# PRAM: a Practical Sybil-Proof Auction Mechanism for Dynamic Spectrum Access with Untruthful Attackers

Xuewen Dong, *Member, IEEE,* Yuanyu Zhang, *Member, IEEE,* , Yuanxiong Guo, *Senior Member, IEEE,* Yanmin Gong, *Senior Member, IEEE,* Yulong Shen, *Member, IEEE,* Jianfeng Ma, *Member, IEEE*

**Abstract**—Auction is becoming increasingly popular for dynamic spectrum access (DSA), while it is extremely vulnerable to sybil attacks. Existing studies on sybil-proof DSA auction impractically assume that attackers bid truthfully based on true appraisals. This paper, for the first time, considers untruthful attackers and investigates the sybil-proof auction design in such more hazardous scenarios. To justify the new assumption, we first show that attackers obtain higher utilities by bidding untruthfully, especially in networks with inadequate channels. Based on this novel finding, we then design a practical sybil attack model named EqualSumBid Sybil, where attackers follow an equal-sum rule (i.e., the sum bid value of the multiple identities of an attacker equals the bid value when it bids with only one identity) instead of their true appraisals. To ensure efficient DSA under the new attack, we finally propose the PRAM, a Practical sybil-pRoof Auction Mechanism, where suspicious identity merging and bid-independent bidder sorting methods are introduced to alleviate the effect of untruthfulness on spectrum auction. Furthermore, winner selection and payment methods are designed to resist the EqualSumBid Sybil attack. Theoretical analyses and numerical results show that PRAM not only resists the EqualSumBid Sybil attack but also achieves individual rationality and truthfulness.

**Index Terms**—Dynamic spectrum access, Spectrum auction, Sybil attack, Truthfulness

## 1 Introduction

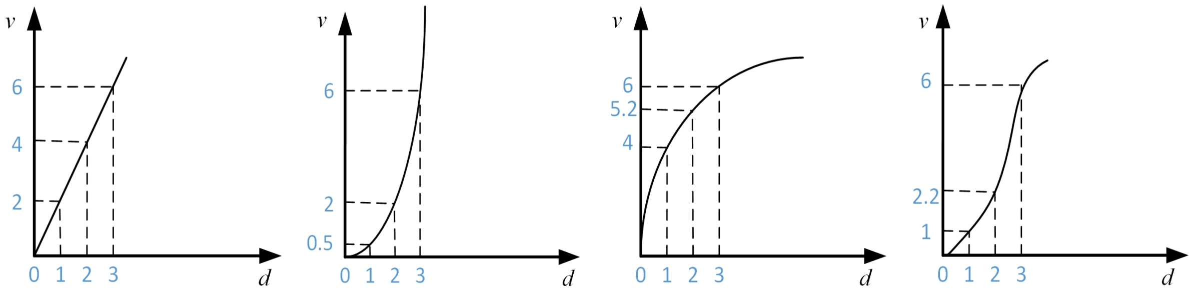
With the emergence of software-defined radios (SDR) and the explosive growth of wireless devices, radio spectrum shortage is becoming an increasingly critical issue, posing a bottleneck to the development of the wireless communication industry [1]. Dynamic spectrum access (DSA), a technology that allows primary owners to lease their unused spectrums to secondary users (SUs) for improved spectrum utilization, has been recognized as a highly promising solution to the radio spectrum shortage issue [2].

Various approaches have been adopted to address the DSA issue, among which auction has attracted considerable attentions, thanks to its high fairness. In auction, each bidder has appraisals of the goods, which represent his/her estimates on the worth of the goods and are modeled by valuation functions. A valuation function describes the amount $v$ of money a bidder is willing to pay for a certain amount $d$ of goods. Fig. 1 shows some examples of valuation functions, which can be linear, concave, convex or irregular. In a spectrum auction, the goods are spectrum channels and the bidders are SUs that request for the channels. SUs submit one or multiple bids for the channels they need according to their valuation functions. An auctioneer (usually a PU or a trustworthy third party) collects the bids from all the SUs, selects part of them as winners and charge the winning SUs an amount of payments for the channels they bid. Extensive auction-based DSA mechanisms have been proposed for various network scenarios, such as [3], [4], [5], [6]. These results show that, through proper design of auction mechanisms, unused spectrums can be effectively allocated and re-used among users, which greatly improves the spectrum utilization.

Despite its benefits, auction is vulnerable to the Sybil attack [7], [8], in which a malicious bidder (i.e., attacker) can claim multiple fictitious identities to gain more revenues. As demonstrated in recent studies [7], [9], [10], it is fairly easy for a cognitive radio user to generate multiple fictitious "names" identified by service-set identifiers (SSIDs). To counteract the Sybil attack, several recent research efforts have been devoted to the design of Sybil-proof auction mechanisms for the DSA [7] (Please see Section 2 for the detailed introduction fo these studies). Although these works represent a notable progress in the study of Sybil-proof

- *Manuscript received XXX, XX, 2020; revised XXX, XX, 2021. This work was supported in part by National Key R&D Program of China under Grant 2018YFB2100400, in part by the US National Science Foundation under grant CNS-1850523 and CNS-2029685, in part by National Natural Science Foundation of China (No. 61972310, 61941114, 61972017, 62072487), in part by Key R&D Program of Shaanxi Province (No. 2019ZDLGY12-03, 2019ZDLGY13-06). (Corresponding author: Yulong Shen, Yuanyu Zhang.)*

- *Xuewen Dong, Yuanyu Zhang, Yulong Shen are with the School of Computer Science & Technology, Xidian University, Xi'an 710071, and are with the Shaanxi Key Laboratory of Network and System Security, Xi'an 710071, China (e-mail: xwdong@xidian.edu.cn, yyuzhang@xidian.edu.cn, ylshen@mail.xidian.edu.cn).*
- *Yuanxiong Guo is with the Department of Information System and Cyber Security, University of Texas at San Antonioy, San Antonio, TX 78249, USA (e-mail: yuanxiong.guo@utsa.edu).*
- *Yanmin Gong is with the Department of Electrical and Computer Engineering, University of Texas at San Antonioy, San Antonio, TX 78249, USA (e-mail: yanmin.gong@utsa.edu).*
- *Jianfeng Ma is with the School of Cyber Engineering, Xidian University, Xi'an 710071, and is with the Shaanxi Key Laboratory of Network and System Security, Xi'an 710071, China (e-mail: jfma@mail.xidian.edu.cn).*



(a) (b) (c) (d)

Fig. 1: Valuation function examples

DSA auction mechanisms, they rely on an overly idealistic assumption that attackers and also their fictitious identities follow the valuation function rule, i.e., bid truthfully according to their true appraisals of the spectrum channels.

This assumption is arguable, because the attackers are rational and thus it is unreasonable to force them to bid truthfully. In addition, it is difficult to judge whether attackers bid truthfully or not, because the valuation functions of attackers are only known to themselves. Furthermore, an attacker may suffer from a decreased probability of winning the auction or an excessive payment for the successfully bided channels, compared with the case where he/she dose not attack, i.e., bids with only one identity. For example, suppose an attacker bids truthfully and follows the valuation function in Fig. 1(b). In the case without attack, he/she submits a bid of $6 for 3 channels. In the case with attack, he/she creates two identities and submits two bids according to the valuation function, e.g., one bid of $\$0.5$ for $1$ channel and the other of $\$2$ for 2 channels. The sum value of the bids in the attack case is $\$2.5$, which is less than the $6 in the no-attack case. As a result, the probability of winning the auction decreases, because the auctioneer prefers to assigning channels to SUs with higher bids. On the contrast, attackers that follow the valuation function in Fig. 1(c) will have a higher winning probability, while their payments may exceed the amount that they should have paid. In either case, attackers are reluctant to perform the traditional Sybil attack with truthful bidding. More importantly, as shown by the simulation results in Section 3.2 and 3.3, attackers have strong incentives to bid untruthfully (i.e., deviate from their valuation functions) as doing so can bring them more revenues, especially in networks with inadequate channels.

The above reasons motivate us to consider a more practical and hazardous DSA scenario in the presence of untruthful attackers, and investigate the design of sybil-proof auction mechanisms therein. To the best of our knowledge, this is the first paper that focuses on the design of sybil-proof DSA auction schemes with untruthful attackers. The main contributions of this paper are summarized as follows.

- This paper, for the first time, discovers that bidders (normal or malicious) can gain more revenues by bidding untruthfully, especially in networks with inadequate channels. We name this novel finding *Short-of-Channel untruthfulness* throughout this paper. Such a phenomenon exists in most of the existing auction-based mechanisms, be they sybil-proof or non-sybil-proof.
- Based on the above finding, we model a new and practical sybil attack named *EqualSumBid Sybil* to characterize the untruthful bidding strategies of attackers. In this attack, attackers deviate from their valuation functions, while the sum of the bid values from all the fictitious identities of an attacker equals the bid value when the attacker bid with only one identity. The equal sum rule is to ensure that by splitting one identity into multiple ones an attacker will not suffer from a decreased winning probability or an excessive payment.
- Existing Sybil-proof auction-based mechanisms fail to tackle the EqualSumBid Sybil attack due to the fact that the attacker's utility computation methods differ significantly between the traditional Sybil attack model and our proposed one. Therefore, to ensure efficient DSA under the new sybil attack, we propose a Practical sybil-pRoof Auction Mechanism named *PRAM*, where suspicious fictitious identity merging and bid-independent bidder sorting methods are introduced to alleviate the effect of untruthful bid values on channel allocation results. Furthermore, winner selection and payment methods are designed and combined to resist the EqualSumBid Sybil attack and avoid Short-of-Channel untruthfulness. To the best of our knowledge, we are the first to propose this intuitive and effective merging and sorting methods in Sybil-proof DSA mechanisms, and delicately design winner selection and payment methods after analyzing EqualSumBid Sybil model and Short-of-Channel untruthfulness in detail.
- We finally provide extensive theoretical analyses and numerical results to show that PRAM not only effectively counteracts the EqualSumBid Sybil attack but also achieves two critical properties, i.e., individual rationality where no bidders including the attackers obtain negative utilities, and truthfulness where bidders including the attackers can obtain the maximal utility by bidding truthfully.

The rest of the paper is organized as follows. In Section II, we briefly introduce the related works. In Section III, we present a technical auction model and our EqualSumBid Sybil attack model and also introduce the Short-of-Channel untruthfulness. We present PRAM in detail in Section IV. In Section V, we prove the individual-rationality, truthfulness and EqualSumBid Sybil-proofness of PRAM. In Section VI, the performance of our PRAM scheme is evaluated. Finally, we conclude this paper in Section VII.

## 2 Related Works

In the last few years, auction has been widely used to design incentive mechanisms for dynamic spectrum allocation (e.g. [11], [12], [13], [14], [6]). Besides individual rationality, spectrum reusability, truthfulness(i.e., strategy-proofness) are three major properties of spectrum auction mechanism.

Zhou and Zheng proposed a truthful double spectrum mechanism with spectrum reusability property and ex-post budget balance property in [13]. In [15], authors designed two payment rules suitable for the core-selecting auction, which aim to minimize the incentives of bidders to deviate from truthful telling. Huang et al. [16] present SPRING, which is the first truthful and privacy-preserving spectrum auction mechanism. Zheng et al. in [17] introduced a truthful combinatorial auction for spectrum reusability and transmission scheduling. In [18] and [19], the proposed strategy-proof auction mechanisms allow each bidder to submit a bid for a single channel. Xu et al. [20] and Wu et al. [21] presented truthful mechanisms for both single-channel and multichannel auctions. Wu et al. designed SPECIAL [22], which is a truthful and efficient multi-channel auction mechanism for wireless networks. Yang et al. [23] designed a framework for spectrum double auctions, which jointly considers spectrum reusability, truthfulness, and profit maximization without the distribution knowledge. In online spectrum auction mechanisms [24] [25], channels are arriving in a dynamic and random order, and bidders are allowed to request channels according to their demands. The above mechanisms guarantee spectrum reusability and truthful while focusing on different aspects. Our mechanism also achieves spectrum reusability and truthful.

Sybil attack is a hot topic that has attracted many researchers' interest. Jan et al. proposed a novel detection scheme for Sybil attacks in a centralized clustering-based wireless sensor network [26]. LSR [27] was introduced to detect Sybil attacks and enhance the security of a privacy-preserving Vehicular Peer-to-Peer Network. Wang et al. [28] proposed how to address a Sybil attack in Peer to peer (P2P) e-commerce applications. Zhang et al. have conducted in the Sybil attack in crowdsourcing and present countermeasures for it [29], [30]. Lin et al. proposed Sybil-proof online incentive mechanisms to deter the Sybil attack for crowdsensing in [31].

Wang et al. proposed an excellent mechanism named "ALETHEIA" in [7], [8], which is the first Sybil-proof and truthful auction mechanism for multichannel allocation. However, ALETHEIA focuses on resisting the traditional Sybil attack with truthful bidding, and did not take into account some untruthful and Sybil-attack situation according to our experiment. In this paper, we propose a practical Sybil attack model and present a truthful spectrum auction mechanism that can support spectrum reusability and resists this new kind of Sybil attack.

## 3 Model and problem formulation

### 3.1 System model

Consider a cognitive radio network with multiple heterogeneous SUs and a primary spectrum owner (PO) who owns multiple homogeneous orthogonal channels to serve its subscribed PUs. If at some time there are idle channels available, the PO can allow SUs to access these channels in order to obtain some extra profits.

In our system model, we formulate the process of multi-channel allocation as a spectrum auction, and the auctioneer is the PO that wants to share idle channels for proper benefits. We consider that the PO has a set $\mathbf{M} = \{1, ..., M\}$ of homogenous orthogonal idle channels, which can be leased to bidders. We assume that there are $N$ bidders that need to use the channels, which are all secondary users and represented as $\mathbf{N} = \{1, ..., N\}$. Generally, a large mount of secondary users are of urgent need of spectrum resources, which implies that the number of bidders $N$ far outweighs the number of idle channels $M$, and all idle channels will be leased in the end of the auction.

Due to spatial reusability, by which two SUs can share the same wireless channel simultaneously once they are well-separated (i.e., out of interference range of each other). Same to Reference [12] and [32], we adopt a SINR (signal-to-interference-plus-noise ratio) based interference model in [33] and an interference range $425m$, which is 1.7 times the outdoor transmission range ($250m$) in IEEE 802.11n. A conflict graph is utilized to simulate the interference relationships among bidders. In the conflict graph, a node represents a bidder and an edge implies that there is a pair of bidders in the interference range. Let $G =< V, E >$ denotes a conflict graph, in which $V$ is the set of bidders, and $E$ is the interference relationship between bidders. We use $N(i)$ to denote the set of interfering neighbors of bidder $i$.

For each bidder $i \in \mathbf{N}$, $i$ submits bid $\beta_i = (b_i, d_i)$ to the auctioneer, which includes the total bid value $b_i$ and the number of request channels $d_i (0 < d_i < M)$. We define $r_i$ as the unit-bid of bidder $i$,

$$r_i = \frac{b_i}{d_i}.$$

Bidder $i$ also has bidder's true valuation function $v_i()$. If bidder $i$ bids truthfully, then $b_i$ = $v_i(d_i)$. The bid profile and unit-bid profile of all bidders are $\widetilde{\beta} = (\beta_1, \beta_2, ..., \beta_N)$ and $\tilde{r} = (r_1, r_2, ..., r_N)$.

After receiving the bid profile, based on our truthful and EqualSumBid Sybil-proof auction, proposed in Section 4, the auctioneer decides the charging profile for all bidder $\widetilde{p} = (p_1, p_2, ..., p_N)$ and the allocation profile $\widetilde{A} = (A_1, A_2, ..., A_N)$, where $A_i$ is set of channels assigned to bidder $i$. $A_{N(i)}$ represents the set of channels that have been allocated to the neighbors of bidder $i$, and

$$A_{N(i)} = \cup_{j \in N(i)} A_j.$$

For each winning bidder, an allocation result returned by the auctioneer includes a price $p_i$ and an assigned channel set $A_i$, which means the winning bidder $i$ can occupy the channels in $A_i$.

The utility of bidder $i$ is

$$U_i = \begin{cases} v_i(|A_i|) - p_i, & |A_i| > 0 \\ 0, & |A_i| = 0. \end{cases} \quad (1)$$

TABLE 1: Notation Definition

| Notation | Description |
|---|---|
| **M** | The set of homogenous and orthogonal idle channels |
| **N** | The set of secondary users |
| $G$ | The conflict graph |
| $\beta_i$ | The bid profile of bidder $i$ submitted to the auctioneer |
| $b_i$ | Bid value of bidder $i$'s request |
| $r_i$ | Unit-bid value of bidder $i$'s request |
| $d_i$ | The number of bidder $i$'s request channels |
| $v_i$ | True valuation of bidder $i$ |
| $p_i$ | Price of bidder $i$ |
| $c_i$ | The critical bidder of bidder $i$ |
| $A_i$ | The assigned channel set of bidder $i$ |
| $U_i$ | Utility of bidder $i$ |
| $U_i^S$ | Utility of bidder $i$ under Sybil attack |
| $N(i)$ | The set of interfering neighbors of bidder $i$ |
| $A_{N(i)}$ | The set of channels that have been allocated to the neighbors of bidder $i$ |
| $Avai(i)$ | Available channels of bidder $i$ |
| $L$ | The sorted bidder list |
| $d_i^{\max}$ | The largest request channels' number in $N(i)$ |

### 3.2 EqualSumBid Sybil attack model

In this subsection, we analyze the shortcomings of the traditional Sybil attack model with truthful bidding and propose the EqualSumBid Sybil attack model. We will introduce our attack model under two and more fictitious identities. Then we prove that our proposed mechanism PRAM is Sybil-proof under this model in section 5.

It is noted that we assume those fictitious identities of a Sybil attacker are with the same position or coordinate in this paper. The strong "same-fictitious-coordinates" assumption mentioned above is to simplify the analysis. If a weak assumption that the fictitious identities of a Sybil attacker do not need to possess the same coordinate is adopted, then any bidder can be a fictitious identity of a Sybil attacker. Due to the large number of the bidders, there are too many cases of the fictitious identities of the attacker, making the analysis extremely complex, if not impossible. The core of the "same-fictitious-coordinates" assumption is that the fictitious bidders of a Sybil attacker have the same interference relationship as that of the original cheating bidder, which is a common requirement in the literature, such as ALETHEIA [7], [8] and [34].

The traditional Sybil attack model with truthful bids is based on a valuation function that is known only to oneself, and this function may be a straight line, convex, concave, or neither. We assume that bidder $i$ applies for $d_i$ channels. According to the valuation function $v_i()$, the bid value is $b_i = v_i(d_i)$. To gain more revenues, the cheating bidder $i$ submits two bid values under two fictitious identities $i'$ and $i''$ in a Sybil attack way, which apply for $d_{i'}$ and $d_{i''}$ ($d_i = d_{i'} + d_{i''}$) channels, respectively. If the cheating bidder $i$ can obtain more revenues by this traditional Sybil attack than bidding honestly, then this traditional Sybil attack succeeds; otherwise, it fails.

The traditional Sybil attack model requires that fictitious identities of the cheating bidder $i$ follow the valuation function to determine their bid values, that is, $b_{i'}(b_{i'} = v_i(d_{i'}))$ and $b_{i''}(b_{i''} = v_i(d_{i''}))$. As for attacking with multiple fictitious identities, they also have $d_i = d_{i_1} + d_{i_2} + ... + d_{i_n}$ and their bid values $b_{i_1} = v_i(d_{i_1}), b_{i_2} = v_i(d_{i_2})..., b_{i_n} = v_i(d_{i_n})$ respectively. So according to the valuation function, there are several cases:

$$\begin{cases} \textbf{Case 1: } b_i = v_i(d_i) > v_i(d_{i_1}) + v_i(d_{i_2}) + ... + v_i(d_{i_n}) \\ \textbf{Case 2: } b_i = v_i(d_i) = v_i(d_{i_1}) + v_i(d_{i_2}) + ... + v_i(d_{i_n}) \\ \textbf{Case 3: } b_i = v_i(d_i) < v_i(d_{i_1}) + v_i(d_{i_2}) + ... + v_i(d_{i_n}) \end{cases}.$$

For the attacker $i$ under $n$ fictitious identities, the utility is

$$U_i = U_{i_1} + U_{i_2} + ... + Ui_n, \tag{2}$$

and each fictitious identity's utility follows Eq.1.

There are some disadvantages in the traditional attack model with truthful bidding. To begin with, it is impracticable to require fictitious identities to submit truthful bids. Then, the valuation function $v_i$ is only known by bidder $i$. As a result, it is impossible to judge whether a bidder bids truthfully or not. Finally, in case 1, the Sybil attacker $i$ may worry about the decrease of being selected as a winner, because the auctioneer prefers to assign channels to higher-bided bidders. In case 3, it will lead to the risk of increased payment and decreased utility. Based on the above analysis, we believe that cheating bidders will be reluctant to perform the traditional Sybil attack with truthful bidding. They are more inclined to carry out a special kind of Sybil attack, where the total bid value does not change before (i.e., not performing EqualSumBid Sybil attack) and after the attack. On this basis, we propose a new Sybil attack model *EqualSumBid Sybil* attack, detailed in the following paragraph.

A cheating bidder $i$ performs a Sybil attack under two fictitious identities $i'$ and $i''$. The corresponding bid values are $b_{i'}$ and $b_{i''}$ without following the valuation function. Only the equation $b_i = b_{i'} + b_{i''}$ needs to be satisfied. Bid values $b_{i'}$ and $b_{i''}$ may be far away from the $v_i(d_{i'})$ and $v_i(d_{i''})$, respectively. The case 2 mentioned above is just a special case of EqualSumBid Sybil attacks. About the number of request channels, $d_i = d_{i'} + d_{i''}$ is required to be satisfied in the EqualSumBid Sybil attack model. Similarly, when an attacker $i$ performs a Sybil attack under multiple fictitious identities $i_1$, $i_2$ ... $i_n$, $b_i = b_{i_1} + b_{i_2} + ... + b_{i_n}$ and $d_i = d_{i_1} + d_{i_2} + ... + d_{i_n}$ also need to be satisfied.

Fig. 2 shows a simple attack example, in which the channel set is $\mathbf{M} = \{CH_1, CH_2, CH_3, CH_4\}$ and the bidder set is $\mathbf{N} = \{a, b, c, d, e\}$. The bidder $a$ is an attacker that tries to improve bidder's utility by EqualSumBid Sybil attack under fictitious identities $a'$ and $a''$.

It is noted that in this paper, a successful Sybil attack we discussed is under an "all-fictitious-winner" assumption that all fictitious identities are winners after allocation. There are two reasons for considering this requirement. One is that under this "all-fictitious-winner" assumption the winning attacker can be allocated with all her requested channels.

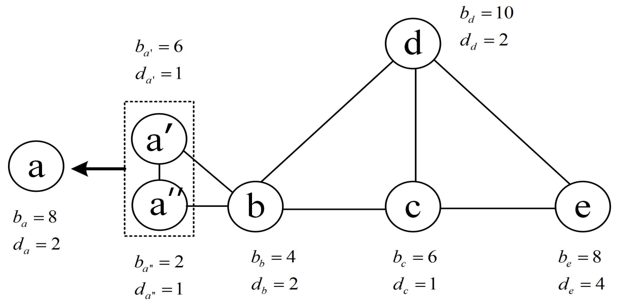


Fig. 2: An EqualSumBid Sybil attacking example of bidder $a$ under two fictitious identities.

In contrast, under the "part-fictitious-winner" assumption, only part of the fictitious are required to be the winners as long as they can increase the total utility, which means only these winning fictitious identities can be allocated channels. From this point of view, the "all-fictitious-winner" assumption result in more channels allocated to the attacker than the "part-fictitious-winner" assumption and can be regarded as a more hazardous attacker case. The other reason is that the "all-fictitious-winner" assumption can simplify the analysis and discussion. Suppose we adopt the "part-fictitious winner" assumption. Since only part of the fictitious identities is required to be the winners, the number of the cases of successful attack is $2^n - 1$, where $n$ is the number of fictitious identities. This number will increase exponentially as the number of fictitious identities increases, significantly increasing the complexity of the problem. Although the "part-fictitious winner" assumption results in a very difficult problem, we believe that the new assumption is of great importance and provide more insights into the problem. Thus, it deserves a dedicated study and will be considered in our future work.

### 3.3 Short-of-Channel untruthfulness

In addition to the EqualSumBid Sybil attack model, we discover a common type of untruthfulness exception in some traditional incentive mechanisms, which determine spectrum allocation results through bidder sorting or critical bidder finding processes. In these truthful spectrum auction schemes, it is common to find critical bidders to determine prices, such as [7], and for each winning SU $i$, $i$'s critical bidder is among $i$'s neighbors. Moreover, $i$'s bid $b_i$ is always higher than $i$'s critical bidder's bid $b_{c_i}$, with which $i$'s price $p_i$ is set. Since the main reason for this attack is that the total number of channels is inadequate, we name it a Short-of-Channel untruthfulness.

There are two kinds of successful Short-of-Channel untruthfulness. The first one will change the sorting results, which affects the allocation result when the total number of channels is less than the bidders' required quantities. We find that the proposed truthful mechanism in Ref. [7] cannot resist this kind of attack, and will present an attack example of ALETHEIA [7]. To better illustrate the attack example, we simply introduce the process of ALETHEIA at first, which is sketched as follows:

- **Bidder Ordering:** The ordered bidder list is built via constructing a Breath-First-Search (BFS) tree. The bidder with the largest per-channel bid is selected as the root node. All its conflicting neighbors becomes its children nodes, in a descending order by their per-channel bids. This construction is iterated until all bidders are included in the tree. We then obtain the ordered list by walking through the tree layer by layer from the root node to the leaf nodes and from left to right on each layer.
- **Pricing Scheme:** We first suppose that $d_i$ channels have been allocated to bidder $i$, and proceed to allocate channels to other bidders sequentially. Find out the losing neighbor bidder with the largest per-channel bid among bidder $i$'s neighbors, which is the critical bidder of bidder $i$. Compute the price for bidder $i$ with $d_i$ multiplied by the per-channel bid of bidder's critical bidder.
- **Allocation Rule:** Determine the winners according to the finally computed prices. Sequentially checks all bidders whether each bidder's bid value is greater than bidder's computed price and whether remaining channels are enough for allocation. If so, the bidder wins the request channels. Otherwise, the bidder loses with no charge.

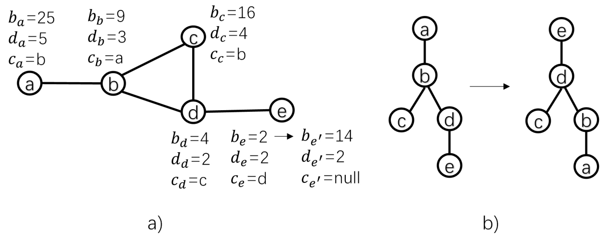


Fig. 3: A Short-of-Channel untruthfulness example changing sorting results. a)Interference graph and bid information, b)BFS trees before and after untruthful bidding

Now, we present an example to show that untruthful bidding may lead to a successful attack in ALETHIA. Suppose there are 5 bidders competing for 5 channels, and the interference graph and bid information are shown in Fig. 3(a). If all bidders bid truthfully, in the Bidder Ordering step, we can construct the BFS tree as the left one in Fig. 3(b), and obtain a sorted list $(a, b, c, d, e)$. In the Pricing Scheme step, we can deduce the critical bidders of $a$, $b$, $c$, $d$, $e$ are $b$, $a$, $b$, $c$, $d$, respectively. In the Allocation Rule step, we can obtain the first winner $a$ and the second winner $c$. If bidder $e$ bids with a untruthful bid $b_{e'}$, then the BFS tree will turn into the right one in Fig. 3(b) with a different sorted list $(e, d, c, b, a)$. The critical bidder of $e$ becomes $null$, and thus $e$ will become the first winner, launching a successful Sybil attack.

The other one happens even if the sorting result remains the same before and after the attack. In the attack example shown in Fig.4, there are two bidders $a$ and $b$ who are in the interference range of each other, and the critical bidder of $a$ and $b$ is $b$ and $null$ respectively. The total number of channels for bidding is 4, and the truthful bid profile is shown in Fig.4. Both bidder $a$ and bidder $b$ satisfy $b_i > p_i (i = a$ or $b)$. Assume that the sorting result of bidders is $(a, b)$, which means bidder $a$ will be discussed before bidder $b$ whether

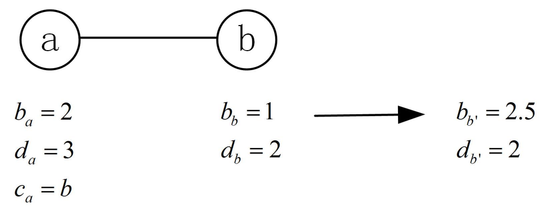


Fig. 4: A Short-of-Channel untruthfulness example without changing sorting results.

it will be selected as a winner or not. Since the number of channels is inadequate, only bidder $a$ will be selected as a winner. If bidder $b'$ bids untruthfully with $b_{b'}$, according to the same sorting result, bidder $a$'s critical bidder does not change and the price of bidder $a$ will increase. If $b_a < p_a$, then bidder $a$ loses and attacker $b'$ wins. Thus, the utility of attacker $b'$ is higher than that of truthful bidder $b$.

### 3.4 Desired Properties

In this paper, we consider the following important properties:

- **Individual rationality** In an individual rational auction, each bidder with truthful bidding has a non-negative utility. That means any bidder $i$ in the winner set pays less than bidder's valuation, $p_i \leq v_i(d_i)$.
- **Truthfulness** A mechanism is truthful if any bidder's utility is maximized when bidding with true valuation.
- **EqualSumBid Sybil-proofness** In a Sybil-proof auction, the utility of a bidder using a single identity is greater than or equal to the utility of EqualSumBid Sybil attack. That is $U_i \geq U_i^S = U_{i_1} + U_{i_2} + ... + U_{i_n}$.

## 4 PRAM

In this section, we will introduce the details of our algorithm named PRAM. The algorithm PRAM is mainly divided into three phases *bid-independent bidder sorting*, *suspicious identity merging and critical bidder finding*, and *allocation determination*.

### 4.1 Bid-independent bidder sorting

In prior spectrum allocation mechanisms, different authors sort bidders in a variety of ways. In ALETHEIA [7], the sorting algorithm is designed based on the Breadth-First-Search (BFS) procedure and per-channel bids. However, through analysis and experiments, we find ALETHEIA cannot prevent Short-of-Channel untruthfulness, and the main reason is that the increase or decrease of bidder's bid may result in a change in the sorting result.

In our *sorting* phase, to achieve truthfulness of spectrum auction mechanism, we present a bid-independent bidder sorting method, which guarantees that changing bid does not affect the sorting result and final allocation result. Bidders are sorted not according to their bids, but according to their abscissa (i.e., X-coordinate) value. A sorted bidder list is produced by sorting bidders from small abscissa to large abscissa. Please note that the key for the proposed PRAM to achieve the desired properties of truthfulness and EqualSumBid Sybil-proofness is to guarantee that the same sorted bidder list is obtained in three different cases (i.e., a bidder biding truthfully, a bidder bidding untruthfully and a bidder launching the Sybil attack) after the subsequent suspicious identity merging introduced in the next subsection. The abscissa-based sorting method we introduced can meet this requirement, while the random list cannot. Thus, from this perspective, the abscissa-based sorting method is actually different from a random list. We provide numerical results in Section 6 to show that the proposed PRAM can achieve the desired properties as long as the same sorted bidder list is obtained in the three cases.

For the same example in Fig. 2, we sort bidders from small abscissa to large abscissa in this phase and a sorted bidder list $L = \{a', a'', b, d, c, e\}$ can be obtained for bidder $a$ has the minimum abscissa. Furthermore, we calculate bidders' unit-bid profile $\widetilde{r}$ based on bidders' bids and the numbers of request channels.

### 4.2 Suspicious identity merging and critical bidder finding

In the *merging and critical bidder finding* phase, there are two steps, described in Algorithm 1. Firstly, we consider that bidders with the same coordinates are suspected of Sybil attacks and are merged into a bidder (Line 2-11 in Algorithm1). After merging, we obtain a new bidder list $L'$. Secondly, for each bidder $i$, we find $i$'s critical bidder $c_i$, and calculate an estimated price for bidder $i$ based on the unit-bid of $c_i$. If bidder $i$ is selected as a winner in the end, the estimated price will turn into the final price. Otherwise, the final price of bidder $i$ is zero.

To find the critical bidder of bidder $i$, we present a pre-allocation method mentioned in Line 24 to 37 of Algorithm 1. We assume that bidder $i$ has been allocated $d_i$ channels, and the set of available spectrum for bidder $i$ is denoted by $Avai(i)$. As a result, we remove bidder $i$ from bidder list $L'(i.e., L_i' = L' \setminus \{i\})$ and also remove $d_i$ channels from remaining channels. Under this premise, remaining bidders are sequentially pre-allocated in the order of $L_i'$.

For the first bidder $j$ in $L_i'$, we will determine whether remaining channels are enough for bidder $j$ to request (Line 27 of Algorithm 1). If the answer is yes and bidder $j$ is neighbor to bidder $i$, then we will judge whether the sum of $d_i$ and the total number of assigned channels to bidder $i'$ neighbors (the union of assigned channels of bidder $j$ and assigned channels of bidder $i$'s neighbors) is less than the total number of channels $M$ (Line 29 of Algorithm 1). If the above conditions are met, then bidder $j$ will be "pre-allocated" with required channels. Remaining bidders are also judged and pre-allocated one by one.

After that pre-allocation process is completed, the bidder with the largest unit-bid among remaining bidders is assigned as the critical bidder of bidder $i$ (Line 38 to 43 in Algorithm 1). If all of bidder $i$'s neighbors win, then the critical bidder of bidder $i$ is set as a *null* bidder with zero unit-bid.

According to line 46 in Algorithm 1, the price of bidder $i$ is set to the unit-bid of critical bidder $c_i$ times the number of request channels $d_i$. If all of the bidder $i$'s neighbors win, then $c_i$ is a *null* bidder with a zero unit-bid. In this way, allocating channels to bidder $i$ is not conflicted with

**Algorithm 1** PRAM-Merging and critical bidder finding

```
Input: The set of bidders N, the set of channels M, the bidder list $L$, the conflict graph $G$, the unit-bid profile $\widetilde{r} = (r_1, r_2, ..., r_n)$ and the bid profile $\widetilde{\beta} = (\beta_1, \beta_2, ..., \beta_n)$.
Output: The price profile $\widetilde{p} = (p_1, p_2, ..., p_n)$.

//Step1:Merging
for $i \in \mathbf{N}$ do
    for $j \in N(i)$ do
        if $i$ and $j$ have the same coordinates then
            $\beta_k = \beta_i + \beta_j$;
            $L' \leftarrow L \backslash \{i, j\}$;
            $L' \leftarrow L' + \{k\}$;
        end if
    end for
end for

//Step 2: Pre-allocation and the critical bidder finding
for $i \in \mathbf{N}$ do
    // Critical bidder finding initialization
    $c_i \leftarrow null, A_{N(i)} \leftarrow \phi$;
    $r_{c_i} = 0$;
    for $k \in \mathbf{N}$ do
        $Avai(k) \leftarrow M$;
        $L_i \leftarrow L'$;
    end for

    // Pre-allocation and the critical bidder finding
    $L_i' \leftarrow L_i \backslash \{i\}$;
    while $L_i' \neq \phi$ do
        $j \leftarrow Top(L_i')$;
        if $|Avai(j)| \geq d_j \&\& A_j = \phi$ then
            Let $S$ represent the $d_j$ channels in $Avai(j)$ with the lowest indices;
            if $j \notin N(i) || (j \in N(i) \&\& |S \cup A_{N(i)}| + d_i \leq M)$ then
                $A_j \leftarrow S$;
                for $q \in N(j)$ do
                    $Avai(q) \leftarrow Avai(q) - S$;
                end for
            end if
        end if
        $L_i' \leftarrow L_i' \backslash \{j\}$;
    end while
    for $k \in N(i)$ do
        if $A_k = \phi \&\& r_k > r_{c_i}$ then
            $c_i \leftarrow k$;
            $r_{c_i} = r_k$;
        end if
    end for

    // Price determination
    $p_i = r_{c_i} \times d_i$;
end for

Return $\widetilde{p}$;
```

other bidders' allocation, and bidder $i$ will get the cheapest estimated price. On the contrary, if the unit-bid of $c_i$ is very large, the allocation of bidder $i$ will cause a great loss, and a high estimated price will be got by bidder $i$.

In Fig. 2, $a'$ and $a''$ are suspected EqualSumBid Sybil attackers and $L' = \{a, b, d, c, e\}$ can be obtained after merging. After pre-allocation and the critical bidder finding phase, the critical bidders of $a$, $b$, $d$, $c$ and $e$ are $null$, $c$, $c$, $d$ and $c$, respectively. Then, the payments are $p_{a'} = 0, p_{a''} = 0, p_b = 12, p_d = 12, p_c = 5$ and $p_e = 24$.

### 4.3 Allocation determination

In the *allocation determination* phase, we assign channels to bidders in the winner set and return the final results, as illustrated in Algorithm 2. We allocate channels in the order of bidders in bidder list $L'$. The algorithm of the allocation part has a certain degree of similarity with the pre-allocation and the critical bidder finding phase in Algorithm 1.

For the top unallocated bidder $i$ in $L'$, if $b_i > p_i$ (Line 12 in Algorithm 2) and the number of available channels is greater than or equal to $d_i$ plus the largest number of channels requested by $i$'s neighbors (named "winner-channel-requirement" condition, in Line 13 of Algorithm 2), then bidder $i$ is selected as a winner. Remove bidder $i$ from $L'$, and iteratively execute the winner determination process until $L'$ is empty. After allocation results are determined, each winning bidder $i$'s price is set to be the product of the unit bit value of the critical bidder (i.e., $r_{c_i}$ ) and the number of bidder $i$'s requested channels. Please kindly note that merging will not change each suspicious bidder's price. If several suspicious bidders have been merged into a bidder and the merged bidder is determined as a winner, then each original suspicious bidder of the merged bidder will be regarded as an unique winner, whose price is still $r_{c_i}$ multiplied by the number of her requested channels.

It is noted that the above "winner-channel-requirement" condition in Line 13 of Algorithm 2, which is different from the allocation condition "the remaining channels being enough for allocation" in ALETHEIA , is used to prevent the Short-of-Channel untruthfulness. Without the "winner-channel-requirement" condition, truthfulness cannot be guaranteed (see more details in Lemma 3).

In addition, this condition will not affect the fairness property of PRAM very much. Instead, it will be a little helpful to increase fairness for the bidders with very large abscissa, because they are with later sequences and less priorities in the abscissa-based bidder sorting results. We conduct experiments on fairness in Fig.10 which shows that PRAM can achieve almost the same fairness as that of ALETHEIA or even higher fairness in some cases. Besides, the main properties of our proposed mechanism PRAM are truthfulness and EqualSumBid Sybil-proofness, rather than fairness. Moreover, the "winner-channel-requirement" condition only restricts whether a bidder will be determined as a winner or not. Since there are always a lot of SUs competing for channels, each channel will always be allocated to some SUs. Every bidder in the sorted bidder list will be determined once, leading to the convergence of Algorithm 2 definitely after the last bidder in the list is determined.

For the simple attack example shown in Fig. 2, the final winner set $W$ is $\{c, a', a''\}$ and the attacker $a$ is assigned with channels $CH_1$ and $CH_2$. After comparison, we find that allocation results and utilities do not change before and after the EqualSumBid Sybil attack. For the two suspicious bidders a′ and a″, both prices are $r_{c_a} * 1$, i.e., the unit-bid value of the corresponding critical bidder multiplied by the number of request channels, which are not related to their own bid values.

**Algorithm 2** PRAM-Allocation determination

```
Input: The set of bidders $N$, the set of channels $M$, the
    bidder list $L'$, the conflict graph $G$, the unit-bid profile
    $\widetilde{r} = (r_1, r_2, ..., r_n)$, the bid profile $\widetilde{\beta} = (\beta_1, \beta_2, ..., \beta_n)$
    and the price profile $\widetilde{p} = (p_1, p_2, ..., p_n)$.
Output: The winner set $W$ and allocated channel profile
    $\widetilde{A} = (A_1, A_2, ..., A_n)$.
    $W \leftarrow \Phi$
    while $i \in N$ do
3:      $Avai(i) \leftarrow M$
        for $j \in N(i)$ do
            if $d_j$ is the largest request channels' number in $N(i)$
            then
6:              $d_i^{\max} = d_j$
            end if
        end for
9:  end while
    while $L' \neq \phi$ do
        $i \leftarrow Top(L')$;
12:     if $b_i > p_i \&\& A_i = \phi$ then
            if $|Avai(i)| \geq d_i + d_i^{\max}$ then
                Let $S$ represent the $d_i$ channels in $Avai(i)$ with
                the lowest indices;
15:             Assign S to $A_i$;
                $W \leftarrow W \cup \{i\}$;
                for $j \in N(i)$ do
18:                 $Avai(j) \leftarrow Avai(j) - A_i$;
                end for
            end if
21:     end if
        $L' \leftarrow L' \backslash \{i\}$;
    end while
24: Return $W$;
```

## 5 Theoretical Analysis

In this section, we will prove the properties of PRAM which mentioned in Section III-C: *Individual rationality, Truthfulness, and Sybil-proofness.*

**Lemma 1.** *PRAM is individual rational.*

*Proof:* Obviously, according to Eq. 1, the utility of any losing bidder is 0. For each winner $i$, according to Line 12 in Algorithm 2, we have $b_i > p_i$. Therefore, $u_i \geq 0$, and PRAM is individually rational.

**Theorem 2.** *PRAM is truthful.*

*Proof:* Each bidder $i \in \mathbf{N}$ has a true valuation function $v_i(d_i)$ to determine the bid value. Bidder $i$ is untruthful when bidder $i$ requests $d_i$ channels with a cheating bid $b_i \neq v_i(d_i)$. We prove that a bidder cannot get a higher utility through submitting a cheating bid. In addition, whether a bidder have been merged with other bidders will not affect the proof this theorem, because each winning merged bidder will be demerged and each winner is unique with its own price, which is only related to $r_{c_i}$ and the number of her requested channels. Thus, whether a winner have once been merged will not affect the following proof.

TABLE 2:
Four possible auction results with truthful and untruthful bids. The sign √ means the bidder wins and the sign $X$ means he/she loses.

| Case | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| The bidder bids untruthfully | $X$ | $X$ | √ | √ |
| The bidder bids truthfully | $X$ | √ | $X$ | √ |

Four possible results of auction for one bidder when it bids untruthfully or truthfully are shown in Table I. Now, we examine these cases as follows:

- **Case 1:** Bidder $i$ does not win in the case of bids truthfully and untruthfully, resulting in the same utilities to be equal to 0.
- **Case 2:** Bidder $i$ loses when submitting a cheating bid, resulting in a zero utility. According to Eq.(1) and Line 12 in Algorithm 2, a winner will get a non-negative utility. Therefore, the untruthful bidder cannot increase bidder's utility in this case.
- **Case 3:** Bidder $i$ does not win when bids truthfully and the utility of $i$ is equal to 0. There are two different possibilities resulting the occurrence of this case. One is $b_i \leq p_i$, and the other is the inadequacy of the total number of channels, which is the Short-of Channel untruthfulness mentioned in Section 3.3. For the first one, bidder $i$ is selected as a winner when increasing bidder's bid and making $b_i' > v_i(d_i)$. According to Line 12 in Algorithm 2, we have $b_i = v_i(d_i) \leq p_i$ and $b_i' > p_i$. Hence, bidder $i$'s utility bidding with $b_i'$ is less than 0. For the Short-of Channel untruthfulness, we will prove PRAM can avoid it in lemma 3.
  As a result, bidder $i$ cannot obtain a higher utility through bidding untruthfully in this case.
- **Case 4:** Since the calculation of the price of each bidder is independent of bidder's own bid, the price will not change in both ways. The true valuation is also unchanged. According to Eq.1, bidder $i$ obtains the same utility in this case.

In sum, truthfulness can be achieved in all four cases.

**Lemma 3.** *PRAM prevents the Short-of-Channel untruthfulness.*

*Proof:* As mentioned in Section 3.3 , there are two kinds of Short-of-Channel untruthfulness. We will explain resistance proofs for them one by one.

The first kind of Short-of-Channel untruthfulness is that a SU's altering bids will change the sorting results. To preclude the possibility of this affection, in the sorting part of PRAM, we present a bid-independent bidder sorting method to avoid the first kind of Short-of-Channel untruthfulness. The same sorting results will be obtained whether the attacker changes bid value or not, which can effectively prevent this kind of Short-of-Channel untruthfulness.

As for the second kind of Short-of-channel untruthfulness, the main reason for it is the influence between neighbors. Therefore, PRAM has an additional condition in the allocation determination phase. According to the "winner-channel-requirement" condition (Line 13 in Algorithm 2) , we make sure that the number of available channels is greater than or equal to the number of bidder $i$'s request channels plus the largest request channels number of $i$'s neighbors, which can successfully eliminate the influence between neighbors.

As a result, PRAM can prevent the Short-of-Channel untruthfulness.

**Lemma 4.** *PRAM is EqualSumBid Sybil-proof under two fictitious identities.*

*Proof:* We assume that bidder $i$ conducts EqualSumBid Sybil attack with fictitious identities $i'$ and $i''$. The bids of $i'$ and $i''$ are $\beta_i' = (b_i', d_i')$ and $\beta_i'' = (b_i'', d_i'')$, respectively, where $b_i = b_{i'} + b_{i''}$ and $d_i = d_{i'} + d_{i''}$. According to the interference graph, we have $N(i) = N(i') = N(i'')$.

There are five cases to be considered.

- **Case 1:** Bidder $i$ was a winner before the attack, and both $i'$ and $i''$ are winners after the attack.

  The utility of the attacker $i$ is

  $$U_i{}^S = U_{i'} + U_{i''} = v_{i'} - p_{i'} + v_{i''} - p_{i''} = v_i - p_{i'} - p_{i''}. \tag{3}$$

  Therefore, we mainly compare the price before and after the attack. According to Line 46 in Algorithm 1, the price $p_i$ without a Sybil attack equals $r_{c_i} \times d_i$. After a Sybil attack, we have $p_i' = r_{c_i'} \times d_i'$ and $p_i'' = r_{c_i''} \times d_i''$. The total price for attacker $i$ in the Sybil attack is

  $$p_i{}^S = p_{i'} + p_{i''} = d_{i'} \times r_{c_{i'}} + d_{i''} \times r_{c_{i''}}. \tag{4}$$

  We assume the critical bidder of $i'$ and $i''$ are bidder $c_{i'}$ and bidder $c_{i''}$, respectively, and $c_{i'} < c_{i''}$, that means the index of $c_{i'}$ in the sorted list is smaller than $c_{i''}$.

  As for the fictitious identity $i'$, according to the merging and critical bidder finding phase in Algorithm 1, $c_{i'}$ must not be pre-allocated in this phase. So $c_{i'}$ does not satisfy the condition in Line 29 of Algorithm 1. As the critical bidder of a bidder must be bidder's neighbor, thus, $c_{i'}$ should satisfy

  $$|\cup_{j \in N(i'), j \le c_{i'}} A_k| + d_{i'} > M.$$

  Since $c_{i'} < c_{i''}$, the bidder $c_{i''}$ also has

  $$|\cup_{j \in N(i'), j \le c_{i''}} A_k| + d_{i'} > M,$$

  Therefore, $c_{i'}$ and $c_{i''}$ both satisfy the condition of the critical bidder of bidder $i'$. According to Line 39 in Algorithm 1, we will find the critical bidder which has the largest unit-bid, so

  $$r_{c_{i'}} = \max\{r_{c_{i'}}, r_{c_{i''}}\},$$

  Since $N(i) = N(i') = N(i'')$, we can get $|\cup_{j \in N(i''), j \le c_{i'}} A_k| + d_{i''} > M$ and $|\cup_{j \in N(i''), j \le c_{i''}} A_k| + d_{i''} > M$. The identity $i''$ also have

  $$r_{c_{i''}} = \max\{r_{c_{i'}}, r_{c_{i''}}\}.$$

  Similarly, as for $i$ before Sybil attack, we also have $|\cup_{j \in N(i), j \le c_{i'}} A_k| + d_i > M$ and $|\cup_{j \in N(i), j \le c_{i''}} A_k| + d_i > M$. That is

  $$r_{c_i} = \max\{r_{c_{i'}}, r_{c_{i''}}\}.$$

  Finally, we find that the unit-bids $r_{c_i}$, $r_{c_{i'}}$ and $r_{c_{i''}}$ are equal. According to Eq.(2) and Eq.(3), we have

  $$\tilde{p}_i = r_{c_i} \times d_i = p_i, \tag{5}$$

  and

  $$U_i = U_i{}^S$$

  .

  As a result, the attacker $i$ cannot improve $i$'s utility and the EqualSumBid Sybil attack failed. PRAM is EqualSumBid Sybil-proof in this case.
- **Case 2:** Bidder $i$ was a winner before the attack, and either $i'$ or $i''$ is a winner after the attack.

  Obviously, the attack in this case is a failure, because the attacker $i$ cannot get enough channels.
- **Case 3:** Bidder $i$ was a winner before the attack, and neither $i'$ nor $i''$ is a winner after the attack.

  In this case, both $i'$ and $i''$ are not winners, so the utility of attacker is zero after the attack, which is lower than that of it without Sybil attack. Therefore, this case fails.
- **Case 4:** Bidder $i$ was not a winner before the attack, and both $i'$ and $i''$ are winners after the attack.

  As for attacker $i$, based on the attack model, we can obtain $r_i' \le r_i \le r_i''$ or $r_i'' \le r_i \le r_i'$. According to the conclusions in case 1, we have $r_{c_i} = r_{c_{i'}} = r_{c_{i''}}$. If bidder i was not a winner before Sybil attack, we can find $b_i < p_i$ in Line 12 of Algorithm 2. Hence, we have $r_i < r_{c_i}$. Then at most one fictitious identity can be a winner, which conflicts with the assumption of case 4. Thus, this case does not exist.
- **Case 5:** Bidder $i$ was not a winner before the attack, and either $i'$ or $i''$ is a winner after the attack.

  Similar to case 2, the attacker cannot get all the required channels, so this is also a failure case of the attack.

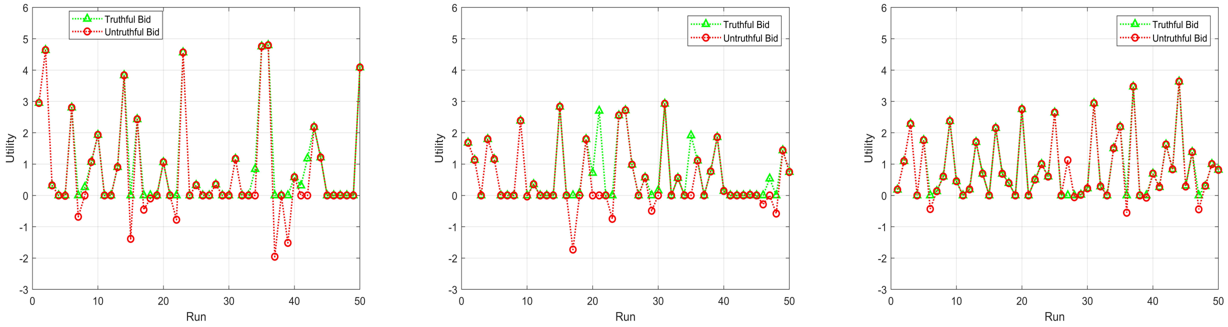
  In all, a cheating bidder cannot earn a higher utility by an EqualSumBid Sybil attack in all five cases, that is to say, PRAM is EqualSumBid Sybil-proof under two fictitious identities.

  $$U_{i'} + U_{i''} \le U_i. \tag{6}$$

**Lemma 5.** *PRAM is EqualSumBid Sybil-proof under multiple fictitious identities.*

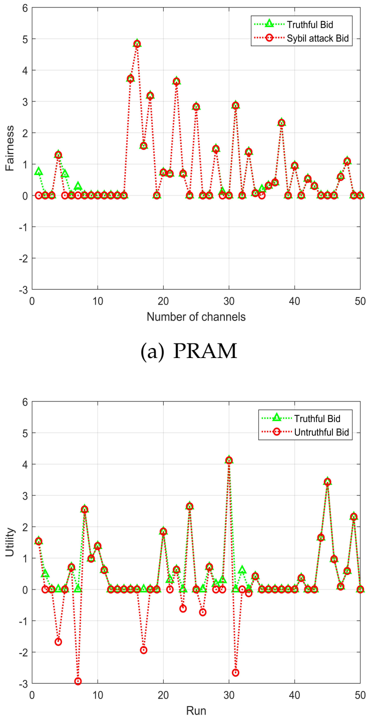
*Proof:* We will prove this lemma in a recursive way: if PRAM is EqualSumBid Sybil-proof under $n$ fictitious identities, then it is EqualSumBid Sybil-proof under $n+1$ fictitious identities. For multiple fictitious identities, we assume two identities can be merged into one identity. We take three fictitious identities case as an example to present the proving process.

For example, the attacker $i$ is divided into three fictitious identities $i_1, i_2$ and $i_3$. We assume the two of them are merged into a new identity, that is, the identities of the attacker are $i_{12}$ and $i_3$. In lemma 3, we have already proven



(a) PRAM (b) PRAM-random (c) ALETHEIA

Fig. 5: Utilities of Bidder 7 when bidding truthfully and untruthfully



(a) PRAM

(b) PRAM-random

Fig. 6: Utilities of Bidder 23 when bidding truthfully and untruthfully

that PRAM can resist the EqualSumBid Sybil attack with two fictitious identities. As a result, we can deduce that

$$U_{i_1} + U_{i_2} \leq U_{i_{12}},$$

and

$$U_{i_{12}} + U_{i_3} \leq U_i.$$

Therefore, PRAM is EqualSumBid Sybil-proof under three fictitious identities. A similar proving process can be obtained for any number of fictitious identities. As a result, PRAM is EqualSumBid Sybil-proof under multiple fictitious identities.

According to the above two lemmas, we have the following theorem.

**Theorem 6.** *PRAM is an EqualSumBid Sybil-proof mechanism.*

# 6 Performance Evaluation

In this section, we validate the truthfulness and EqualSumBid Sybil-proofness of PRAM. To better illustrate these properties, we use ALETHEIA and PRAM-random for comparison, where PRAM-random represents PRAM that results in the same random sorted bidder list when bidders bid truthfully, untruthfully or in a Sybil attack way, instead of the abscissa-based sorting method introduced in Section 4.1.

## 6.1 Simulation Setup

In our simulation, bidders are deployed following independent uniform distribution in a $2000 \times 2000$ square area. Same as in [12] and [32], the interference range is set to be $425m$, which is 1.7 times the outdoor transmission range ($250m$) in IEEE 802.11n. If the distance of two bidders' is less than the interference range, they will interfere with each other. As for $\beta_i = (b_i, d_i)$, bidders' unit-bid $r_i$ follow independent uniform distribution within $(0, 1]$, the number of occupied channels $d_i$ is randomly distributed in the range of $[0, 5]$. All results are averaged over 100 rounds at least.

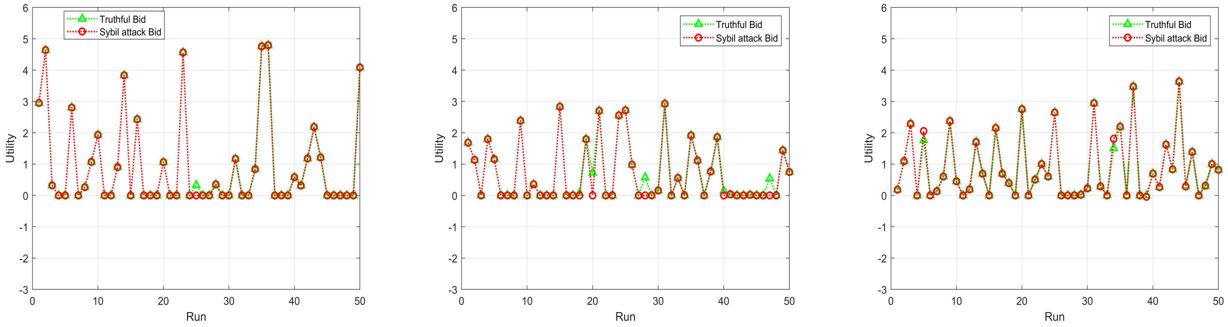
The number of channels $M$ and bidders $N$ varies from 5 to 50 and from 50 to 500, respectively. In simulations, we vary only one factor while fixing other factors.

## 6.2 Truthfulness

In this subsection, we will verify the truthfulness of PRAM and prevent the Short-of-Channel untruthfulness. That is, the attacker increase or decrease bid value ($b_i \neq v_i$) to obtain a higher utility.

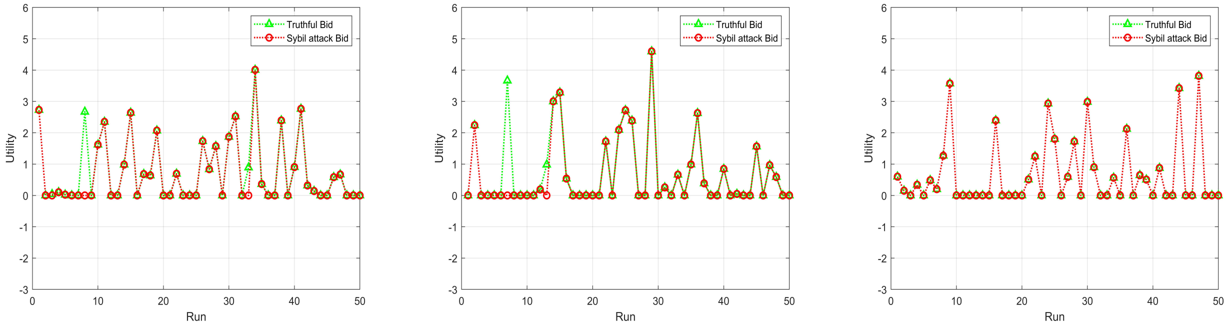
In our simulations, we randomly sample bidders and record the utilities they obtain by bidding truthful, untruthfully and after performing Sybil attack, respectively. The number of bidders in this simulation is set to 100 and the number of channels for allocation is 25.

The truthful and untruthful utilities of a randomly selected bidder (bidder 7) are shown in Fig. 5. It is noted that the bidders with different locations and bid values are randomly generated, resulting in a totally different conflict graph and a specific auction, in each round. Since the bidder



(a) PRAM (b) PRAM-random (c) ALETHEIA

Fig. 7: Utilities when bidding truthfully and under two fictitious identities EqualSumBid Sybil attack



(a) PRAM-10 meters (b) PRAM-30 meters (c) PRAM-50 meters

Fig. 8: Utilities when bidding truthfully and under two fictitious identities with different adjacent positions

7 is randomly selected from all the bidders, the results for the other bidders are similar to that of bidder 7. We can see from Fig. 5(a) and Fig. 5(b), that the utility of an untruthful bid is always lower than or equal to that of the truthful one. This means that PRAM is a truthful auction mechanism. The same experiment in Fig. 5(c) implies that there are some untruthful cases where ALETHEIA has no way to avoid this kind of attack. Fig. 5(a)-5(c) show that PRAM only beats ALETHEIA in about 20% rounds, which validates ALETHEIA is a considerably excellent mechanism. However, as long as there exists one untruthful case, ALETHEIA cannot be considered as a truthful mechanism.

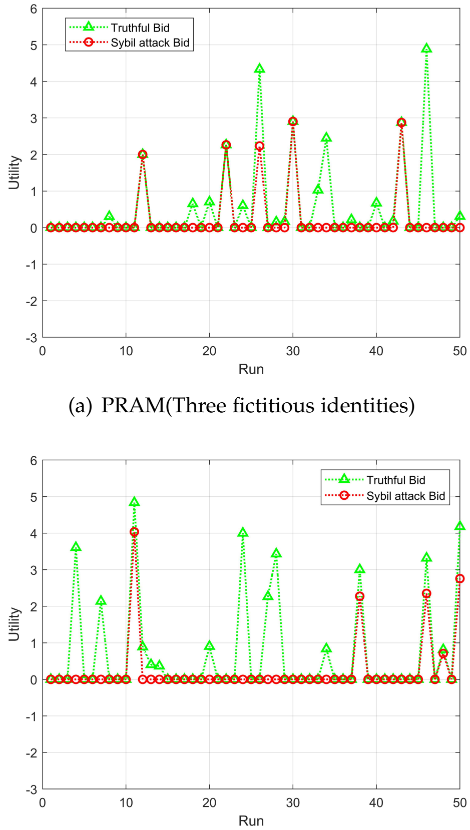
We also conduct the experiment on another randomly selected bidder (bidder 23). Similar results can be obtained in Fig. 6(a) and Fig. 6(b), which validates the truthfulness of PRAM further.

### 6.3 EqualSumBid Sybil-proofness

Fig. 7 shows the utilities of a randomly selected bidder (bidder 7). The bidder 7 performs an EqualSumBid Sybil attack by submitting two bids. Only the sum of requested channels and the sum of bid values are required no change before and after the EqualSumBid Sybil attack. From Fig. 7(a) and Fig. 7(b), we can see that the utility of Sybil attack bid is always lower than or equal to that of the truthful one. Therefore, Fig. 7(a) demonstrates that PRAM is two fictitious identities EqualSumBid Sybil-proof. The same experiment in Fig. 7(c) implies that ALETHEIA cannot prevent EqualSumBid Sybil attack well. As shown in Fig. 7(c), there are two successful attacks in 50 sets of contrast experiments. The results indicate that ALETHEIA cannot prevent EqualSumBid Sybil attack well.

In addition, we have experimentally proved that PRAM can also resist the multiple fictitious identity EqualSumBid Sybil attack in Fig. 9. We assume that the attacker is divided into three and six fictitious identities, respectively. By comparing Fig. 7(a), Fig. 9(a) and Fig. 9(b), it can be concluded that with the increasing number of fictitious identities the attacker uses, the attackers' utility goes down. In all, the experimental results show that PRAM is EqualSumBid Sybil-proof under two fictitious identities and multiple fictitious identities.

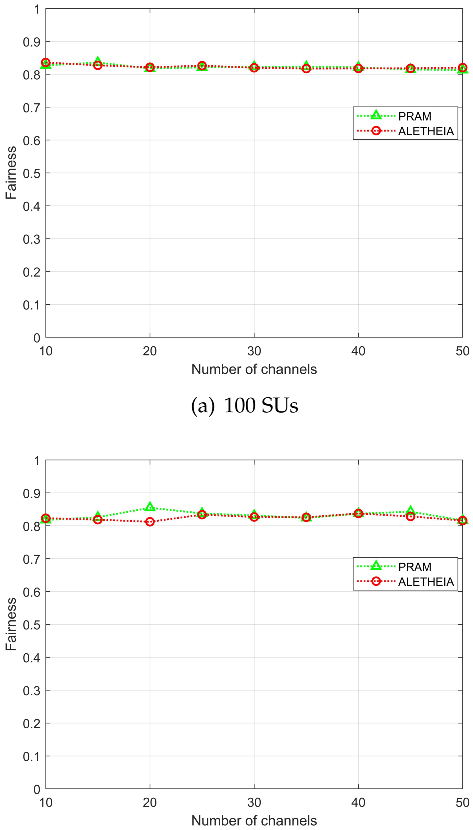
In addition, to validate that PRAM can achieve EqualSumBid Sybil-proofness without the "same-fictitious-coordinate" limitation, we conduct experiments where a randomly selected bidder performs EqualSumBid Sybil attacks under two fictitious identities with different coordinates but the same interference relationship within 10-meter, 30-meter and 50-meter ranges. The results with above settings are shown in Fig.8(a), Fig.8(b) and Fig.8(c), respectively. Similar results can be achieved under more fictitious identities, which validates that PRAM can also guarantee the EqualSumBid Sybil-proofness without the "same-fictitious-coordinate" limitation. It is noted that those fictitious identities must be in a certain range, which ensures the same neighboring relationship in the interference graph.



(a) PRAM(Three fictitious identities)

(b) PRAM(Six fictitious identities)

Fig. 9: Utilities when bidding truthfully and under multiple fictitious identity EqualSumBid Sybil attack



(a) 100 SUs

(b) 500 SUs

Fig. 10: Fairness of PRAM and ALETHEIA on the number of channels

To the best of our knowledge, we are the first to validate the Sybil-proofness without "same-fictitious-coordinate" limitation. Other mechanisms in this field are all require the "same-fictitious-coordinate" limitation explicitly or implicitly.

### 6.4 Fairness

Similar to Ref. [8], [12], we evaluate the fairness of PRAM and ALETHIA by using Jain's fairness index [35], which is defined as

$$J = \frac{(\sum_{i \in W} a_i)^2}{|W| \cdot \sum_{i \in W} a_i^2}, \tag{7}$$

where $a_i$ is the number of channels allocated to buyer $i$, and $W$ is the set of winning buyers. The index ranges from $1/|W|$ (the worst case) to 1 (the best case).

Fig. 10(a) and Fig. 10(b) show the fairness index when we vary the number of channels and set the number of SUs to 100 or 500, respectively. The fairness indices of PRAM are always near $0.82$, which are almost the same as or a little larger than those of ALETHEIA.

## 7 Conclusion

In this paper, we are the first to point out that the traditional Sybil attack model with truthful bidding is too restrictive to follow and present a practical EqualSumBid Sybil attack model. Aiming to resist this kind of Sybil attack, we propose PRAM, a practical Sybil-proof auction mechanism for multichannel allocation while achieving individual rationality, truthfulness and EqualSumBid Sybil-proofness. And we have theoretically proven the EqualSumBid Sybil-proofness of PRAM and extensively evaluated its performance. Evaluation results show that PRAM achieves truthfulness and EqualSumBid Sybil-proofness on spectrum redistribution. In our future work, the "part-fictitious-winner" assumption mentioned in Section 3.2 and the "different-fictitious-coordinates" assumption, where fictitious identities may possess different coordinates, are worthy of attention and will be discussed for studying more practical Sybil attacks.

## References

[1] M. A. Mchenry, "Nsf spectrum occupancy measurements project summary," *Shared Spectrum Company Report*, 2005.

[2] P. Klemperer, "Auctions: Theory and practice," *Economics Papers*, vol. 8, no. 1, pp. 184–184, 2004.

[3] Q. Wang, J. Huang, Y. Chen, X. Tian, and Q. Zhang, "Privacy-preserving and truthful double auction for heterogeneous spectrum," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 848–861, 2019.

[4] Y. Chen, X. Tian, Q. Wang, M. Li, M. Du, and Q. Li, "Armor: A secure combinatorial auction for heterogeneous spectrum," *IEEE Transactions on Mobile Computing*, vol. 18, no. 10, pp. 2270–2284, Oct 2019.

[5] X. Dong, T. Zhang, D. Lu, G. Li, Y. Shen, and J. Ma, "Preserving geo-indistinguishability of the primary user in dynamic spectrum sharing," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2019.

[6] X. Dong, Y. Gong, J. Ma, and Y. Guo, "Protecting operation-time privacy of primary users in downlink cognitive two-tier networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6561–6572, July 2018.

[7] Q. Wang, B. Ye, T. Xu, T. Xu, S. Guo, S. Lu, and W. Zhuang, "Aletheia: Robust large-scale spectrum auctions against false-name bids," in *ACM International Symposium on Mobile Ad Hoc NETWORKING and Computing*, 2015, pp. 27–36.

[8] Q. Wang, B. Ye, B. Tang, T. Xu, S. Guo, S. Lu, and W. Zhuang, "Robust large-scale spectrum auctions against false-name bids," *IEEE Transactions on Mobile Computing*, vol. 16, no. 6, pp. 1730–1743, June 2017.

[9] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," 06 2008, pp. 1 – 8.

[10] K. Ezirim, E. Troja, and S. Sengupta, "Sustenance against rl-based sybil attacks in cognitive radio networks using dynamic reputation system," in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, Nov 2013, pp. 1789–1794.

[11] P. Xu, X. H. Xu, S. J. Tang, and X. Y. Li, "Truthful online spectrum allocation and auction in multi-channel wireless networks," in *INFOCOM, 2011 Proceedings IEEE*, 2011, pp. 26–30.

[12] F. Wu, Q. Huang, Y. Tao, and G. Chen, "Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks," *IEEE/ACM Transactions on Networking*, vol. 23, no. 4, pp. 1271–1285, 2015.

[13] X. Zhou and H. Zheng, "Trust: A general framework for truthful double spectrum auctions," in *IEEE INFOCOM 2009*, April 2009, pp. 999–1007.

[14] Q. Wang, J. Huang, Y. Chen, C. Wang, F. Xiao, and X. Luo, "*prost*: Privacy-preserving and truthful online double auction for spectrum allocation," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 374–386, Feb 2019.

[15] Y. Zhu, B. Li, and Z. Li, "Core-selecting combinatorial auction design for secondary spectrum markets," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 1986–1994.

[16] Q. Huang, Y. Tao, and F. Wu, "Spring: A strategy-proof and privacy preserving spectrum auction mechanism," in *INFOCOM, 2013 Proceedings IEEE*, 2013, pp. 827–835.

[17] Z. Zheng, F. Wu, and G. Chen, "A strategy-proof combinatorial heterogeneous channel auction framework in noncooperative wireless networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 6, pp. 1123–1137, June 2015.

[18] Q. Huang, Y. Gui, F. Wu, G. Chen, and Q. Zhang, "A general privacy-preserving auction mechanism for secondary spectrum markets," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1881–1893, June 2016.

[19] X. Wang, Y. Ji, H. Zhou, and Z. Liu, "A privacy preserving truthful spectrum auction scheme using homomorphic encryption," in *IEEE Global Communications Conference*, 2014, pp. 1–6.

[20] P. Xu, X. Li, and S. Tang, "Efficient and strategyproof spectrum allocations in multichannel wireless networks," *IEEE Transactions on Computers*, vol. 60, no. 4, pp. 580–593, April 2011.

[21] F. Wu, Q. Huang, Y. Tao, and G. Chen, "Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks," *IEEE/ACM Transactions on Networking*, vol. 23, no. 4, pp. 1271–1285, Aug 2015.

[22] F. Wu, T. Zhang, C. Qiao, and G. Chen, "A strategy-proof auction mechanism for adaptive-width channel allocation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2678–2689, Oct 2016.

[23] D. Yang, Z. Xiang, and G. Xue, "Promise: A framework for truthful and profit maximizing spectrum double auctions," in *IEEE Infocom -ieee Conference on Computer Communications*, 2015.

[24] Y. Chen, P. Lin, and Q. Zhang, "Lotus: Location-aware online truthful double auction for dynamic spectrum access," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1092–1099, 2015.

[25] Q. Wang, Q. Sun, K. Ren, and X. Jia, "Themis: Collusion-resistant and fair pricing spectrum auction under dynamic supply," *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1–1, 2017.

[26] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A sybil attack detection scheme for a centralized clustering-based hierarchical network," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug 2015, pp. 318–325.

[27] X. Lin, "Lsr: Mitigating zero-day sybil vulnerability in privacy-preserving vehicular peer-to-peer networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 237–246, September 2013.

[28] G. Wang, F. Musau, S. Guo, and M. B. Abdullahi, "Neighbor similarity trust against sybil attack in p2p e-commerce," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 824–833, March 2015.

[29] X. Zhang, G. Xue, D. Yang, and R. Yu, "A sybil-proof and time-sensitive incentive tree mechanism for crowdsourcing," in *IEEE Global Communications Conference*, 2015, pp. 1–6.

[30] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Countermeasures against false-name attacks on truthful incentive mechanisms for crowdsourcing," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 478–485, Feb 2017.

[31] J. Lin, M. Li, D. Yang, G. Xue, and J. Tang, "Sybil-proof incentive mechanisms for crowdsensing," in *INFOCOM 2017 - IEEE Conference on Computer Communications, IEEE*, 2017, pp. 1–9.

[32] M. Cheng, X. Gong, and L. Cai, "Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3770–3779, 2009.

[33] X. Zhou, Z. Zhang, G. Wang, X. Yu, B. Y. Zhao, and H. Zheng, "Practical conflict graphs for dynamic spectrum distribution," in *Proceedings of the ACM SIGMETRICS/International Conference on Measurement and Modeling of Computer Systems*, ser. SIGMETRICS '13. New York, NY, USA: ACM, 2013, pp. 5–16. [Online]. Available: http://doi.acm.org/10.1145/2465529.2465545

[34] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting sybil attacks in wireless sensor networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042–3056, 2009.

[35] R. Jain, D. Chiu, and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," *CoRR*, vol. cs.NI/9809099, 1998.

**Xuewen Dong** received the BE, MS and PhD degrees in computer science and technology from the Xidian University of China, in 2003, 2006 and 2011, respectively. From 2016 to 2017, he was with the Oklahoma State University of USA as a visiting scholar. He is currently a professor in the School of Computer Science and Technology, Xidian University. His research interests include cognitive radio network, wireless network security and Blockchain.

**Yuanyu Zhang** (S'17–A'17–M'18) received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree from Future University Hakodate, Hakodate, Hokkaido, Japan in 2017. He is currently an Associate Professor of the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China. Before joining Xidian University, he was an Assistant Professor of the Graduate School of Science and Technology, Nara Institute of Science and Technology, Ikoma, Japan. His research interests include physical layer security, distributed ledger technology and IoT security.

**Yuanxiong Guo** (M'14, SM'19) received the B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2009, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2012 and 2014, respectively. Since 2019, he has been an Assistant Professor in the Department of Information Systems and Cyber Security at the University of Texas at San Antonio, San Antonio, TX, USA. His current research interests include data analytics, security, and privacy with applications to Internet of Things and edge computing. He is on the Editorial Board of IEEE Transactions on Vehicular Technology. He servers as the track co-chair for IEEE VTC 2021-Fall. He is a recipient of the Best Paper Award in the IEEE Global Communications Conference 2011.

**Yanmin Gong** (M'16, SM'21) received the B.Eng. degree in electronics and information engineering from Huazhong University of Science and Technology, Wuhan, China, in 2009, the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2012, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2016. She is currently an Assistant Professor at the Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX. Her research interests include security and privacy for machine learning, machine learning in wireless networks, wireless security, and Internet of things. She was a recipient of the Best Paper Award of Globecom 2017 and NSF CAREER Award 2021. She serves as the Technical Program Committee members for IEEE INFOCOM and IEEE CNS. She is serving as an Associate Editor for IEEE Wireless Communication.

**Yulong Shen** received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xian, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, and also an Associate Director of the Shaanxi Key Laboratory of Network and System Security. He has also served on the technical program committees of several international conferences, including the NANA, the ICEBE, the INCoS, the CIS, and the SOWN. His research interests include wireless network security and cloud computing security.

**Jianfeng Ma** received the BS degree in mathematics from Shaanxi Normal University, China in 1985, and the ME and PhD degrees in computer software and communications engineering from Xidian University, China, in 1988 and 1995, respectively. From 1999 to 2001, he was with the Nanyang Technological University of Singapore as a research fellow. Now, he is a professor in the School of Computer Science at Xidian University, China. His current research interests include distributed systems, computer networks, and information and network security.