Crowd-Sourced Authentication for Enforcement in Dynamic Spectrum Sharing

Vireshwar Kumar, *Member, IEEE*, He Li, *Member, IEEE*, Jung-Min (Jerry) Park, *Fellow, IEEE*, and Kaigui Bian, *Member, IEEE*

***Abstract*—The harmful interference caused by rogue radios poses a serious threat to spectrum sharing ecosystems. One approach for mitigating this problem is to adopt an enforcement scheme that can be used by an enforcement entity (e.g., Federal Communications Commission's Enforcement Bureau) to uniquely identify transmitters by authenticating their waveforms. In this approach, the enforcement entity that is authenticating the waveform is not the intended receiver, and hence it has to decode the authentication signal "blindly" with little or no knowledge of the transmission parameters. In real-world scenarios, an enforcement entity may need to cope with additional challenges, including poor signal strength of the received signals and simultaneous co-channel transmissions from multiple transmitters. In this paper, we propose a novel concept that effectively addresses some of these challenges, which we refer to as crowd-sourced blind authentication of co-channel transmitters (CBAT). We also present a concrete instantiation of this concept called frequency offset embedding for CBAT (FREE). Our results show that FREE enables the enforcement entity to blindly authenticate multiple co-channel transmitters with good accuracy by harnessing the power of crowd-sourcing.**

***Index Terms*—Dynamic spectrum sharing, enforcement, transmitter authentication, frequency offset, crowd-sourcing.**

I. Introduction

THE EXPLODING demand for radio frequency (RF) spectrum to support wireless applications has motivated spectrum regulatory agencies in industrialized countries to pursue initiatives to realize *dynamic spectrum sharing* (DSS) [2]. In the DSS paradigm, the secondary users (SUs) need to employ software-defined radios (SDRs) to harmoniously coexist with the primary users (PUs) as well as other SUs. Unlike a legacy radio, which is hardware or firmware-based, a SDR enables a user to readily re-configure its transmission parameters through changes in the code, allowing for greater flexibility. However, this "programmability" of SDRs also significantly increases the possibility of "rogue" or malfunctioning SU transmitters [3]. We define a rogue transmitter as a non-compliant transmitter that violates spectrum access rules, and causes interference to the PUs and other SUs.

The problem of rogue transmitters is an especially critical issue in the U.S.A., where spectrum sharing between federal government, including the military, systems and commercial systems will become a reality in the near future. For example, per its Report and Order (GN Docket 12-354 [4]), the Federal Communications Commission (FCC) has opened up the 3.5 GHz band to SU access, and has mandated the deployment of technologies to realize spectrum sharing between military radar systems and commercial small-cell networks. The harmful interference due to rogue transmitters poses a serious threat to the federal incumbent users, and is a major security problem that is being actively studied [5].

One viable approach for deterring rogue transmissions is to enable a regulatory enforcement entity (e.g., FCC's Enforcement Bureau) to uniquely identify transmitters by authenticating their waveforms. This *ex post enforcement* approach would enable the enforcement entity to identify an interference source and collect verifiable evidence of interference [6]. To realize *transmitter authentication*, all radios (employed in a spectrum sharing ecosystem) should be required to employ a mechanism for embedding an authentication signal—which contains the regulator-assigned identity of the transmitter—into the message signal that are transmitted. Note that the mandatory adoption of this mechanism can be incorporated as part of the radios' certification process, and it is consistent with the requirements stipulated in the FCC's Report and Order [4] for realizing spectrum sharing in the 3.5 GHz band.

To carry out transmitter authentication in DSS, an enforcement entity faces the following three real-world challenges. Firstly, the enforcement entity is considered a "blind receiver" which denotes a receiver that has little, if any, knowledge of the physical (PHY) layer parameters needed to demodulate and decode the received signals, and moreover, has no knowledge of the upper-layer protocols that is needed to interpret the decoded data correctly [7]. The enforcement entity is modeled as a blind receiver because it is *not* the intended receiver of the transmitted signals. Here, the intended receiver denotes the receiver which coordinates with the transmitter to obtain

Manuscript received November 25, 2018; revised February 27, 2019; accepted March 27, 2019. Date of publication April 2, 2019; date of current version September 9, 2019. This work was partially sponsored by the National Science Foundation (NSF) through grants 1563832, 1642928, 1822173, 1547241, and 1265886, and by the industry affiliates of the Broadband Wireless Access & Applications Center. A preliminary version of some portions of this work appeared in [1]. The associate editor coordinating the review of this paper and approving it for publication was L. Duan. *(Corresponding author: Vireshwar Kumar.)*

V. Kumar is with the Department of Computer Science, Purdue University, West Lafayette, IN 47906 USA (e-mail: viresh@purdue.edu).

H. Li and J.-M. Park are with the Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: heli@vt.edu; jungmin@vt.edu).

K. Bian is with the School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China (e-mail: bkg@pku.edu.cn).

Digital Object Identifier 10.1109/TCCN.2019.2909028

the information about the transmission parameters and protocols so that it can demodulate and decode the message signal. Secondly, the enforcement entity may need to cope with the reception of very poor-quality signals due to multipath fading and very low message signal to noise ratio (MSNR). Thirdly, the enforcement entity needs to cope with the possibility of multiple simultaneous transmissions from multiple transmitters operating in the same frequency that are located within the reception range of the enforcement entity. In such a situation, the signals received at the enforcement entity may contain multiple unique authentication signals, which need to be separated, extracted, and verified.

The vast majority of the existing PHY-layer authentication schemes [8], [9], [10], [11], [12] are designed to work only when the enforcement entity is assumed to be the intended receiver and the MSNR of the received signal is sufficiently high enough to demodulate and decode the message signal correctly. The authentication schemes proposed in [5], [7], [13] have attempted to address the problem of blind transmitter authentication. However, none of these schemes can be utilized for authentication of multiple co-channel transmitters. The PHY-layer identification framework presented in [14] enables identification of multiple co-channel transmitters by enforcing time-sharing of the available frequency channel. This time-sharing among the transmitters lowers the achievable data throughput of the transmitters. Hence, none of the schemes reported in the current literature adequately address all the three aforementioned challenges.

We assert that to realize transmitter authentication in real-world deployment scenarios, we need a network of enforcement nodes collaborating with each other. Unfortunately, deploying and maintaining a network of *dedicated* enforcement nodes for this purpose is prohibitively expensive [15]. There is a more economically viable alternative. This approach involves the use of a limited number of dedicated enforcement nodes, and the employment of a much greater number of SUs' radios that act as *non-dedicated* enforcement nodes to greatly enhance the enforcement capability of the dedicated nodes. We refer to a network of dedicated and non-dedicated enforcement nodes as a *crowd-sourced enforcement network* (CEN). In the CEN, the SUs use their spare resources to act as enforcement nodes in exchange for well-defined incentives [16].

We investigate the idea of *Crowd-sourced Blind Authentication of co-channel Transmitters* (CBAT) which refers to the mechanism of the CEN authenticating multiple co-channel transmitters by extracting the transmitters' unique and identifiable information from the received signals at the PHY layer. Specifically, we consider CBAT in a scenario where a CEN consists of a data fusion station (DFS), and a number of dedicated and non-dedicated enforcement nodes. Note that all nodes in the CEN can be considered as blind receivers. CBAT proceeds through two phases. In the first phase of CBAT, each blind receiver extracts the authentication information from its received signals, and then sends its results to the DFS. In the second phase, the DFS performs data fusion to integrate the results collected from the blind receivers to authenticate one or more transmitters whose signals have been recorded. Note that in most of the existing literature on crowd-sourcing in DSS [15], [17], no authentication/identification signal is embedded in the transmitted signal, and the crowd-sourced receivers try to detect "anomalies" in the spectrum sensing data with the aim of detecting rogue transmissions. The aim of CBAT is different; the blind receivers in CBAT extract the authentication signal that is embedded in the message signal with high accuracy under challenging conditions.

In this paper, we propose the very first instantiation of CBAT called *FREquency offset Embedding for CBAT* (FREE). In FREE, the transmitter's authentication information is embedded into the waveform as a series of controlled frequency offsets. According to our findings, FREE is very effective in addressing all of the aforementioned challenges. The main contributions of this paper are summarized as follows.

1) We propose a transmitter authentication scheme for DSS called FREE which provides high accuracy and reliability even when the received signal's quality is very poor. This is possible by harnessing the power of crowd-sourcing and collaborative processing.
2) We illustrate that FREE reliably separates and verifies authentication signals from multiple simultaneous co-channel transmissions.
3) We demonstrate the viability of FREE with simulation results as well as experimental results.

The rest of the paper is organized as follows. In Section II, we present the model, assumptions and notations utilized in this paper. We provide a high-level overview of FREE in Section III. We comprehensively describe the details of the operations at the transmitter, the blind receiver and the DFS in Sections IV, V, and VI, respectively. We analyze the performance of FREE in Section VII, and evaluate FREE by comparing with the prior art in Section VIII. Section IX presents the experimental results, and Section X concludes the paper by highlighting the main contributions.

II. Model, Assumptions and Notations

We consider a network scenario where the transmitters, intended receivers and blind receivers share the same wireless network, and are uniformly distributed in a hexagonal cell.

Transmitters: Let there be an authentic SU transmitter that is allotted a particular channel as per the rules stipulated in DSS. The transmitter transmits the message signal continuously to communicate with its intended receiver. It utilizes the cyclic prefix (CP) based orthogonal frequency division multiplexing (OFDM) for its message signal. The message signal is transmitted in frames, where each frame contains two parts—a preamble, and a message data. The preamble in each frame is utilized by the intended receivers to perform time and frequency synchronization. The message data contains the information which needs to be delivered to the intended receiver along with the information regarding the modulation and the encoding of the message data. Let there be other rogue transmitters which follow the same OFDM-based communication protocol, but cause interference to the authentic transmitter by transmitting incessantly at the same

channel. To enable transmitter authentication, every transmitter adopts a mechanism for embedding its authentication signal into its message signal. The tamper-resistance techniques are employed to deter malicious users from circumventing or altering the embedding process carried out by the transmitter's radio [18].

Intended Receivers: The intended receivers readily extract the preamble and the message data from each frame, and demodulate and decode the message data. The intended receivers are not required to alter their conventional message signaling procedure even after embedding of the authentication signal in FREE. Hence, we do not discuss the specific details related to the intended receivers in this paper.

Blind Receivers: The blind receivers are aware of the fact that OFDM is employed by the transmitters to modulate and transmit the message signals in frames. The blind receivers also know the sampling frequency, the length of the Fast Fourier Transform (FFT), and the length of CP utilized in the transmitted signals. These parameters are typically standardized as part of the air-interface standard, e.g., IEEE 802.11g. The blind receivers receive signals with multipath Rayleigh fading and at a very low MSNR (e.g., below 0 dB). The multipath propagation is modelled as a tapped delay line [19]. In such a case, the message data in each frame cannot be processed by the blind receivers. This means that the blind receivers cannot obtain the information (e.g., modulation and channel coding techniques) that is required to demodulate and decode the message signal.

DFS: The DFS utilizes polling-based protocol on a secondary channel (with good MSNR) with the blind receivers to obtain the results of the authentication information extraction procedures at the blind receivers. Further, let there be a fine-grained clock synchronization between each of the blind receivers and the DFS. This can be facilitated by the DFS using the conventional techniques, e.g., distributed primary reference clock and packet-based time synchronization [20], [21].

Adversary: We assume that a conventional digital signature scheme is utilized to generate the authentication data, and the adversary does not know the key used to generate the signature. This means that the adversary cannot successfully launch attacks, such as, tampering with the authentication data, impersonation attacks and replay attacks. However, the adversary attempts to perturb the authentication mechanism by tampering with the data fusion procedure at the DFS.

Notations: In this paper, we assume that in a particular communication channel, the number of transmitters is represented by N_t. The i^{th} transmitter is represented by $\mathsf{Tx_i}$, where $i \in [1, N_t]$. Also, there are N_b blind receivers receiving the signals in the communication channel. The j^{th} blind receiver is represented by $\mathsf{BRx_j}$, where $j \in [1, N_b]$. A parameter represented by x_{ik} corresponds to k^{th} frame of the $\mathsf{Tx_i}$, and a parameter represented by $\widehat{x}_{jik}$ corresponds to the estimate of the parameter x_{ik} at the $\mathsf{BRx_j}$. We also utilize the notation $\boldsymbol{x}[\mathrm{n}]$ to represent the n^{th} element of the sequence $\boldsymbol{x}$. We utilize the values of the parameters given in Table I (unless stated otherwise) for generating the simulation and experimental results in this paper. These parameter values are obtained from [22], and used in conventional OFDM-based 802.11 systems.

TABLE I
NOTATIONS AND VALUES OF PARAMETERS USED TO OBTAIN SIMULATION AND EXPERIMENTAL RESULTS

Notation	Description	Value
F_s	Sampling frequency	5 MHz
L_t	Taps in multipath Rayleigh fading channel	10
K_a	Length of authentication signal	512
K_r	Frames used in computing decision variable	10
N_a	Number of OFDM symbols in each frame	40
N_b	Number of blind receivers	1
N_c	Length of CP in each OFDM symbol	16
N_f	Length of FFT in each OFDM symbol	64
N_o	Number of samples in a frame	3200
N_t	Number of transmitters in a band	1
M_a	Order of modulation of authentication data	2
M_i	Order of modulation of message data	4
R_i	Rate of convolution coding of message data	1/2
f_a	FO parameter set by the DFS	2.5 kHz
f_{aik}	EFO in the k^{th} frame at $\mathsf{Tx_i}$	$\pm$2.5 kHz
ω_{mj}	Trustworthiness weight of $\mathsf{BRx_j}$	1

III. OVERVIEW OF FREE AND OUR CONTRIBUTIONS

We propose a concrete instantiation of the CBAT concept called FREquency offset Embedding for CBAT (FREE). FREE addresses all of the following three challenges: (1) authenticating received signals with minimal knowledge of the PHY-layer transmission parameters; (2) authenticating received signals with multipath fading and very low MSNR; and (3) authenticating signals emitted simultaneously from multiple co-channel transmitters. Here, we provide an overview of the operations at each of the entities in FREE, and highlight our contributions in this paper.

In FREE, the transmitter carries out four major operations. Firstly, the transmitter generates a sequence of frames of the message signal using the conventional OFDM procedures employed in modern communication systems. Secondly, it generates the authentication signal which contains the transmitter's authentication data. This procedure plays a pivotal role in FREE because the DFS verifies the authentication data to uniquely identify the transmitter. The authentication data, at a minimum, contains information that enables the enforcement entity to determine the regulator-assigned identity of the transmitter as well as the regulator-imposed spectrum access constraints, in terms of frequency, spatial, and temporal domains. Thirdly, the transmitter embeds the authentication signal into the message signal by modifying the frequency offset (FO) of each frame of the message signal. The frequency offset is induced in such a way that the authentication signal does not interfere with the decoding process of the message signal at the intended receivers. Lastly, the transmitter transmits the embedded signal using the RF front-end procedures.

At the blind receiver in FREE, there are four major operations. Firstly, the blind receiver down-converts and samples the received signal. Then, it computes a decision variable by calculating the auto-correlation induced due to the repetition of the training samples in the preamble. Secondly, with

the decision variable, the blind receiver utilizes a heuristic algorithm proposed in this paper to determine the number of transmitters and the location of the start of the received frames from the transmitters. This is an important step which enables FREE to address the third challenge of detecting multiple co-channel transmitters. Thirdly, for each detected transmitter, the blind receiver estimates the frequency offset embedded into the frames of the message signal by utilizing the correlation between the CP samples and the corresponding data samples of the OFDM symbols. Note that the frequency offset of a frame is estimated at the blind receiver with only limited knowledge about the transmission parameters. In this way, FREE addresses the first challenge of blind authentication of the transmitters. The blind receiver also estimates the time of arrival of the received frames and the signal to interference and noise ratio of the received frames. Finally, the blind receiver communicates the estimated values to the DFS.

At the DFS, there are four major operations. Firstly, from the reported values of the time of arrival of the received frames at the blind receivers, the DFS synchronizes the reported data in time, and estimates the total number of transmitters in the frequency channel. Secondly, for each transmitter, the DFS aggregates the values of the estimated frequency offsets reported from multiple blind receivers. In this aggregation procedure, the DFS utilizes the "trustworthiness" weights of the blind receivers to differentiate between an honest blind receiver which is reporting honest values of frequency offsets, and a rogue blind receiver which is reporting wrong information to the DFS. Thirdly, the DFS utilizes the aggregated frequency offsets to estimate the authentication signal, and verify the validity of the authentication data. The collaboration of the blind receivers enabled by the DFS significantly improves the error performance of the estimated authentication signal, and addresses the aforementioned second challenge of robust authentication at very low MSNR. Finally, after each successful verification, the DFS utilizes a heuristic algorithm proposed in this paper, and updates the trustworthiness weights of the blind receivers by comparing their reported frequency offsets to the true frequency offsets generated from the verified authentication signal.

In the following three sections, we provide elaborate technical details of the operations performed at the three entities.

IV. Operations at the Transmitter in FREE

A. Generate Frames of the Message Signal

The $\mathsf{Tx_i}$ generates the frames of the message signal using the conventional OFDM signaling with length of FFT represented by N_f and length of CP represented by N_c. The message data bits are encoded using a convolution code of rate R_i, and modulated to message data symbols using the quadrature amplitude modulation (QAM) of order M_i. Also, the preamble is generated by employing the conventional structure utilized in standards, e.g., IEEE 802.11g and IEEE 802.11af [22]. It consists of 10 repetitions of a set of short training samples, a CP guard interval, and two repetitions of a set of long training samples. The number of samples in the set of short training samples is equal to $N_f/4$; in the CP guard interval is equal to $N_f/2$; and in the set of long training samples is equal to N_f. The preamble (with the total length of four OFDM symbols or $5{\cdot}N_f$ samples) is appended at the start of the OFDM symbols with the message data. The total number of OFDM symbols in a frame is represented by N_a, and the total number of samples in a frame is given by $N_o = N_a \cdot (N_f + N_c)$. The sequence of the samples in k^{th} frame is represented by $\boldsymbol{s}$.

B. Generate the Authentication Signal

The $\mathsf{Tx_i}$ generates an authentication data, represented by $\{T_{si}, I_i, F_c, L_i, T_{hi}, \pi_i\}$, which contains a time-stamp, represented by T_{si}; a regulator-assigned identity of the $\mathsf{Tx_i}$, represented by I_i; a frequency channel allowed for transmission, represented by F_c; a registered location of the $\mathsf{Tx_i}$, represented by L_i; a time-interval of operation authorized by the regulator, represented by T_{hi}, and a digital signature, represented by π_i. The signature π_i is generated using the Elliptic Curve Cryptography (ECC) based digital signature scheme [23], [24]. The authentication data is encoded using a channel coding scheme to correct the bit inversion errors and erasures. Finally, a sequence of authentication synchronization bits is appended to generate the authentication signal, represented by $\boldsymbol{a}$.

C. Embed the Authentication Signal Into the Message Signal

We propose the following methodology to generate the embedded frequency offset (EFO) based on the authentication signal, and then embed the EFOs into the message samples.

1) Modulate Authentication Signal: We utilize a technique called *F*rame *F*requency *M*odulation (FFM) where the frequency offset of each frame of the message signal is modified (modulated) according to the authentication signal. FFM of order M_a (represented by M_a-FFM) is represented by a set of M_a possible frequency offsets corresponding to $M_a = 2^q$ possible q-bit authentication symbols. Here, an authentication symbol is defined as a set of q authentication bits, and is obtained by using q-bit Gray code. The set of EFOs in M_a-FFM can be represented by $\{f_p\}$ such that

$$f_p = f_a \cdot \left(1 - 2 \cdot \frac{p-1}{M_a - 1}\right), \tag{1}$$

where $p = 1, 2, \ldots, M_a$, and f_a is the maximum positive EFO that can be used to embed the authentication signal into a frame of the message signal. The values of M_a and f_a are set by the DFS and utilized by all the transmitters. These values play an important role in determining the robustness of the embedded authentication signal against noise (see Section VII-B1). Figures 1(a) and 1(b) illustrate the mapping schemes for 1-bit authentication symbols and 2-bit authentication symbols, respectively.

2) Embed Authentication Signal: We assume that the number of authentication symbols obtained by modulating the authentication signal is represented by K_a. In FREE, one authentication symbol is embedded into one frame of the message signal by inducing the corresponding EFO from the set of EFOs in the FFM. In the k^{th} frame, where $k \in [1, K_a]$, the EFO is denoted by f_{aik}. The samples of the k^{th} frame

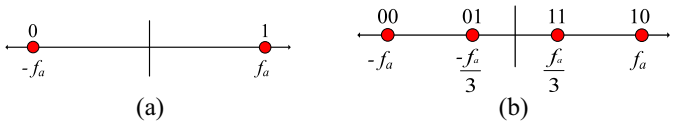

Fig. 1. Mapping of authentication bits to EFO in M_a-FFM. (a) $M_a = 2$. (b) $M_a = 4$.

of the embedded signal (i.e., the message signal embedded with the authentication signal in the baseband) is computed as $\boldsymbol{e}[n] = \boldsymbol{s}[n] \cdot e^{\mathrm{j}2\pi \frac{f_{aik}}{F_s} n}$, $\forall n \in [0, N_o - 1]$, where F_s is the sampling frequency.

D. Transmit the Embedded Signal

The embedded signal is up-converted to the carrier frequency F_c and transmitted. Assuming that the FO induced due to the inaccurate oscillator at the $\mathsf{Tx_i}$ is represented by f_{ti}, the samples of the k^{th} frame of the transmitted signal in the baseband are given by $\boldsymbol{x}[n] = \boldsymbol{e}[n] \cdot e^{\mathrm{j}2\pi \frac{f_{ti}}{F_s} n}$, $\forall n \in [0, N_o - 1]$.

V. Operations at the Blind Receiver in FREE

A. Down-Convert, Sample and Compute the Decision Variable

The $\mathsf{BRx_j}$ down-converts and obtains N_r discrete samples of the received signal at the carrier frequency F_c. The n^{th} sample of the received signal is represented by

$$\boldsymbol{r}[n] = \boldsymbol{y}[n] \cdot e^{\mathrm{j}2\pi \frac{f_{rj}}{F_s} n} + z, \tag{2}$$

where f_{rj} represents the FO induced due to the inaccurate oscillator at the $\mathsf{BRx_j}$, and z represents the complex Gaussian noise with zero mean and variance equal to σ_z^2. Also, the signal $\boldsymbol{y}$ is computed as $\boldsymbol{y} = \sum_{i=1}^{N_t} \boldsymbol{h} \otimes \boldsymbol{x}$, where $\otimes$ represents the convolution between coefficients of the L_t-tap Rayleigh fading channel $\boldsymbol{h}$, and the transmitted signal in the baseband $\boldsymbol{x}$.

Further, considering $\widetilde{\alpha}$ as the assumed start of the first frame in the received signal, the $\mathsf{BRx_j}$ segments the received samples into K_r frames, where $K_r = \lfloor \frac{N_r - \widetilde{\alpha}}{N_o} \rfloor$. Here, $\lfloor v \rfloor$ denotes the largest integer less than or equal to v. For each $k \in [1, K_r]$, the auto-correlation induced due to the repetition of the short and long training samples in the preamble [25] is computed as $P_{k\widetilde{\alpha}}$. For each $\widetilde{\alpha} \in [0, N_o - 1]$, a decision variable is obtained by computing the average of the auto-correlation over the K_r frames as $\boldsymbol{\Psi_j}[\widetilde{\alpha}] = \frac{|\sum_{k=1}^{K_r} P_{k\widetilde{\alpha}}|}{K_r}$, where $|v|$ denotes the absolute value of v. Note that to perform real-time processing, an intended receiver traditionally utilizes the individual value of the auto-correlation in each frame for synchronization. However, this mechanism is not suitable for synchronization at very low MSNR. In FREE, the averaging over multiple frames enables the $\mathsf{BRx_j}$ to robustly estimate the frame boundaries at very low MSNR.

Figure 2 shows an example which illustrates the values of the decision variable corresponding to different values of the assumed start of the first frame $\widetilde{\alpha}$ when the signals from two co-channel transmitters are received at the $\mathsf{BRx_j}$. The MSNRs of the signals from two transmitters are equal to 0 dB and -3 dB. Other PHY-layer parameters for generating the transmitted signals are shown in Table I. In this figure, we observe that there are two conical hills at $\widetilde{\alpha} = 500$ and $\widetilde{\alpha} = 1000$ corresponding to the signals from two transmitters. We also note that the width of the hill is equal to the length of the preamble, i.e., $5 \cdot N_f$ samples.

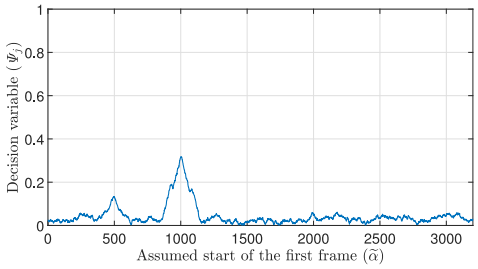

Fig. 2. Decision variable vs. assumed start of the first frame.

Algorithm 1 Transmitter Detection Algorithm

1) Set $i = 1$, and $\boldsymbol{\Lambda_{ji}} = \boldsymbol{\Psi_j}$.
2) Compute a mean value, $\lambda_{ji} = \frac{\sum_{\widetilde{\alpha}=0}^{N_o-1} \boldsymbol{\Lambda_{ji}}[\widetilde{\alpha}]}{N_o}$, and set a threshold, $\tau = 2 \cdot \lambda_{ji}$.
3) Compute $\widehat{\beta}_{ji} = \mathrm{argmax}_{\widetilde{\alpha}}\, \boldsymbol{\Lambda_{ji}}[\widetilde{\alpha}]$.
4) If $\boldsymbol{\Lambda_{ji}}[\widehat{\beta}_{ji}] > \tau$, set $\widehat{\beta}_{ji}$ as the start of the frame from i^{th} transmitter; otherwise, set $\widehat{N}_{tj} = i - 1$ and exit. In this step, the $\mathsf{BRx_j}$ detects a transmitter and a corresponding peak in the values of $\boldsymbol{\Psi_j}$.
5) Set $\boldsymbol{\Lambda_{j(i+1)}} = \boldsymbol{\Lambda_{ji}}$.
6) Set $\boldsymbol{\Lambda_{j(i+1)}}[\widetilde{\alpha}] = \lambda_{ji}$, for each $\widetilde{\alpha} = [\widehat{\beta}_{ji} - 5 \cdot N_f/2 + 1, \widehat{\beta}_{ji} + 5 \cdot N_f/2]$. Here, the $\mathsf{BRx_j}$ removes the peak and the corresponding hill by setting their values equal to the mean value.
7) Set $i = i+1$ and go back to Step 2.

B. Detect Transmitters and Their Frame Boundaries

Driven by the observations from Figure 2, we propose Algorithm 1 to detect the number of transmitters, represented by $\widehat{N}_{tj}$; and the start of the first received frame from the transmitters, represented by $\widehat{\beta}_{ji}$, for all $i \in [1, \widehat{N}_{tj}]$.

Algorithm 1 detects multiple transmitters by detecting multiple conical hills in the values of $\boldsymbol{\Psi_j}$. For each detected transmitter, $i \in [1, \widehat{N}_{tj}]$, the number of frames received at the $\mathsf{BRx_j}$ is obtained as $\widehat{K}_{rj} = \lfloor \frac{N_r - \widehat{\beta}_{ji}}{N_o} \rfloor$, and the samples corresponding to the k^{th} frame are represented by

$$\boldsymbol{u}[n] = \boldsymbol{r}\Big[k \cdot N_o + \widehat{\beta}_{ji} + n\Big], \ \forall n \in [0, N_0 - 1]. \tag{3}$$

C. Estimate the Parameters

For each frame of each detected transmitter, the $\mathsf{BRx_j}$ estimates the following three parameters.

1) Time of Arrival: Let the $\mathsf{BRx_j}$ start the detection at time represented by T_{rj}. Hence, the time of arrival of the k^{th} frame of the i^{th} transmitter, represented by $\widehat{t}_{jik}$, is computed

as $\widehat{t}_{jik} = T_{rj} + T_s \cdot \widehat{\beta}_{ji} + T_s \cdot N_o \cdot k$, where T_s is the sampling time which is computed as $T_s = 1/F_s$.

2) Embedded Frequency Offset: Note that the true frequency offset of the received signal at the $\mathsf{BRx_j}$ from the $\mathsf{Tx_i}$ is given by $f_{ojik} = f_{aik} + f_{ti} + f_{rj}$. Hence, the frequency offset in the frame of the message signal has one constant part, represented by $f_{mji} = f_{ti} + f_{rj}$, and a variable part, given by the EFO f_{aik}. Through the following steps, the $\mathsf{BRx_j}$ obtains the estimate of f_{mji}, represented by $\widehat{f}_{mji}$, and the estimate of f_{aik}, represented by $\widehat{f}_{jik}$. For each frame, the $\mathsf{BRx_j}$ computes the auto-correlation induced due to the repetition of samples in the CP samples and the corresponding data samples as

$$P_f = \frac{1}{N_a \cdot N_c} \sum_{l=0}^{N_a-1} \sum_{n=0}^{N_c-1} \boldsymbol{u}^*\big[l \cdot \big(N_f + N_c\big) + n\big] \times \boldsymbol{u}\big[l \cdot \big(N_f + N_c\big) + N_f + n\big]. \quad (4)$$

The frequency offset for k^{th} frame is estimated as $\widehat{f}_{ojik} = \frac{F_s}{2\pi N_f} \angle P_f$, where $\angle\, v$ denotes the polar angle of the complex number v. Further, the estimate of the constant part of the frequency offset is computed as $\widehat{f}_{mji} = \frac{\sum_{k=1}^{\widehat{K}_{rj}} \widehat{f}_{ojik}}{\widehat{K}_{rj}}$. For each $k \in [1, \widehat{K}_{rj}]$, the estimate of the EFO is obtained as $\widehat{f}_{jik} = \widehat{f}_{ojik} - \widehat{f}_{mji}$.

3) Authentication Signal to Interference and Noise Ratio (ASINR): The $\mathsf{BRx_j}$ utilizes the auto-correlation in the received samples to estimate the message signal to interference and noise ratio (MSINR) of the received frame [26]. Let the estimate of the MSINR corresponding to k^{th} frame be represented as $\widehat{\rho}_{jik}$. Hence, the estimate of the ASINR [27] corresponding to k^{th} frame is computed as $\widehat{\sigma}_{jik} = \frac{4\pi^2 \cdot N_c \cdot N_a \cdot N_f^2 \cdot f_a^2}{F_s^2} \cdot \frac{\widehat{\rho}_{jik}^{\,2}}{2 \cdot \widehat{\rho}_{jik} + 1}$.

D. Communicate the Parameters

After computing the estimated values of the parameters, the $\mathsf{BRx_j}$ communicates the set of the estimated values, represented by $\boldsymbol{D_{jik}} = \{\widehat{t}_{jik}, \widehat{f}_{jik}, \widehat{\sigma}_{jik}\}$, for all $i \in [1, \widehat{N}_{tj}]$, $k \in [1, \widehat{K}_{rj}]$, to the DFS.

VI. Operations at the DFS in FREE

A. Synchronize the Reported Data and Detect Transmitters

In FREE, for the center frequency F_c, the DFS receives the set of estimated values $\boldsymbol{D_{jik}}$ for all $j \in [1, N_b]$, $i \in [1, \widehat{N}_{tj}]$, $k \in [1, \widehat{K}_{rj}]$. The DFS determines the number of transmitters to be $\widehat{N}_t$ by evaluating the number of unique values of the time of arrival of the first frame, $\widehat{t}_{ji1}$, for all $j \in [1, N_b]$, $i \in [1, \widehat{N}_{tj}]$. Further, the DFS segregates the set of estimated values $\boldsymbol{D_{jik}}$ corresponding to each of the detected transmitter. Let each of the N_b blind receivers report $\widehat{K}_{ai}$ frames corresponding to the i^{th} transmitter. We assume that $K_a \leq \widehat{K}_{ai} < 2 \cdot K_a$, so that one complete sequence of K_a authentication symbols is successfully received at the DFS.

B. Aggregate the Reported Data

For all $k \in [1, \widehat{K}_{ai}]$, the DFS merges the reported frequency offsets to obtain an aggregated estimate of the EFO as $\widehat{f}_{aik} = \frac{\sum_{j=1}^{N_b} \omega_{mj} \cdot \widehat{\sigma}_{jik} \cdot \widehat{f}_{jik}}{\sum_{j=1}^{N_b} \omega_{mj} \cdot \widehat{\sigma}_{jik}}$, where ω_{mj} represents a weight value corresponding to the trustworthiness of the reported values of the blind receiver, $\mathsf{BRx_j}$, as perceived and computed by the DFS (see Section VI-D). Note that without these trustworthiness weights, the data aggregation becomes the conventional maximal ratio combining (MRC) [28]. In FREE, the trustworthiness weights are employed to make the data aggregation procedure robust against Byzantine attacks [29].

Algorithm 2 Trustworthiness Weight Update Algorithm

1) Compute $\mu_j = \frac{1}{2} - \widehat{\sigma}_{jik} \cdot \frac{\sum_{k=1}^{K_a} (\widehat{f}_{jik} - f_{aik})^2}{K_a}$, for each $j \in [1, N_b]$. Note that the expected value of μ_j is 0.
2) Calculate a normalized parameter $\nu_j = \frac{N_b \cdot \mu_j^{-2}}{\sum_{j=1}^{N_b} \mu_j^{-2}}$, for each $j \in [1, N_b]$. Note that the expected value of ν_j is 1.
3) Finally, for each $j \in [1, N_b]$, update the trustworthiness weight as $\omega_{(m+1)j} = \frac{m \cdot \omega_{mj} + \nu_j}{m+1}$.

C. Demodulate, Decode and Verify the Authentication Signal

For each $k \in [1, \widehat{K}_{ai}]$, the DFS maps the aggregated estimate of the EFO $\widehat{f}_{aik}$ to the closest one among $\{f_p\}$, for $p = 1, 2, \ldots, M_a$, given by equation (1), and obtains the estimate of the authentication symbol embedded in the transmitted frame. Then, the DFS concatenates the estimated q-bit authentication symbols to obtain the bits of the authentication signal. After synchronizing using a local copy of the authentication synchronization bits, and detecting and correcting any bit inversion errors and erasures in the estimated authentication bits, the estimated authentication data is obtained. Further, the estimates of the contents of the authentication data (i.e., $T_{si}, I_i, F_c, L_i, T_{hi}$, and π_i) are extracted from the estimated authentication data, and then verified using the digital signature verification procedure.

D. Update the Trustworthiness Weights

After the *successful* completion of each verification procedure by the DFS, the trustworthiness weights are adjusted based on the accuracy of the estimated EFOs reported by each blind receiver. The blind receivers' trustworthiness weights are initialized as $\omega_{mj} = 1$, for $m = 0$ and $\forall j \in [1, N_b]$. Note that a digital signature can only be correctly verified if all the bits in the digital signature are estimated correctly. This means that if the digitally signed authentication data is verified as valid, then the DFS knows exactly all the bits of the authentication signal; and the corresponding values of the true EFOs f_{aik}. Hence, after the successful verification of $(m+1)^{\text{th}}$ authentication data, the DFS utilizes the true values of the EFOs f_{aik} as feedback information for updating the trustworthiness weights ω_{mj}, $\forall j \in [1, N_b]$, using Algorithm 2.

To present the functioning of Algorithm 2, we provide the following three illustrative scenarios. In the first scenario, an honest $\mathsf{BRx_j}$ reports low values of ASINRs along with the

actually estimated values of the EFOs. In this scenario, there can be significant difference between the true EFOs and the reported EFOs. However, since the reported ASINRs are low, μ_j may still have a low absolute value, and ν_j may still have a value close to 1. Hence, the updated weight $\omega_{(m+1)j}$ remains close to ω_{mj}. This means that the trustworthiness weight of an honest $\mathsf{BRx_j}$ does not change significantly due to wrongly reported data at low ASINR.

In the second scenario, a rogue $\mathsf{BRx_j}$ reports incorrect values of the estimated EFOs, and provides low values of ASINRs to ensure low value of μ_j. In this scenario, the trustworthiness weight of the rogue $\mathsf{BRx_j}$ may remain unchanged. However, due to low ASINRs, the rogue $\mathsf{BRx_j}$ cannot significantly impact the aggregate estimate of the EFOs $\widehat{f}_{aik}$ (discussed in Section VI-B). In the third scenario, a rogue $\mathsf{BRx_j}$ reports incorrect values of the estimated EFOs. Also, it may either report actually received ASINRs or incorrectly provide high values of ASINRs to affect the aggregate estimate of the EFOs. In this scenario, μ_j will have a large absolute value, and ν_j will have a small value. If the value of ν_j is less than the value of the current weight ω_{mj}, the updated weight $\omega_{(m+1)j}$ is set to a lower value than ω_{mj}. In this way, the DFS lowers the trustworthiness weight of the rogue $\mathsf{BRx_j}$ after an incorrect set of reported data at high ASINR.

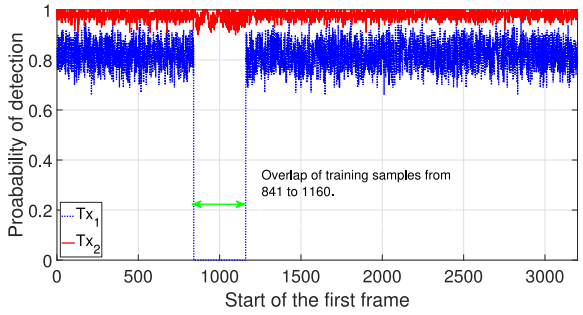

Fig. 3. Effect of interference on the detection performance.

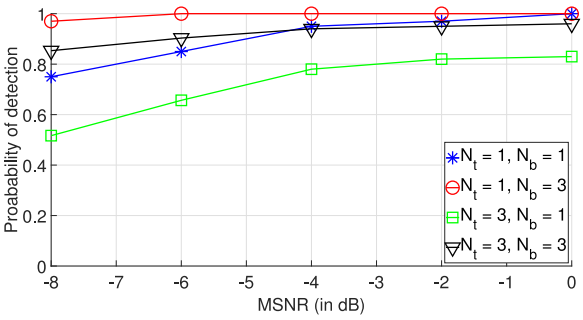

Fig. 4. Effect of crowd-sourcing on the detection performance.

VII. Analysis of FREE

A. Detection Performance of Transmitters

In FREE, each blind receiver detects the frame boundaries of the signals received from multiple transmitters using the auto-correlation induced by the training samples. After merging the reported time of arrival data from all the blind receivers, the DFS makes the final decision of the detection of transmitters. Hence, a transmitter is detected at the DFS if it is detected by at least one of the blind receivers. Considering that the detection of a transmitter in FREE involves multiple steps, it is prohibitively complex to find a closed-form expression for its performance. Therefore, we evaluate the detection performance through simulation.

Figure 3 presents the effect of overlap of the training samples of two transmitters, $\mathsf{Tx_1}$ and $\mathsf{Tx_2}$, on their probability of detection at a blind receiver. In this simulation, ten continuous frames from both the transmitters overlap in time such that the start of the first frame of $\mathsf{Tx_2}$ is fixed at the time corresponding to 1001^{th} sample, while the start time of the first frame of $\mathsf{Tx_1}$ is varied from 1^{st} sample to 3200^{th} sample. Here, the MSNR of the signals received from $\mathsf{Tx_1}$ and $\mathsf{Tx_2}$ are set to -3 dB and 0 dB, respectively. In Figure 3, we observe that $\mathsf{Tx_2}$ (with higher MSNR) is detected with high probability irrespective of the amount of overlap of the training samples. For $\mathsf{Tx_1}$, when the training samples do not overlap, the detection performance remains relatively consistent. However, when the training samples overlap, the $\mathsf{Tx_1}$ is not detected by the blind receiver. This is because according to the Step 6 in the Algorithm-1, when the $\mathsf{Tx_2}$ is detected, the values of the decision variable corresponding to the training samples of $\mathsf{Tx_2}$ are set to the mean value of the decision variable. This procedure also removes the conical hill corresponding to $\mathsf{Tx_1}$ in the values of the decision variable.

Although the detection procedure employed in FREE is robust against multipath fading and channel noise, it limits the detection performance at one blind receiver. However, in a crowd-sourced network, different blind receivers (due to their spatial distribution) may receive the signals from the co-channel transmitters at different fading coefficients and MSNRs. Hence, *different* transmitters can be detected at different blind receivers with high probability, and *all* the transmitters in a channel can be detected at the DFS with high probability when a sufficiently large crowd-sourced network is utilized. This observation is verified through Figure 4 which presents the effect of crowd-sourcing on the average probability of detection of a transmitter at the DFS in FREE. In the figure, we observe that the effect of co-channel interference on the probability of detection can be mitigated by crowd-sourcing.

B. Error Performance of the Authentication Signals

1) One Transmitter: We theoretically evaluate the error performance of the authentication signal for a typical scenario when there is no co-channel interference, no multipath fading, and the frame boundaries have been perfectly estimated at the DFS. In this scenario, the mean square error (MSE) of the frequency offset estimated at the DFS is lower bounded by the following Cramer-Rao Lower-Bound (CRLB) [27]

$$\text{CRLB} = \frac{1}{8\pi^2 N_a N_c N_b} \cdot \frac{F_s^2}{N_f^2} \cdot \left(\frac{1}{\rho_d^2} + \frac{2}{\rho_d} \right), \tag{5}$$

where ρ_d represents the average of the MSNR received at the blind receivers. Further, an error in the authentication

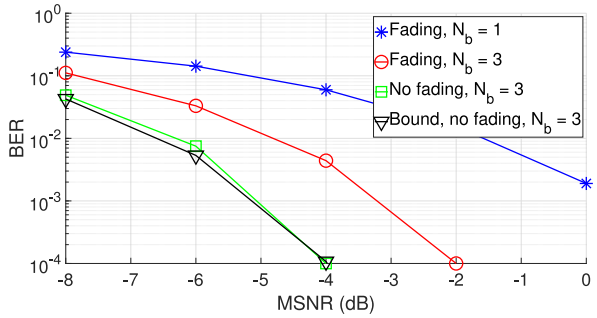

Fig. 5. Effect of multipath fading and crowd-sourcing on the BER of the authentication signal.

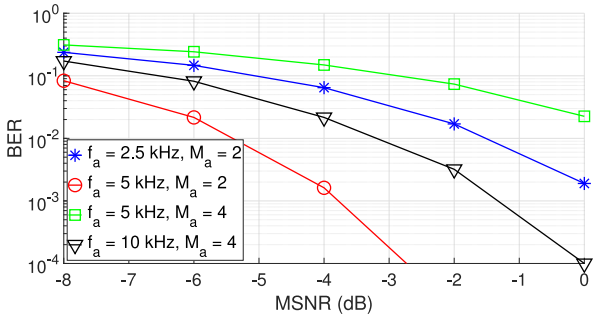

Fig. 6. Effect of f_a and M_a on the BER of the authentication signal.

symbol received at the DFS occurs when the mapping of estimated EFO, $\widehat{f}_{aik}$, to the closest one among $\{f_p\}$, for $p = 1, 2, \ldots, M_a$, leads to a different EFO as compared to the transmitted EFO, f_{aik}. This happens when the error in the estimate of the EFO exceeds the magnitude of half of the difference between two consecutive EFOs in M_a-FFM, i.e., $|\widehat{f}_{aik} - f_{aik}| > \frac{f_a}{M_a - 1}$. Using the lower bound on the MSE, the lower bound on the bit error rate (BER) of the authentication signal at the DFS is computed as

$$P_{ea} = \frac{1}{2} \cdot erfc\left(\sqrt{\frac{1}{\text{CRLB}} \cdot \frac{f_a^2}{2 \cdot (M_a - 1)^2}}\right), \tag{6}$$

where *erfc* represents the complementary error function. The equations (5) and (6) can be readily utilized to analyze the effects of different parameters on the error performance of the authentication signal.

In FREE, the EFOs in the frames of the message signal are estimated using the correlation properties between the CP samples and corresponding data samples. This means that the change in the correlation among those samples due to multipath fading and noise may hamper the estimation of the EFOs. Figure 5 presents the BER of the authentication signal vs. MSNR curves in FREE for different number of blind receivers, N_b. In the figure, we observe that multipath fading significantly increases the BER of the authentication signal. However, the effect of multipath fading on the BER can be significantly mitigated by crowd-sourcing, i.e., by increasing N_b. We also observe that the black curve with triangle markers representing the theoretical BER lower bound closely matches the curve representing the simulated BER with the same values of the parameters.

Figure 6 presents the BER of the authentication signal vs. MSNR curves for different values of f_a and M_a utilized in FREE. We observe that as the value of f_a is increased, the BER of the authentication signal decreases. This is because by increasing the value of f_a, we effectively account for a larger margin of error in the estimation of the EFO. However, in the existing standards describing PHY-layer specifications, there is a limited margin allowed for the carrier frequency offset in the message signals at the transmitters [22]. Hence, we need to ensure that $f_{ti} + f_a < F_o$, where F_o is the allowed frequency offset as per the standard. In Figure 6, we also observe that as the value of M_a increases, the BER of the authentication signal increases. Note that FREE with $M_a = 2$ can carry only one authentication bit per frame of the message signal, but FREE with $M_a = 4$ can carry two authentication bits per frame of the message signal. This means that the rate of transmission of one complete authentication bit sequence is increased by increasing the value of M_a. Hence, the value of M_a leads to a trade-off between the error performance and the rate of transmission of the authentication signal.

2) Multiple Co-Channel Transmitters: Significant undesirable modifications in the correlation between the CP samples and corresponding data samples may be caused by co-channel transmissions in addition to multipath fading and imperfect detection at the blind receivers. However, in FREE, as a result of collaborative detection by multiple blind receivers, the transmitted signals are received with different channel conditions at different blind receivers. Due to this diversity, signals simultaneously emitted from multiple co-channel transmitters can be detected and their EFOs can be extracted at different blind receivers. By aggregating the results from these blind receivers, it is possible for the DFS to *authenticate the multiple co-channel transmitters*. This is the most important characteristic of FREE that distinguishes it from prior art.

To evaluate FREE in this case, we utilize a parameter called "verification rate" which is defined as the ratio between the number of successfully verified digital signatures (see π_i in Section IV-B) in the authentication data and the total number of received digital signatures in the authentication data at the DFS. Figure 7 presents the average verification rate of the authentication data vs. MSNR for different values of the number of co-channel transmitters N_t, and the number of blind receivers N_b. In this simulation, we utilize the conventional (63,53) Reed Solomon code for channel coding to correct the errors in the authentication bits. In the figure, we observe that if there is only one blind receiver, then the authentication data's verification rate is low at very low MSNR and in the presence of co-channel interference. However, the interference from the other co-channel transmitters can be significantly mitigated through crowd-sourcing, i.e., by increasing N_b.

C. Security: Robustness Against the Byzantine Attack

In the context of crowd-sourced enforcement network utilized in FREE, a Byzantine attack represents a scenario in which a subset of the blind receivers (called rogue blind receivers) provides intentionally incorrect estimates of the EFOs to the DFS. In FREE, the trustworthiness weights

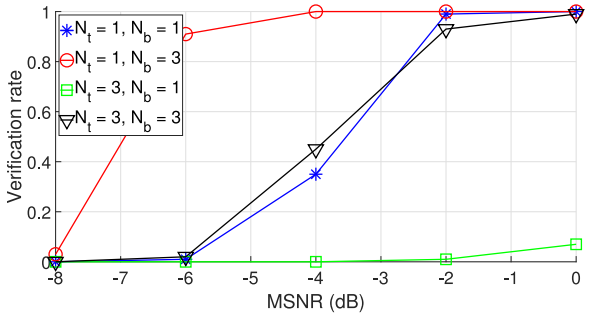

Fig. 7. Effect of crowd-sourcing on the verification rate.

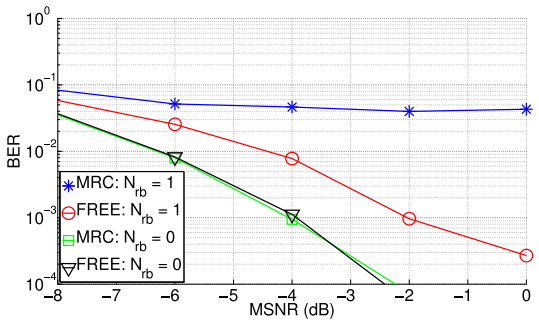

Fig. 8. Effect of byzantine attack on the BER performance.

are employed to make the data aggregation algorithm robust against Byzantine attacks. Figure 8 shows the authentication signal's BER vs. MSNR curves for FREE in two scenarios—when the number of *rogue* blind receivers, N_{rb}, is one or zero. The total number of blind receivers is four, i.e., $N_b = 4$. The figure also presents the same curves for the conventional MRC algorithm as a benchmark. Here, a rogue blind receiver does not report the correct estimates of EFO for half of the total number of EFO estimates; the reported values of the EFO are randomly selected from the range of possible values of EFO at the rogue blind receiver. In the figure, we observe that when $N_{rb} = 1$, FREE clearly outperforms MRC. This result can be attributed to the fact that MRC has no mechanism for mitigating the impact of incorrectly reported values (i.e., the Byzantine attack). Note that the feedback information utilized by FREE's algorithm is the primary contributor to FREE's robustness against the Byzantine attack.

D. Delay in the Verification of the Authentication Signal

Here, we illustrate that FREE can satisfactorily ensure successful verification of the authentication signal under real-world delay constraints. For the following illustration, we consider the specifications of the software defined radio wireless regional area network in IEEE 802.22 standard [30]. Specifically, we consider that the duration of a transmitted frame (frame size) is 10 milliseconds (ms), and the nominal data rate of a secondary channel between the blind receiver and the DFS is set to 1 Mbps.

Let each of the components of the authentication data (i.e., T_{si}, I_i, F_c, L_i and T_{hi}) be represented by 32 bits. The recommended length of the ECC-based digital signature π_i is

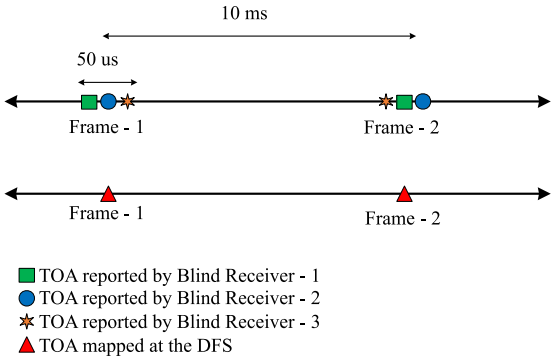

Fig. 9. An illustration presenting the time of arrival (TOA) reported by blind receivers and TOA mapped by the DFS.

259 bits [23]. Hence, along with the authentication synchronization bits and channel coding, the authentication signal can be represented by 512 bits. This means that in FREE, the transmitter's authentication signal can be transmitted in $(512 \times 10/1000 = 5.12)$ seconds. Further, let each of the components of the reported data (i.e., $\widehat{t}_{jik}, \widehat{f}_{jik}, \widehat{\sigma}_{jik}$) by the blind receiver be represented by 32 bits. Hence, the reported data corresponding to one instance of the authentication signal of a transmitter can be transmitted to the DFS through the secondary channel in $(512 \times 96/10^6 = 0.0492)$ second.

Further, in FREE, let the DFS periodically broadcast a reference signal on the secondary channel. Using this reference broadcast, the blind receivers synchronize their data aggregation and reporting procedure with the DFS. Considering different types of delay (e.g., the clock jitter, and differences in acquisition, processing and travel time among multiple nodes) involved in this synchronization mechanism, the worst-case time misalignment between the DFS and the blind receivers can be limited to less than 25μs [20], [21]. This means that the worst-case time misalignment between the time of arrival values (of a frame transmitted by a transmitter) reported by any two blind receivers is limited to 50μs which is significantly less than the frame size (10 ms). Hence, for each frame, the DFS can readily map the TOA values reported by different blind receivers to a mapped TOA which is utilized to synchronize their reported data. An illustrative example (with three blind receivers and the DFS) of this synchronization mechanism is presented in Figure 9.

Our experiments (discussed in Section IX) suggest that the DFS can readily collect the authentication signal from the blind receivers, and authenticate it within six seconds. Note that in the dynamic spectrum management framework proposed by FCC for 3.5 GHz band, Citizen Broadband Radio Service (CBRS) must check the status of the available frequency channels and report any changes in every 60 seconds [31]. Hence, the required time to authenticate a transmitter in FREE is within the technical requirements suggested by FCC.

E. Incentives for Crowd-Sourced Blind Receivers

The design of FREE enables SUs in the DSS paradigm to act as crowd-sourced blind receivers. These SUs need to

invest significant computational, communication and memory resources for the extensive set of operations required at blind receivers as discussed in Section V. Hence, SUs need to be sufficiently compensated with appropriate incentives to motivate them to participate in the enforcement network. In DSS, incentives can be provided through two methods: spectrum access opportunities and monetary credits. In the first method, the channel allocation strategy in DSS may allow the crowd-sourced SUs to access the spectrum for additional amount of time. For instance, the time made available by revoking the transmission rights of the rogue transmitter can be utilized for this purpose. In the second method, the penalty amount collected from rogue transmitters can be paid to crowd-sourced SUs. Note that when the two methods are employed with FREE, the incentives can be commensurate with the trustworthiness weights of SUs. A detailed discussion on incentives in the crowd-sourced enforcement networks is out of scope this work, and the readers are referred to [15], [16], [32] for further readings on this topic.

VIII. Comparison With the Prior Art

To evaluate FREE, we compare its performance with two benchmarks—viz., *FEAT* [7] and *Gelato* [5]. We select FEAT and Gelato since they, like FREE, support blind receivers and are backward-compatible with the PHY-layer of the intended receivers. In all the three schemes, FREE, FEAT and Gelato, the message signal is generated using the parameters shown in Table I. In FREE and FEAT, the authentication signal is embedded into the message signal by modifying its frequency offset. Note that the procedures for embedding the authentication signal are the same in FREE and FEAT, but the procedures for extracting the authentication signal are *different*. In Gelato, the authentication signal is embedded into the transmitted OFDM signal by repeating 12 message data symbols over the sub-carriers to generate a cyclo-stationary signature. In all the three schemes, by design, one bit of the authentication signal is embedded into each frame of the message signal.

Overhead: This attribute includes the evaluation of the significantly disadvantageous changes related to various aspects, including the computational complexity of the transmitter and the intended receivers; the transmission power and the throughput of the message signal at the transmitter; and the BER of the message signal at the intended receiver. In FREE and FEAT, the transmitter embeds the frequency offset into the message signal through simple vector multiplication over each frame. This means that no significant computational overhead is incurred at the transmitter. Also, there are no changes in transmission power and message throughput at the transmitter. FREE and FEAT do not impact the BER performance of the message signal at the intended receiver. In Gelato, the computational overhead to embed the authentication signal at the transmitter is non-significant. However, since 12 out of 64 message data sub-carriers are loaded with redundant symbols, the message throughput is significantly reduced. Gelato does not negatively impact an intended receiver's BER performance.

Compatibility: This attribute recognizes the changes to the demodulation and decoding procedures needed at an intended receiver. This is an important criterion in terms of evaluating a scheme's real-world validity, because a non-compatible scheme would require all receivers (including those that do not need to authenticate the received signals) to modify their demodulation/decoding procedures, which would be prohibitively expensive in some cases. In the existing air-interface standards, there is a margin of error allowed for the carrier frequency offset (CFO) in the message signals due to inaccurate oscillators at the transmitters and the receivers. For instance, as per the IEEE 802.11g standard [22], a CFO of less than 25 ppm of the carrier frequency is allowed. This means that for signals transmitted at 2.4 GHz, a CFO of ± 60 kHz is allowed. FREE and FEAT are designed to function correctly within the allowed CFO margin of error, and hence they are *compatible* with the legacy receivers. Although Gelato is compatible with the PHY-layer of the legacy receivers, it is not compatible with the upper-layers. For correct decoding of the message data, Gelato requires the message decoding procedure at an intended receiver to be modified to discard the redundant symbols at the 12 sub-carriers.

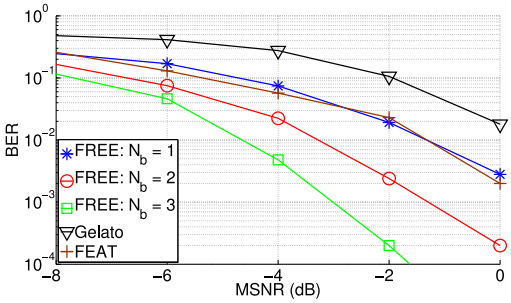

Fig. 10. BER performance in FEAT, Gelato and FREE.

Authentication Signal's Error Performance: In Figure 10, we compare the BER performance of the authentication signal in FREE, FEAT and Gelato. In this figure, we observe that the collaborative authentication performed by multiple blind receivers provides FREE with a noticeable advantage over the other two schemes in terms of the BER. This advantage becomes more pronounced as the number of blind receivers, N_b, is increased. Note that unlike FREE, FEAT and Gelato were not designed to support the crowd-sourced authentication.

Authentication of Multiple Co-Channel Transmitters: In real-world scenarios, the enforcement entity may need to authenticate signals being transmitted simultaneously from multiple (possibly rogue) co-channel transmitters. Unfortunately, FEAT and Gelato were not designed to function correctly under such circumstances. However, our findings show that FREE can reliably authenticate transmitters even under such challenging conditions. This is the most distinguishing feature of FREE when compared to the prior art.

IX. Experimental Validation

To evaluate the validity of FREE in a testbed environment, we implemented FREE on Universal Software Radio Peripheral (USRP) radio boards. We used National

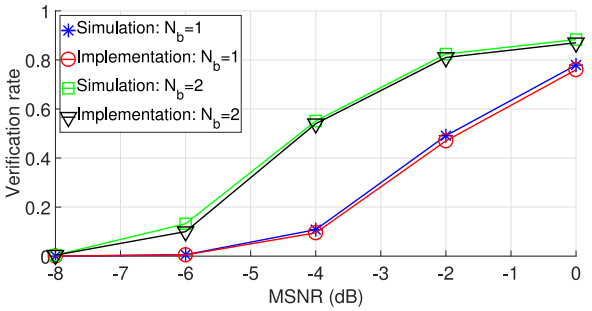

Fig. 11. Verification rate obtained using implementation.

Instruments' LabVIEW as the system-design platform to configure the USRP radios. The parameters provided in Table I were utilized by two USRP transmitters to generate the message signals, embed them with the authentication signals, and transmit the embedded signals over-the-air at 900 MHz. Two USRP blind receivers were utilized to receive and extract the authentication signals. The USRP radios were placed at random locations in an indoor lab facility. A PC was used as the DFS. The PC was also utilized to generate the time-stamps for recording the time of arrival of the reported data from the USRP blind receivers.

We faced with two challenges during our experiments at very low MSNR. Firstly, the USRP radios suffered from low receiver sensitivity. Secondly, the distances among the radios were limited as the radios needed to be connected to the PC running the LabVIEW application through network cables. Hence, the channel conditions experienced by the signals received at the blind receivers in our experiments were limited to additive Gaussian noise (without any fading).

In our experiments, we were able to verify that using the proposed techniques in FREE, the blind receivers were able to detect two co-channel transmitters (that are transmitting simultaneously) with high accuracy. Further, Figure 11 shows the performance of FREE in the LabVIEW implementation experiments in terms of verification rate of the authentication signals from two co-channel transmitters. In this figure, we observe that the verification rate in FREE with two blind receivers is significantly better than that with one blind receiver, specifically at low MSNR. For instance, at the average MSNR of -4 dB, the DFS is able to verify the two transmitters with accuracy around 10% when $N_b = 1$, and around 55% when $N_b = 2$. Figure 11 also includes the curves obtained from MATLAB simulations as benchmarks. We can observe that the LabVIEW implementation's curves closely track those of the simulations.

X. Conclusion

In this paper, we proposed a novel CBAT scheme called FREE. Using theoretical analysis, simulations, and experimental results, we showed that FREE can reliably authenticate multiple transmitters that are transmitting simultaneously in the same channel.

References

[1] V. Kumar, H. Li, J.-M. Park, and K. Bian, "Enforcement in spectrum sharing: Crowd-sourced blind authentication of co-channel transmitters," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw. (DySPAN)*, 2018, pp. 1–10.

[2] F. Teng, D. Guo, and M. L. Honig, "Sharing of unlicensed spectrum by strategic operators," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 668–679, Mar. 2017.

[3] J.-M. Park *et al.*, "Security and enforcement in spectrum sharing," *Proc. IEEE*, vol. 102, no. 3, pp. 270–281, Mar. 2014.

[4] "Amendment of the commission's rules with regard to commercial operations in the 3550–3650 MHz band," Federal Commun. Commission, Washington, DC, USA, Rep. GN Docket No. 12–354, Apr. 2015.

[5] A. Nika, Z. Zhang, B. Y. Zhao, and H. Zheng, "Toward practical spectrum permits," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 1, pp. 112–122, Mar. 2017.

[6] A. Malki and M. B. H. Weiss, "Ex-post enforcement in spectrum sharing," in *Proc. TPRC*, Mar. 2014, pp. 1–22.

[7] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2014, pp. 787–798.

[8] V. Kumar, J.-M. Park, and K. Bian, "PHY-layer authentication using duobinary signaling for spectrum enforcement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1027–1038, May 2016.

[9] V. Kumar, J.-M. Park, and K. Bian, "Transmitter authentication using hierarchical modulation in dynamic spectrum sharing," *J. Netw. Comput. Appl.*, vol. 91, pp. 52–60, Aug. 2017.

[10] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. ACM Conf. Wireless Netw. Security (WiSec)*, Jun. 2011, pp. 79–90.

[11] X. Wan, L. Xiao, Q. Li, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced communication overhead," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[12] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[13] X. Jin, J. Sun, R. Zhang, and Y. Zhang, "SafeDSA: Safeguard dynamic spectrum access against fake secondary users," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2015, pp. 304–315.

[14] G. Atia, A. Sahai, and V. Saligrama, "Spectrum enforcement and liability assignment in cognitive radio systems," in *Proc. 3rd IEEE Symp. New Front. Dyn. Spectr. Access Netw. (DySPAN)*, Oct. 2008, pp. 1–12.

[15] A. Dutta and M. Chiang, "'See something, say something' crowdsourced enforcement of spectrum policies," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 67–80, Jan. 2016.

[16] N. Kaufmann, T. Schulze, and D. J. Veit, "More than fun and money. Worker motivation in crowdsourcing—A study on mechanical turk," in *Proc. Americas Conf. Inf. Syst. (AMCIS)*, 2011, pp. 1–11.

[17] O. Fatemieh, R. Chandra, and C. A. Gunter, "Secure collaborative sensing for crowd sourcing spectrum data in white space networks," in *Proc. IEEE Symp. New Front. Dyn. Spectr. Access Netw. (DySPAN)*, Apr. 2010, pp. 1–12.

[18] S. Xiao, J.-M. Park, and Y. Ye, "Tamper resistance for software defined radio software," in *Proc. 33rd IEEE Int. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, 2009, pp. 383–391.

[19] Y. H. Kim, I. Song, H. G. Kim, T. Chang, and H. M. Kim, "Performance analysis of a coded OFDM system in time-varying multipath Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 48, no. 5, pp. 1610–1615, Sep. 1999.

[20] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *ACM SIGOPS Oper. Syst. Rev.*, vol. 36, pp. 147–163, Dec. 2002.

[21] K. Tan *et al.*, "Fine-grained channel access in wireless LAN," in *Proc. ACM SIGCOMM Conf.*, 2010, pp. 147–158.

[22] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2012, 2012.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, Sep. 2004.

[24] V. Kumar *et al.*, "Direct anonymous attestation with efficient verifier-local revocation for subscription system," in *Proc. ACM Asia Conf. Comput. Commun. Security (AsiaCCS)*, 2018, pp. 567–574.

[25] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[26] G. Ren, H. Zhang, and Y. Chang, "SNR estimation algorithm based on the preamble for OFDM systems in frequency selective channels," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2230–2234, Aug. 2009.
[27] M.-H. Cheng and C.-C. Chou, "Maximum-likelihood estimation of frequency and time offsets in OFDM systems with multiple sets of identical data," *IEEE Trans. Signal Process.*, vol. 54, no. 7, pp. 2848–2852, Jul. 2006.
[28] A. F. Molisch and M. Z. Win, "MIMO systems with antenna selection," *IEEE Microw. Mag.*, vol. 5, no. 1, pp. 46–56, Mar. 2004.
[29] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. 27th IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 31–35.
[30] C. R. Stevenson *et al.*, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 130–138, Jan. 2009.
[31] M. M. Sohul, M. Yao, T. Yang, and J. H. Reed, "Spectrum access system for the citizen broadband radio service," *IEEE Commun. Mag.*, vol. 53, no. 7, pp. 18–25, Jul. 2015.
[32] B. Gao *et al.*, "Incentivizing spectrum sensing in database-driven dynamic spectrum sharing," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, 2016, pp. 1–9.

Vireshwar Kumar (M'13) received the Ph.D. degree in computer engineering from Virginia Tech, USA, in 2016. He is currently a Post-Doctoral Research Associate with the Department of Computer Science, Purdue University, USA. His research interests include designing lightweight security protocols for cyber physical systems and Internet of Things. He was a recipient of the Best Ph.D. Student Award by the Center for Embedded Systems for Critical Applications at Virginia Tech in 2016. He currently serves as a reviewer in a number of IEEE journals.

He Li received the B.Sc. and M.S. degrees in electrical and computer engineering from Shanghai Jiao Tong University, China, in 2010 and 2013, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Virginia Tech. His research interests include security and privacy issues in wireless networks, spectrum enforcement, and applied cryptography.

Jung-Min (Jerry) Park (F'17) received the Ph.D. degree in electrical and computer engineering from Purdue University in 2003. He is currently a Professor with the Department of Electrical and Computer Engineering, Virginia Tech and the Site Director of a National Science Foundation (NSF) Industry-University Cooperative Research Center called Broadband Wireless Access and Applications Center. He served as an Executive Committee Member for the U.S. National Spectrum Consortium (NSC) from 2016 to 2018. NSC is a large consortium of wireless industry stakeholders and universities collaborating with multiple U.S. federal government agencies through a $1.25 billion agreement to support the development of advanced spectrum access technologies. His research interests include dynamic spectrum sharing, emerging wireless technologies, including 5G and V2X, wireless security and privacy, and applied cryptography. Current or recent research sponsors include NSF, National Institutes of Health, Defense Advanced Research Projects Agency, Army Research Office, Office of Naval Research, and several industry sponsors. He was a recipient of the 2017 Virginia Tech College of Engineering Dean's Award for Research Excellence, the 2015 Cisco Faculty Research Award, the 2014 Virginia Tech College of Engineering Faculty Fellow Award, the 2008 NSF Faculty Early Career Development (CAREER) Award, the 2008 Hoeber Excellence in Research Award, and the 1998 AT&T Leadership Award. He is currently serving on the editorial boards of a number of IEEE journals, and is actively involved in the organization of a number of flagship conferences. He is currently serving as the Steering Committee Chair for the IEEE International Symposium on Dynamic Spectrum Access Networks. He is an IEEE Fellow for his contributions to dynamic spectrum sharing, cognitive radio networks, and security issues.

Kaigui Bian (M'11) received the Ph.D. degree in computer engineering from Virginia Tech in 2011. He is currently an Associate Professor with the School of Electronics Engineering and Computer Science, Peking University, China. His main research interests include mobile computing, cognitive radio networks, and network security and privacy. He was a recipient of the 2018 IEEE Asia–Pacific Board Outstanding Young Researcher Award. He is currently on the editorial board of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE ACCESS.