SECURE BLOCKCHAINS FOR DYNAMIC SPECTRUM ACCESS

A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access

Khashayar Kotobi and Sven G. Bilén

Digital Object Identifier 10.1109/MVT.2017.2740458
Date of publication: 25 January 2018

In this article, we propose a blockchain verification protocol as a method for enabling and securing spectrum sharing in moving cognitive radio (CR) networks. The spectrum-sharing mechanism is used as a medium-access protocol for accessing wireless bandwidth among competing CRs. We introduce a virtual currency, called *Specoins*, for payment to access the spectrum. An auction mechanism based on a first-come-first-served queue is used, with the price for the spectrum advertised by each primary user in a decentralized fashion. The blockchain protocol facilitates the transactions between primary and secondary users and is used to validate and save each user's virtual wallet. Also important for mobile networks, the blockchain serves as a distributed database that is visible

1556-6072/18©2018IEEE

©ISTOCKPHOTO.COM/ BEEBRIGHT

by all participating parties, and any node can volunteer to update the blockchain. The volunteer nodes are called *miners*, and they are awarded with Specoins. We propose diverse methods to exchange the Specoins to make leasing possible even by CRs that are not miners. We show the improvement of the proposed algorithm compared with the conventional Aloha medium-access protocol in terms of spectrum usage. This difference is investigated using small-scale fading variation in the wireless channel to compare the performance of our secure method with the conventional medium access used in vehicular communications. The secure blockchain verification protocol is not only secure but also outperforms the conventional system in moderate cases of small-scale fading. In the case of severe small-scale fading, the blockchain protocol will outperform the conventional system if multipath diversity is not used.

Need for Dynamic Spectrum Access

Blockchains are distributed databases that can be securely and iteratively updated. Although the concept has been around since the early 1990s [1], only recently have applications employing blockchains been developed, primarily to facilitate secure, private financial transactions and, as a specific implementation, as Bitcoin, which has made it a well-known technology. In this article, we propose using blockchain technology to improve the medium-access protocol and security of CRs obtaining access to unused licensed spectrums.

Blockchains are used to improve the recording and sharing of financial transaction information, which can be seen in terms of increased transaction speed, decreased procedural cost, fewer transaction errors, increased general security, and a decentralized approach [2]. This decentralized method removes a central point of system failure and vulnerability to cyberattacks. For example, Bitcoin is defined by the transactions that are recorded in a blockchain, which acts as a universal ledger. Using the power of peer-to-peer calculations, a network can verify and approve each transaction and save them in this distributed database. The main idea behind blockchain usage in virtual financial transactions is that the wallet of each user is not centrally saved; rather, it is secured by storing the record of transactions between users in a blockchain.

The current paradigm of fixed wireless spectrum assignments is a major challenge facing the ever-growing demand for mobile wireless communications. To address the desire of mobile device users to be connected at all times, anywhere, and for any application, more spectrum bandwidth and/or more efficient usage of that bandwidth is needed. Many studies have shown that fixed spectrum allocations are wasteful because the license holders (which we call *primary users*) do not continuously utilize their full spectrum allocation (see the references in [3]). One method for addressing the spectrum scarcity problem, e.g., in a wireless sensor network [4], [5], is to introduce secondary users that opportunistically monitor the spectrum and then transmit their data whenever the spectrum is idle [6]. Security concerns in such sharing schemes and their corresponding medium-access protocols are current thrusts of particular research interest [7].

Security in vehicular ad hoc networks (VANETs) is a major concern because malicious users may try to attack the network. Infrastructure-based VANETs provide new private keys in real time to ensure security; however, this approach requires infrastructure and provides a central point of attack for malicious users. One proposal is to introduce certification authorities (CAs) for the VANET, with a CA responsible for each cell. The CAs provide certificates for CRs inside each cell and foreigner certificates for CRs associated with another cell when they enter its cell [8]. This approach not only requires infrastructure to be implemented for each cell but also requires a protocol for defense against central-point attacks. The other drawbacks associated with this protocol are greater calculation complexity and longer packet lengths, which increases overhead in VANETs.

In contemporary advanced vehicles, there are multiple sensors, control units, and actuators that generate data that need to be sent to the cloud over wireless links, either directly or through a vehicle's network gateway. If these elements are considered to be CRs, then they may access a shared spectrum to exchange their vital information. The shared spectrum is easy to access by a malicious attacker, and a secure medium-access communication protocol is needed to prevent cyberassaults. To analyze VANET security protocols, we use the following metrics: signature methods, the security and complexity of hash functions, transfer mechanisms, and secure multiparty functions [8]. In addition, VANETs are vulnerable to intruders in the

Auction mechanisms have been proposed as multiple-access protocols for secondary users to access unused spectrum resources.

network who may attack and take control of CAs. In this article, the trust between the CRs in a VANET is obtained using a trusted and distributed database.

Auction mechanisms have been proposed as multiple-access protocols for secondary users to access unused spectrum resources. These auctions can be separated into two categories. In a single-round auction, the available spectrum is awarded to the best bid provided by a secondary user [9], [10]. In a repeated auction, secondary users learn about the environment as well as their competitors' strategies in each round, which eventually makes the medium-access protocol very complicated.

There are a number of major drawbacks to the repeated-auction approach. First, a bidder must find an optimal strategy to maximize its long-term utility function, and, as a result, its complexity can grow exponentially [11], [12]. Some auctions will require a lot of computational power to converge to an optimal solution or a Nash equilibrium, but the required computational power is generally not feasible for ordinary CRs. Second, the computational delay is usually longer than the timescale of the small-scale fading assumed for a typical wireless channel [13], [14]. This drawback is because a CR starts calculating its bid under a specific wireless channel condition and uses that condition as its feedback information, but when the repeated auction concludes, the wireless channel has changed to a new state that may no longer reflect an optimal solution.

As mentioned, security is another major concern for medium-access protocols. Nearly all proposed medium-access protocols for CRs lack the verification and validation scheme necessary to ensure the security of the network (see [9], [15]). Generally, proposed mechanisms have not included authentication methods for validating transactions, and those that have included them have suggested centralized validation mechanisms. However, having a decentralized validation algorithm enables a medium-access protocol to be more accessible, and the implementation will be easier because there is no need for a central-authority node. Lacking a centralized node for validating a transaction and monitoring the spectrum access makes the overall system robust against single-point failures.

Overview of Blockchains

Blockchains are decentralized databases that are inherently resistant to the modification of the data contained within them. Recently, they have been proposed as a way to secure online transactions, with the most significant usage to date being Bitcoin virtual currency. The database is authenticated through the collaboration of self-interested parties. The initial use of this technology has been to share and send virtual currency safely and anonymously between users without the use of a third party like a credit-card company or bank.

The following is an example of how blockchains work: Assume that Alice wants a service from Bob in exchange for virtual currency. After agreeing on the details of the transaction, Alice's virtual wallet initiates the change in the blockchain. This results in a reduction in virtual currency in Alice's virtual wallet and an increase in Bob's virtual wallet. To validate this, other users check if Alice's virtual wallet has enough funds. Then, after validation, miners will start to make a new block to be added to the chain. This will lead to an updated blockchain.

To update the blockchain, the hash value of each transaction that occurred during a specific interval must be added into a Merkle tree. This combined hash value with the hash value of the previous block's header and a timestamp make up the new block's header. Then, the header becomes part of a puzzle that can be solved only by trial and error. A miner who finds the answer sooner is awarded with virtual currency and creates the new blockchain [16].

In this article, we take advantage of the open-source nature of blockchains to propose a secure distributed medium-access protocol for CRs to lease and access available wireless channels. In our proposed scheme, every spectrum-leasing transaction is verified and cleared, then stored within a block. The new block is linked to the previous block, forming a chain. Each block records the transactions of potentially thousands of users in such a manner that the records cannot be altered by a malicious user or users. The main features of blockchains are as follows:

- *Distributed:* Having a distributed database makes the system robust against hacker attacks. Hacking a central database is one of the main vulnerabilities of current online systems. With blockchains, there is no official centralized copy, and no user is trusted more than others.
- *Public:* There is no central authority to validate or record the data and transactions, which results in a more transparent system without a loss of security.
- *Secure:* The distributed database is encrypted via a two-key system, i.e., private and public keys. The difficulty of the encryption process is rewarded via virtual currency.
- *Permissionless:* Because there is no single trusted user as the central authority, applications can be added to the overall system without seeking the approval of other users.

In this article, we employ all of these features. We propose a distributed medium-access protocol that has no central authority and is open to any secondary user. The protocol employs a secure algorithm that stops malicious users from gaining access to the spectrum without payment. We use the permissionless property to address the security of the protocol. The proposed Specoins can be used in transactions, as a reward for mining to update the blockchain, and by secondary users to lease available spectrum owned by a primary user.

System Model and Blockchain Definition

Secondary users, who have no spectrum allocation, must access the spectrum opportunistically. Hence, the spectrum allocation and monitoring problem is defined as finding an optimal collision-free method to access the unused spectrum. Policing the CRs so they follow the protocol and act cooperatively is an important element of any proposed algorithm.

System Model

We present a network consisting of primary and secondary users. In our wireless system, primary users are spectrum license holders and can lease their allocated spectrum to increase spectrum efficiency as well as generate additional revenue. Primary users are CRs 1, 2, …, P with half-duplex transceivers, meaning they can transmit or receive at any instant of time on a specific wireless channel. The frequency spectrum is divided into R orthogonal channels $1, 2, \ldots, R$ that are symmetric and assumed to be error free. In our simulation, time is divided into $T_2, \ldots, T_n$ equal-length slots for simplicity, and $T_1 \neq T_i$ represents overhead. Furthermore, we assume that a common control channel is available for exchanging control messages between primary and secondary users. This channel is used to advertise the available channels and the auction information needed to access it. The control channel is also used to synchronize the time bases of the CRs. When the control channel is busy, e.g., when auction availability and information regarding it is being advertised, time synchronization can be achieved via other methods, such as a local global positioning system receiver. Our medium-access control frame (Figure 1) consists of information exchanges and an allocation period, as opposed to conventional overhead with an extra sensing period.

A CR that uses its processing power to update the blockchain will be rewarded in Specoins, which can then be used to lease available spectrum from a primary user. The protocol also provides a mechanism for converting between a real currency and Specoins and vice versa. This allows a cognitive secondary user with limited processing power to obtain Specoins in lieu of updating the blockchain. The currency conversion mechanism helps CRs in two major scenarios that occur in simulations and in practical applications. In the first scenario, if a CR has a large amount of data to transmit and does not have enough Specoins to lease the spectrum it needs (i.e., it has not earned enough by updating the blockchain), then it loses the opportunity to transmit that data. In the second scenario, a CR does not have sufficient processing power, battery, and/or time to update the blockchain and, as a result, also cannot transmit its data.

LACKING A CENTRALIZED NODE FOR VALIDATING A TRANSACTION AND MONITORING THE SPECTRUM ACCESS MAKES THE OVERALL SYSTEM ROBUST AGAINST SINGLE-POINT FAILURES.

Blockchain Usage in Spectrum Access

In the previous section, we defined two methods for secondary users to obtain Specoins: exchanging real currency for them and/or preparing and updating the blockchain. The main purpose of the blockchain is to record all transactions between secondary users, such as exchanging currency, mining and updating the blockchain, and leasing available spectrum through an auction.

To compare our proposed blockchain scheme with existing multiple-access techniques for accessing wireless channels, we first need to develop the metrics used to evaluate their performance. We use an approach similar to [17] to define a metric to evaluate and compare our scheme with existing protocols. The system requirements that need to be addressed for our spectrum access scheme using a Specoin blockchain include the following:

- *Scalability:* Adding additional secondary users should not significantly decrease the quality of service of the network. More primary users mean more available channels for spectrum sharing and, thus, an improved quality of service. In general, it means that our spectrum access method is able to support a large number

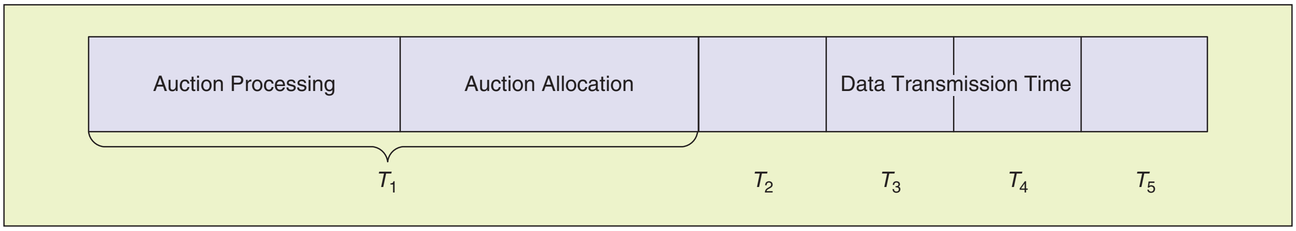

FIGURE 1 A time frame for a CR to access the available spectrum.

POLICING THE CRS SO THEY FOLLOW THE PROTOCOL AND ACT COOPERATIVELY IS AN IMPORTANT ELEMENT OF ANY PROPOSED ALGORITHM.

of primary and secondary users without impacting the quality of service.

- *Power efficiency:* Our scheme supports power efficiency by allowing the CRs to buy Specoins rather than participating in blockchain building or verification. Buying the Specoins also significantly reduces the data transmission between CRs that are sensitive to power constraints.
- *Security:* Secondary users' permission to access the spectrum must be verified. Malicious users cannot access the network without participating in an auction or paying fees. Other forms of security concerning encrypting the transmitted messages are addressed in a network layer.
- *Distributed topology:* By allocating the security verification and authentication to individual users as miners, the need for a central-authority node is removed. This results in no firewall requirement to protect single-entry-point attacks, such as denials of service.
- *Accessibility:* By introducing direct exchanges and mining as methods to earn Specoins, the network can accommodate any type of CR as a secondary user competing to access the unused spectrum. Blockchain accessibility by all users allows them to validate bids.
- *Multicasting:* A primary user does not need to advertise its available spectrum to a single entity. The need for a middleman is removed by introducing a blockchain registry. The auction advertisement is available to any interested secondary user.

In the next section, we compare our proposed medium-access protocol to conventional systems via simulation. Each simulation happens for 1,000 iterations, and the average of the results is presented in the figures. For moving vehicles, small-scale fading results in rapid variations in the received signal. We investigate this effect on our secure spectrum-sharing scheme.

Simulation Results

Method for Spectrum Allocation

Assume that a secondary user S_1's wallet, W_1^s, has enough Specoins to lease spectrum A_1 advertised by a primary user P_1. First, a puzzle mechanism similar to the one introduced in [9] is advertised by the primary user, and, if the secondary user wins the auction, the spectrum A_1 is leased by the primary user P_1 to the secondary user S_1, and the transaction is approved. Then, in a process similar to how the Bitcoin blockchain works, P_1 will generate the new block and broadcast it to all available miners (which could include S_1). The first miner, S^z, that makes the hash will be granted the ability to update the blockchain. S^z will encrypt the transaction with its private key and update the blockchain B_1. For its effort,

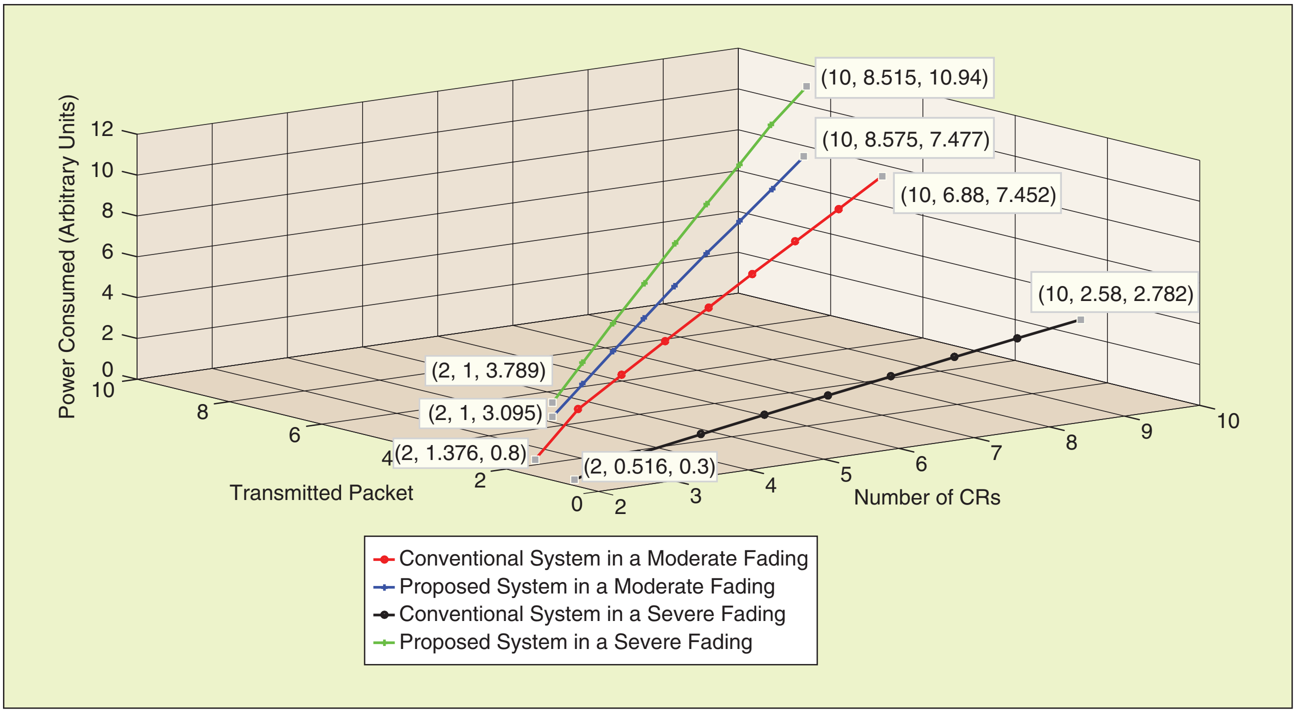

FIGURE 2 A performance comparison of data transmitted versus power consumption and the number of CRs for conventional and proposed wireless systems in severe and moderate fading conditions.

it will be rewarded in Specoins according to a cost function C. The cost function here is a function of time because, as time passes, the updating of the blockchain will require more processing power and time. Here, we define a simple cost function:

$$C_i = C_{i-1} + C_0, \tag{1}$$

where C_0 is set according to the number of participating secondary and primary users, and i represents the number of transactions so far.

Specoins can also be exchanged between users by updating the blockchain. The party that receives the Specoins will advertise the update of blockchain B_i, and the winning miner S_i will gain C_i according to (1). Before any exchange or leasing, a cognitive user decrypts the blockchain using its private key and confirms the availability of funds claimed by the CR that desires spectrum access.

In our simulation, we assume that there are n_p available primary users to provide enough available spectrum that comparison between two systems is fair. For each step, we increase the number of secondary users n_s by 1 with n_s = 10 initially and satisfy $P = n_s + n_p$, where P is the total number of players and ensuring n_p provides enough primary users so, statistically, there is not a lack of available spectrum. For each simulation campaign, the number of time slots, T, and orthogonal wireless channels, R, is the same for the conventional system and our proposed system.

In the simulations, we assume an Aloha medium-access protocol as our conventional scheme. The fading coefficients change based on a Rayleigh distribution and in a setup similar to [14]. According to the model defined in the "System Model" section, we calculated the transmitted packets for all CRs and their power consumption to make the blockchain and perform the wireless transmission. In a wireless environment with a poor fading condition, our results show that, although consuming more power, the proposed system transmits more packets compared to a conventional system using Aloha medium access (Figure 2). In more severe fading conditions, our system performs almost as well as the conventional system when there are few participating secondary users, but it outperforms as more users join the network, as shown in Figure 2, where the beginning and ending points are shown with format (number of CRs, packets transmitted, power consumed).

To more broadly investigate the impact of fading and secure spectrum sharing, we drastically altered the fading parameters in Figure 3. In this simulation setup, similar to one introduced in [14], the small-scale fading is varied with the normalized multipath fading coefficient changing from 0.2 to 1. In the first setup, the conventional multiple-access method does not use multipath-fading diversity gain (similar to [14]), and, as a result, our secure proposed system outperforms the conventional system both in terms of power consumption and packets transmitted (Figure 3). In Figure 3, we see that the conventional system can transmit more packets with lower power consumption for severe fading when the normalized fading coefficient is more than 0.7. As expected, because we are using orthogonal channels

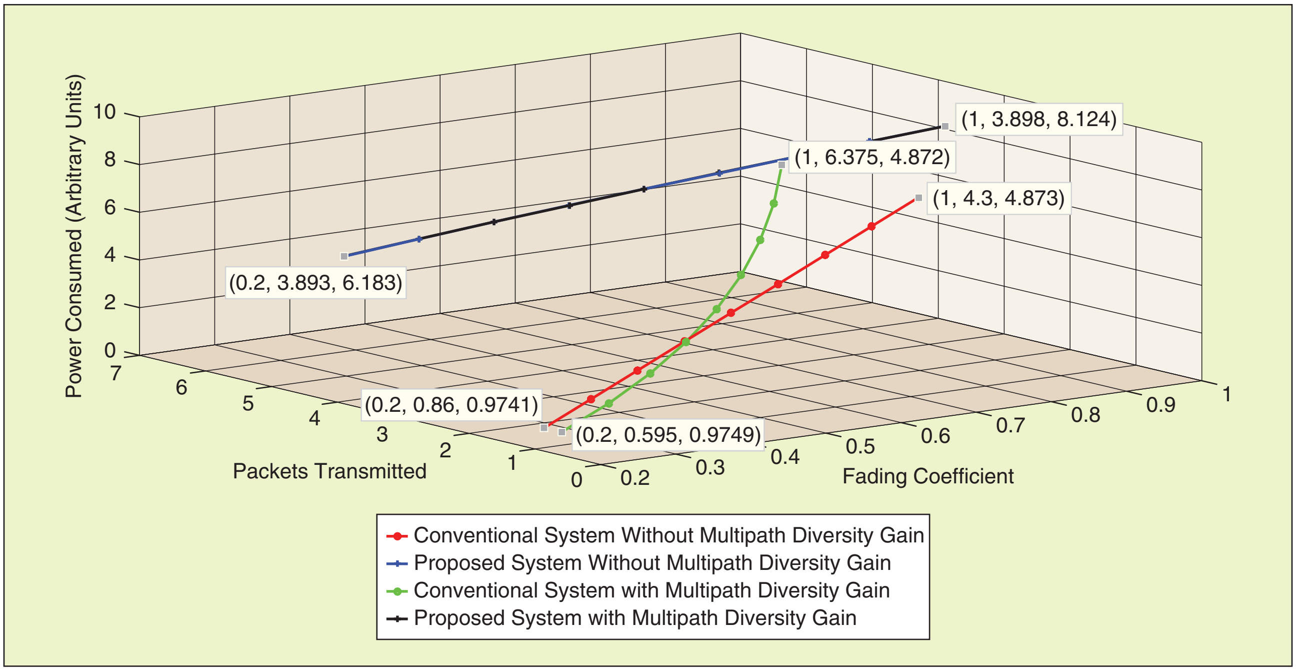

FIGURE 3 A performance comparison of data transmitted versus power consumption and the fading coefficient for conventional and proposed wireless systems with only five CRs in both systems and with a random number of available orthogonal wireless channels (seven for this simulation) with and without using multipath fading for diversity.

in our system, we do not obtain a diversity gain due to multipath fading. In Figure 3, the beginning and ending points are shown with the format (fading coefficient, packets transmitted, power consumed).

Algorithm 1 ***A secure spectrum allocation.***

```
Result: Secondary user $S_i$ accesses unused spectrum $A_j$
        owned by a primary user $P_k$
Initialization;
while $A_j$ is not used do
    Advertise $A_j$ as available spectrum;
    if $W_i^s > C_s(A_j)$ then
        $S_i \leftarrow A_j$ Request to update $B_t \leftarrow B_{t+1}$;
        Remove $A_j$ from the available spectrum pool;
    else
        Remove $S_i$ from the bidding pool;
    end
end
```

Algorithm 2 ***Updating the blockchain.***

```
Data: Block $M_t$
Result: Miner $S_k$ updates the $t+1$th iteration of blockchain,
        $B_{t+1}$
Initialization;
while hash of $M_{t+1}$ is not verified do
    Advertise new transaction $S_i \leftarrow A_j$;
    with $C(A_j)$;
    if hash of $M_{t+1}$ is correct then
        $S_k \leftarrow C(B_{t+1})$
    else
        Remove $S_i$ from the bidding pool;
    end
end
```

Algorithm 3 ***A new compressed blockchain.***

```
Data: Blockchain $B_t$
Result: Miner $S_m$ removes the unused transaction of $B_t$
Initialization;
while hash of $B_{t+1}$ is not verified do
    Advertise compressing $B_t$;
    if hash of $B_{t+1}$ is correct then
        $S_m \leftarrow C(B_{t+1})$
    else
        Remove $S_m$ from the bidding pool;
    end
end
```

Algorithms

In our simulations, we assume that CRs are following three main algorithms for securing their spectrum access. First, a secondary and primary user agree on a price for an available spectrum resource. Then, the availability of funds from the secondary user will be checked. If the secondary user has sufficient funds, it will be granted the available spectrum resource; otherwise, it will be flagged as a malicious user. After approval of the transaction, A_j, which is the spectrum resource to be leased, is removed from the available spectrum pool. This eliminates the probability of collision in our proposed algorithm. This procedure is documented in Algorithm 1.

Second, after verifying that the transaction can proceed between primary and secondary CRs, the blockchain needs to be updated. The new transaction must now be included in the blockchain. The first CR to find the correct hash of the new block, M_{t+1}, will make the new blockchain B_{t+1} and be rewarded with $C(B_{t+1})$ according to (1). After this step, the winning miner's wallet, W_l^s, will be increased by $C(B_{t+1})$ and the primary user's wallet, W_k^p, by $C_s(A_j)$, and the secondary user's wallet, W_i^s, is decreased by $C_s(A_j)$. If S_i acts maliciously and tries to guess the hash, then it will be removed from the bidding pool, similarly to the mechanism presented in [9]. This blockchain update procedure is presented in Algorithm 2.

Finally, the blockchain needs to be reset. In the context of secure spectrum sharing, we are interested in implementing a computationally simple algorithm. In contrast to building and updating the Bitcoin blockchain, which requires more computationally expensive mining, here, we reset the blockchain after a certain amount of time (e.g., daily). With Bitcoin, the total available virtual currency is limited, and, as more miners participate, the increasing complexity of the hash generation acts as a natural moderator to the Bitcoin value. However, we do not require that feature, as spectrum, unlike currency, is an expiring resource; rather, we prefer to limit overall complexity in hash generation, so we elect to periodically reset the blockchain. The blockchain reset procedure is shown in Algorithm 3. In performing a reset, a miner will put the current balances of all CRs into a new block B_{t+1}.

Comparing the Results

As shown in Figure 2, for any number of secondary users, our proposed algorithm outperforms the conventional system in terms of data transmitted. This increase in throughput comes at a cost of higher power consumption, which can be critical for a CR. Here, we can see a tradeoff between the expensive spectrum and the ability of wireless devices to store power. The same points are valid for the worse fading condition in Figure 2. Here, the improvement in terms of throughput does not start as more CRs join the network. It can be viewed as a free market in the sense that, with more secondary users participating, the new system can outperform the random access and opportunistic nature of a conventional multiple-access system, which performs well under good wireless conditions and a limited number of users.

Conclusions

In this article, we proposed using a blockchain as a decentralized database to verify and secure spectrum sharing between mobile CRs. This medium-access protocol can outperform current conventional systems in sharing available unused spectrum under both moderate and severe fading conditions. This method can be used to access available licensed spectrum resources without the need for constant spectrum sensing. Here, we focused on fading as a single parameter to distinguish different wireless channels. We have also investigated the impact of multipath small-scale fading, and, by using diversity to improve the performance of the conventional system, we showed that a conventional system may be able to outperform our secure system in terms of power consumption.

In our scheme, the primary user signals the beginning of an auction to the other parties. The winning bidder(s) use Specoins to buy that spectrum. Secondary users can earn Specoins by making the blockchain or through direct exchange. All transactions are recorded in the blockchain and updated by miners. This blockchain is then used to validate any transactions. We have shown how our proposed multiple-access scheme can improve and secure leasing of spectrum provided by a license holder. Our scheme is public, and, because it has a permissionless property, it is secure against single-point attacks. Studying the impact of other parameters of a wireless channel is a future research direction. Another is mitigating the issues related to higher power-consumption rates when there is a limitation in resources (e.g., battery, memory, processing power, and so forth).

Author Information

Khashayar Kotobi (khashi@gmail.com) received his B.S. degree in electrical engineering from the University of Tehran, Iran, in 2009 and his M.S. degree in telecommunication from the Delft University of Technology, The Netherlands, in 2011. He received his Ph.D. degree in electrical engineering from Pennsylvania State University, University Park, in 2017. He is now a data science post doc at the University of Tennessee at Chattanooga. His research interests include cross-layer design in wireless networks and dynamic resource allocation using machine-learning techniques in cognitive radio networks. He is a Member of the IEEE.

Sven G. Bilén (sbilen@psu.edu) received his B.S. degree in electrical engineering from Pennsylvania State University, University Park, in 1991 and his M.S.E. and Ph.D. degrees in electrical engineering from the University of Michigan, Ann Arbor, in 1993 and 1998, respectively. He is a professor of engineering design, electrical engineering, and aerospace engineering at Pennsylvania State University and the head of the School of Engineering Design, Technology, and Professional Programs. His research interests include software-defined radio techniques and systems, wireless sensor systems, and cognitive radio. He is a Senior Member of the IEEE.

References

[1] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in *Proc. Conf. Theory and Application of Cryptography*, 1990, pp. 437–455.

[2] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in *Proc. Int. Conf. Financial Cryptography and Data Security*, 2013, pp. 6–24.

[3] K. Kotobi, P. B. Mainwaring, C. S. Tucker, and S. G. Bilén, "Data-throughput enhancement using data mining–informed cognitive radio," *Electronics*, vol. 4, pp. 221–238, Mar. 2015.

[4] A. Sani and A. Vosoughi, "Bandwidth and power constrained distributed vector estimation in wireless sensor networks," in *Proc. Military Communications Conf. (MILCOM 2015)*, pp. 1164–1169.

[5] K. Kotobi and S. G. Bilén, "Spectrum sharing via hybrid cognitive players evaluated by an M/D/1 queuing model," *EURASIP J. Wireless Commun. Networking*, vol. 2017, p. 85, May 2017.

[6] S. Lal and A. Mishra, "A look ahead scheme for adaptive spectrum utilization," in *Proc. Radio and Wireless Conf. 2003 (RAWCON '03),* pp. 83–86.

[7] A. Shukla, A. Alptekin, J. Bradford, E. Burbidge, D. Chandler, M. Kennett, P. Levine, and S. Weiss, "Cognitive radio technology: A study for OFCOM," QinetiQ Ltd., Cody Technology Park, Farnborough, Hampshire, U.K., Tech. Rep. 830000143, 2006.

[8] G. Lee, H. Oguma, A. Yoshioka, R. Shigetomi, A. Otsuka, and H. Imai, "Formally verifiable features in embedded vehicular security systems," in *Proc. 2009 IEEE Vehicular Networking Conf. (VNC)*, pp. 1–7.

[9] K. Kotobi, P. B. Mainwaring, and S. G. Bilén, "Puzzle-based auction mechanism for spectrum sharing in cognitive radio networks," in *Proc. 2016 IEEE 12th Int. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–6.

[10] H. Li, D. Grace, and P. D. Mitchell, "Cognitive radio multiple access control for unlicensed and open spectrum with reduced spectrum sensing requirements," in *Proc. 2010 7th Int. Symp. Wireless Communication Systems (ISWCS),* pp. 1046–1050.

[11] J. Bae, E. Beigman, R. A. Berry, M. L. Honig, and R. Vohra, "Sequential bandwidth and power auctions for distributed spectrum sharing," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 1193–1203, Sept. 2008.

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

[13] Q. Zhao, B. Krishnamachari, and K. Liu, "On myopic sensing for multi-channel opportunistic access: Structure, optimality, and performance," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 5431–5440, Dec. 2008.

[14] K. Kotobi, "Energy conservation of cooperative communication over composite channels," M.S. thesis, Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, The Netherlands, 2011.

[15] K. Kotobi and S. G. Bilén, "Introduction of vigilante players in cognitive networks with moving greedy players," in *Proc. 2015 IEEE 82nd Vehicular Technology Conf. (VTC2015-Fall)*, pp. 7–8.

[16] S. Nakamoto. (2008, Oct.). Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: http://www.en.bitcoinr.cz/includes/img/bitcoin.pdf

[17] P. Pawelczak, R. V. Prasad, L. Xia, and I. G. M. M. Niemegeers, "Cognitive radio emergency networks—Requirements and design," in *Proc. 1st IEEE Int. Symp. New Frontiers Dynamic Spectrum Access Networks, 2005 (DySPAN 2005)*, pp. 601–606.

VT