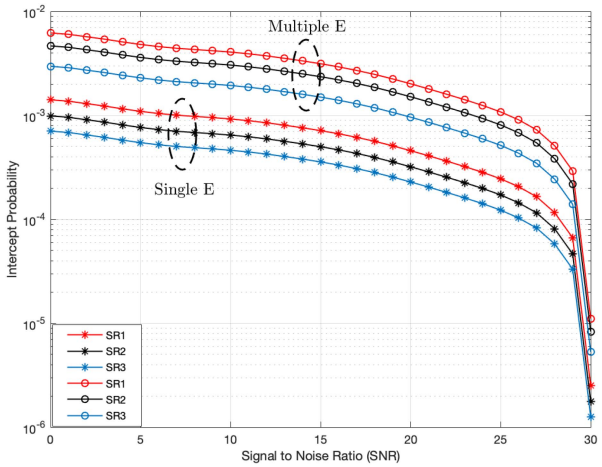

FIGURE 5. SRs' Intercept probability according to their historical behavior and wallets from the physical layer in both scenarios.

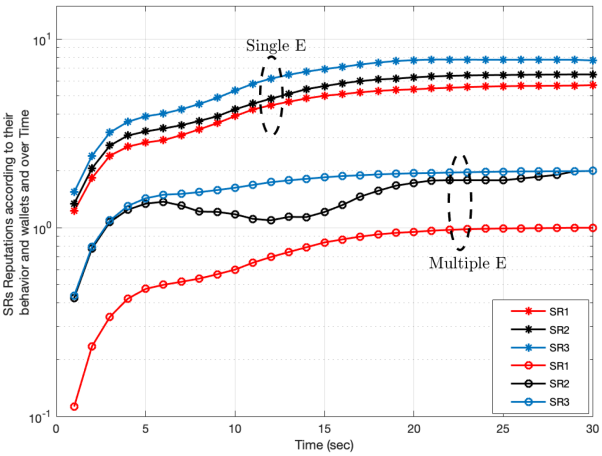

FIGURE 6. SRs Reputations according to their historical behavior and wallets from the physical layer in both scenarios.

seconds and approaches SR_3. This fluctuation is due to the overall behavior of the relays involved in the network.

D. TRUST VALUE CALCULATIONS

In Figs. 7, 8, and 9, we show high and low reputation responses and weights, g_1, g_2, χ_1, and χ_2, respectively, based on (22) and (23) for the two eavesdropping scenarios. Figs. 7(a), 8(a), and 9(a) shows the reputation weights of SR over time, where the relays whose reputation exceeds the thresholds are labeled as χ_1, while the rest are assigned to χ_2. Based on these reputation values, we show in Figs. 7(b), 8(b), and 9(b) the number of repetitions where the reputation of the involved relays is above or below a predefined threshold ($\delta = 0.6, 2.6$). Since the selected threshold has a direct effect on g_1 and g_2, as shown in Figs. 7 and 8, it should be chosen carefully. In the simulation, we choose a threshold value ($\delta = 0.6$). In the next step, after calculating the values for g_1, g_2, χ_1, and χ_2, the trust values for each involved SR can be calculated.

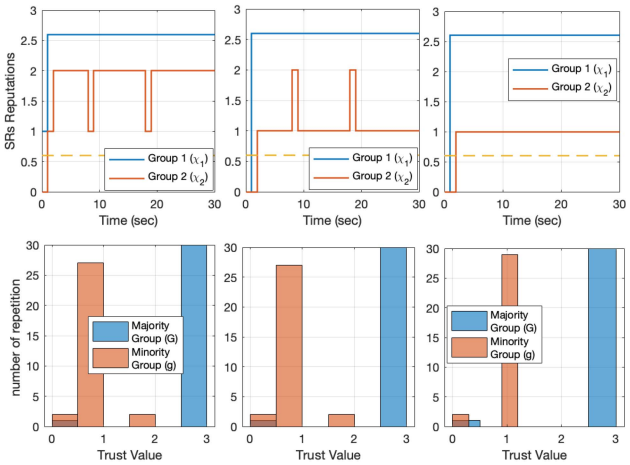

FIGURE 7. (a) Group1 and Group2 distribution, (b) SRs repetition number based on the participated SRs' reputations at $\delta = 0.6$ in case of single eavesdropper scenarios.

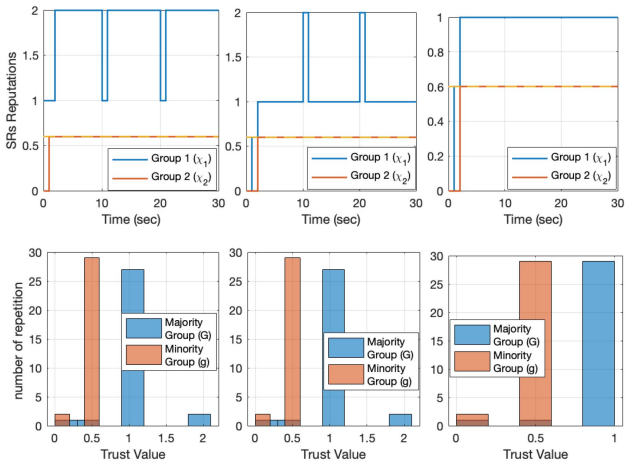

FIGURE 8. (a) Group1 and Group2 distribution, (b) SRs repetition number based on the participated SRs' reputations at $\delta = 2.6$ in case of single eavesdropper scenarios.

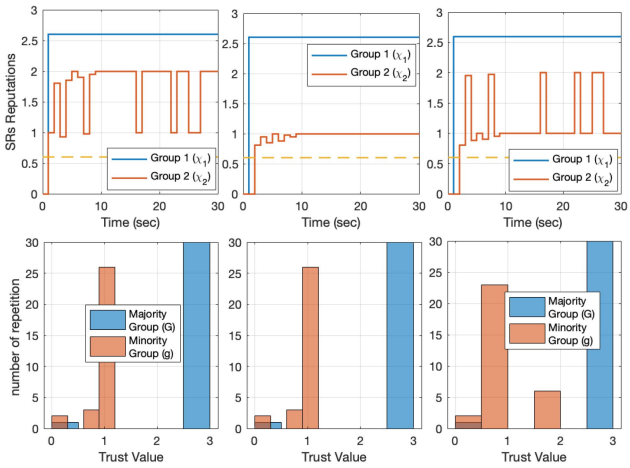

FIGURE 9. (a) Group1 and Group2 distribution, (b) SRs repetition number based on the participated SRs' reputations at $\delta = 0.6$ in case of multiple eavesdroppers scenarios.

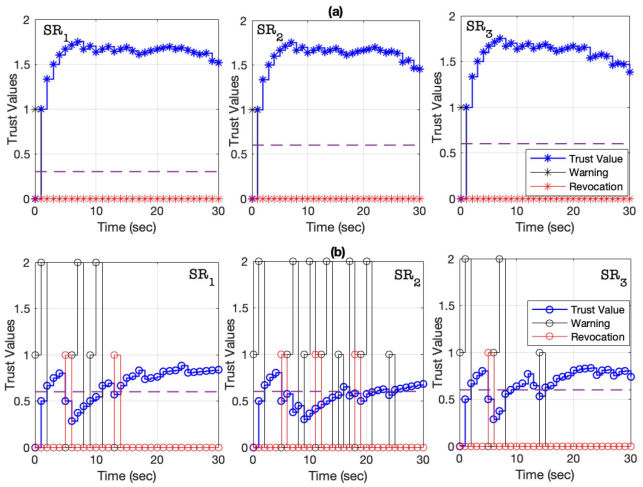

FIGURE 10. Warning messages and the Revocation list for the untrusted users based on their trusted value misbehavior over time in case of (a) single eavesdropper scenario, (b) multiple eavesdroppers scenarios.

E. REWARDING AND PENALIZING PROCEDURE

Based on the values stored in CAT (Table 4), the trust values for single and multiple eavesdropper scenarios can be evaluated according to (21). Fig. 10 illustrates the warning messages and revocation list for non-reputable SRs. In the proposed system, a reputation-aware detection system can be used to detect and prevent attacks. When an SR has a trust value below the threshold, the miners send a warning message to that SR. From Fig. 10(a), it can be seen that all relays receive a warning message only at the beginning because their trust value falls below 0.6. The main purpose of this self-learning algorithm is to detect both internal and external attacks on the system. In particular, we implement this mechanism in order to detect untrusted behaviors of SRs by warning the relay and forcing it to increase its trust value by being engaged in more mining activities or increasing the credibility of the transmitted messages. When a relay receives two consecutive warnings, it is revoked and blocked from future transmissions to ensure that all relays involved are trusted and internal attacks are avoided. Fig. 10(b) illustrates the warning messages and the blocking list, including the misbehaving relays for Scenario 2. From Fig. 10(b), it can be seen that the presence of more eavesdroppers increases the vulnerability of SRs to attacks and thus negatively affects their trust values. As shown in Fig. 10(b), a higher number of warning messages are sent to all relays compared to Scenario 1. Any relay that cannot improve its trustworthiness is excluded from further communication in the network after its public and private keys are verified.

F. DETECTION PROBABILITIES

Fig. 11 depicts detection probabilities based on the calculations of our proposed framework algorithm. We can observe that the detection accuracy for the non-reputable relay is 96% and 90% for single and multiple eavesdroppers, respectively. Moreover, the detection accuracy for the reputable relay is

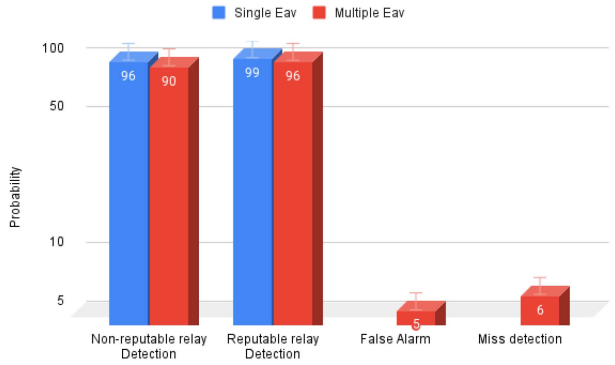

FIGURE 11. Detection probabilities based on probabilistic calculations in case of (a) single eavesdropper scenario, (b) multiple eavesdroppers scenarios.

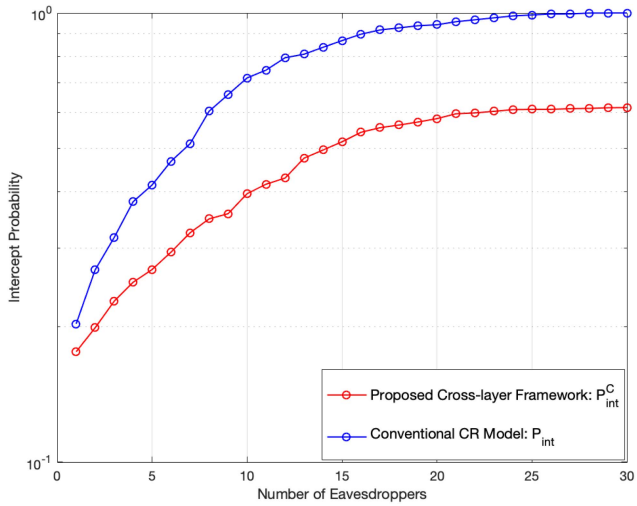

FIGURE 12. Intercept probability versus increasing the number of eavesdroppers.

99% and 96% for scenarios with one and multiple eavesdroppers, respectively. The calculated false alarm probability for Scenario 1 and Scenario 2 is 0% and 5%, respectively. Finally, the miss detection probability for both scenarios is 0% and 6%. These results prove that the proposed system is able to perfectly classify the non-reputable relays even in the multiple eavesdropper scenario.

Fig. 12 shows the performance of our proposed cross-layer framework in the case of an increase in the number of eavesdropping devices. The intercept probability increases with the number of eavesdropping devices increases. It is worth noting that our cross-layer framework increases the system's security by almost 70% compared to CR systems without a cross-layer design. These results demonstrate the efficiency and effectiveness of our cross-layer framework for securing transmission in a CR vehicular network without compromising the network's reliability.

VII. CONCLUSION

In this paper, we proposed a cross-layer reliable relay selection scheme for vehicular CR networks based on blockchain

and an auction model. In particular, we used blockchain as a trustworthy technique to increase the credibility index of SRs and contribute to improving the overall network security. Based on the calculated trust values, a mathematical model was built to evaluate the trust values of vehicles and the selection process for the best SR. The numerical results showed the effectiveness of the whole system in both single and multiple eavesdropper scenarios, in which an improved performance in terms of SR's reputation, trust value, intercept probability, and channel secrecy capacity is observed. It should be noted that the presented approach is deployed offline, and therefore no real-time delay occurs.

REFERENCES

[1] L. Bariah, S. Muhaidat, P. C. Sofotasios, F. El Bouanani, O. A. Dobre, and W. Hamouda, "Large intelligent surface-assisted nonorthogonal multiple access for 6G networks: Performance analysis," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5129–5140, Apr. 2021.

[2] J. Xiang, Y. Zhang, and T. Skeie, "Medium access control protocols in cognitive radio networks," *Wireless Commun. Mobile Comput.*, vol. 10, no. 1, pp. 31–49, Dec. 2010.

[3] L. Zhang, M. Xiao, G. Wu, M. Alam, Y.-C. Liang, and S. Li, "A survey of advanced techniques for spectrum sharing in 5G networks," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 44–51, Oct. 2017.

[4] Z. Tabakovic, "A survey of cognitive radio systems," *Post Electron. Commun. Agency*, vol. 13, no. 1, pp. 1–8, Jul. 2011.

[5] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical issues on cognitive radio-based Internet of Things systems: A survey," *IEEE Access*, vol. 7, pp. 97887–97908, 2019.

[6] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A cognitive radio technique for blockchain-enabled internet of vehicles," *IEEE trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4005–4015, Jul. 2021.

[7] K. D. Singh, P. Rawat, and J.-M. Bonnin, "Cognitive radio for vehicular ad hoc networks (CR-VANETs): Approaches and challenges," *EURASIP J. Wirel. Commun. Netw.*, vol. 2014, no. 1, pp. 1–22, Mar. 2014.

[8] K. Kotobi and S. G. Bilén, "Blockchain-enabled spectrum access in cognitive radio networks," in *Proc. Wireless Telecommun. Symp.*, 2017, pp. 1–6.

[9] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.

[10] A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. AsSadhan, and S. Lambotharan, "Blockchain-based distributive auction for relay-assisted secure communications," *IEEE Access*, vol. 7, pp. 95555–95568, 2019.

[11] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, 2019.

[12] A. Sajid, B. Khalid, M. Ali, S. Mumtaz, U. Masud, and F. Qamar, "Securing cognitive radio networks using blockchains," *Future Gener. Comput. Syst.*, vol. 108, pp. 816–826, Jul. 2020.

[13] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[14] Y. Zou, J. Zhu, X. Li, and L. Hanzo, "Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective," *IEEE Netw.*, vol. 30, no. 5, pp. 74–79, Sep./Oct. 2016.

[15] R. Zhang, R. Nakai, K. Sezaki, and S. Sugiura, "Buffer-aided relaying: A survey on relay selection policies," *IET Commun.*, vol. 14, no. 21, pp. 3715–3734, Jan. 2021.

[16] E. M. Ghourab, M. Azab, M. F. Feteiha, and H. El-Sayed, "A novel approach to enhance the physical layer channel security of wireless cooperative vehicular communication using decode-and-forward best relaying selection," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018.

[17] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, 2012.

[18] P. Ubaidulla and S. Aissa, "Optimal relay selection and power allocation for cognitive two-way relaying networks," *IEEE Wireless Commun. Lett.*, vol. 1, no. 3, pp. 225–228, Jun. 2012.

[19] P. Lan, F. Sun, L. Chen, P. Xue, and J. Hou, "Power allocation and relay selection for cognitive relay networks with primary QoS constraint," *IEEE Wireless Commun. Lett.*, vol. 2, no. 6, pp. 583–586, Dec. 2013.

[20] H. Hu, R. Lu, C. Huang, and Z. Zhang, "PTRS: A privacy-preserving trust-based relay selection scheme in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 5, pp. 1204–1218, Jun. 2017.

[21] G. Rathee, N. Jaglan, S. Garg, B. J. Choi, and K.-K. R. Choo, "A secure spectrum handoff mechanism in cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 3, pp. 959–969, Sep. 2020.

[22] E. M. Ghourab and M. Azab, "Benign false-data injection as a moving-target defense to secure mobile wireless communications," *Ad Hoc Netw.*, vol. 102, pp. 1–12, May 2020.

[23] C. R. Babu and B. Amutha, "Blockchain and extreme learning machine based spectrum management in cognitive radio networks," *Trans. Emerg. Telecommun. Technol.*, pp. 1–13, Oct. 2020.

[24] N. Lasla, M. Younis, W. Znaidi, and D. B. Arbia, "Efficient distributed admission and revocation using blockchain for cooperative ITS," in *Proc. 9th IFIP Int. Conf. New Technol. Mobil. Secur.*., 2018, pp. 1–5.

[25] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[26] W. Ni, Y. Zhang, and W. Li, "Optimal admission control for secondary users using blockchain technology in cognitive radio networks," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst.*, 2019, pp. 1518–1526.

[27] Y. Pei, S. Hu, F. Zhong, D. Niyato, and Y.-C. Liang, "Blockchain-enabled dynamic spectrum access: Cooperative spectrum sensing, access and mining," in *Proc. IEEE Glob. Commun. Conf.*, 2020, pp. 1–6.

[28] E. M. Ghourab, M. Azab, and N. Ezzeldin, "Blockchain-guided dynamic best-relay selection for trustworthy vehicular communication," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 13678–13693, Aug. 2022.

[29] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[30] T. Ariyarathna, P. Harankahadeniya, S. Isthikar, N. Pathirana, H. D. Bandara, and A. Madanayake, "Dynamic spectrum access via smart contracts on blockchain," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2019, pp. 1–6.

[31] X. Fan and Y. Huo, "Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems," *IEEE Access*, vol. 8, pp. 64486–64498, 2020.

[32] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[33] E. M. Ghourab, M. Azab, and A. Mansour, "Spatiotemporal diversification by moving-target defense through benign employment of false-data injection for dynamic, secure cognitive radio network," *J. Netw. Comput. Appl.*, vol. 138, pp. 1–14, Jul. 2019.

[34] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan./Feb. 2015.

[35] C. E. Shannon, "A mathematical theory of communication," *ACM Sigmobile Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, Jul. 2001.

[36] K. Kotobi, P. B. Mainwaring, and S. G. Bilen, "Puzzle-based auction mechanism for spectrum sharing in cognitive radio networks," in *Proc. Int. Conf. Wireless Mobile Comput. Netw. Commun.*, 2016, pp. 1–6.

[37] A. D. Wyner, "The wire-tap channel," *Bell Syst. tech.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.