Ensemble Learning Based Robust Cooperative Sensing in Full-Duplex Cognitive Radio Networks

Yirun Zhang
Centre of Telecommunications Research
King's College London

Qirui Wu
Centre of Telecommunications Research
King's College London

Mohammad Shikh-Bahaei
Centre of Telecommunications Research
King's College London

***Abstract*—We propose an ensemble learning (EL) based cooperative sensing framework in full-duplex cognitive radio networks (FD-CRNs), which is robust with accuracy against malicious attacks and interference. The FD communication further improves the spectrum awareness capability of the secondary users (SUs) by allowing them to sense and transmit simultaneously over the same frequency band. However, it also complicates the sensing environment by introducing self-interference and co-channel interference. In the meantime, the presence of malicious attacks such as Primary User Emulation and Spectrum Sensing Data Falsification attacks also degrade the cooperative sensing performance in practice. To alleviate the influence of interference and attacks, we design an EL framework that provides robust and accurate fusion performance with low time cost. In such a context, we analyse the spectrum waste and collision probabilities in the FD Listen-And-Talk (LAT) protocol to measure the performance. Simulation results show that our proposed EML framework can provide lower and more robust false-alarm probability than single-model based fusion methods with the same detection probability constraint for any size of training sets. It also outperforms the conventional majority vote based fusion strategy in terms of much lower and stable spectrum waste and collision probability for any number of trusted SUs.**

***Index Terms*—Cognitive radio, full-duplex, primary user emulation, spectrum sensing data falsification, ensemble learning.**

I. Introduction

THE rapid development of wireless networks exacerbates the radio resource scarcity issue [1]. Cognitive radio networks (CRNs), in which secondary users (SUs) can sense and access the spectrum white spaces in primary users' (PUs') channels, has become a promising solution to increase spectrum reuse. Cooperative sensing has been proven to be an effective sensing strategy that mitigates the sensing errors made by local SUs in CRNs, where a fusion centre (FC) takes the responsibility for fusing the local sensing result from each cooperative SU and making a final sensing decision [2]. The majority vote (MV) rule is commonly used as a fusion strategy [3]. On the other hand, the full-duplex (FD) communications bring a new transmission protocol to CRNs, which is known as Listen-And-Talk (LAT) [4], [5]. The LAT protocol proposed in [5] allows one FD device to sense and transmit data at the same time and the other one only receives data. However, it also introduces new interference issues including self-interference (SI) and co-channel interference (CCI) to FD-CRNs.

Besides the SI and CCI introduced by the FD LAT protocol, cooperative sensing frameworks also face malicious attacks in the real-world CRNs due to the vulnerable nature of wireless propagations [6]. Two typical malicious attacks toward spectrum sensing are called Primary User Emulation (PUE) attack and Spectrum Sensing Data Falsification (SSDF) attack. A PUE attacker tries to mislead the cooperative SUs by sending jamming signals to pretend that PU is occupying the channel [6]. SSDF SU attackers launch attacks by randomly flipping their sensing results to 'blind' the FC with their own purposes [6]. As a result, the efficiency and reliability of the communications in CRNs could be significantly degraded.

Considerable algorithms regarding mitigating PUE and SSDF attacks in half-duplex (HD) CRNs have been proposed. A PUE detector using K-means is proposed to differentiate the contaminated sensing measurements sent by attacked SUs. Such method intuitively mitigates PUE attacks by discarding malicious reports, which also causes the loss of useful information in these reports. Reputation-based voting mechanisms are introduced in [7], [8] to mitigate SSDF, where a reputation table is established to assign weights to each SU's local result. The authors in [7] also discuss the influence of SI and CCI on the local sensing performance in the FD case.

The presence of SI, CCI and malicious attacks such as PUE and SSDF significantly complicates the sensing environment, where conventional fusion methods such as MV fails to provide robust and accurate fusion results. Inspired by the fast development of machine learning-based fusion strategy for cooperative sensing, in this paper we have presented a novel ensemble learning (EL) framework to provide robust fusion results. The main contributions of this paper can be summarised as follows. We propose a novel EL framework for sensing result fusion, which is robust against interference and malicious attacks. In the EL framework, three different base learners including Temporal Convolutional Recurrent Neural Network (TCRNN), Support Vector Machine (SVM) and Reputation based Weighted Majority Vote (RWMV) algorithm are introduced, followed by a Logistic Regression (LR) meta learner to assign proper weight to each base learner's result. Then we analyse the spectrum waste and collision probabilities of LAT for our proposed EL framework. Through simulation and numerical results, we address the conclusion that our proposed EL framework outperforms MV fusion method.

The rest of the paper is organised as follows. Section II describes the system model, cooperative sensing metrics and malicious attacks. In Section III, we elaborate on our proposed

978-1-7281-7440-2/20/$31.00 ©2020 IEEE

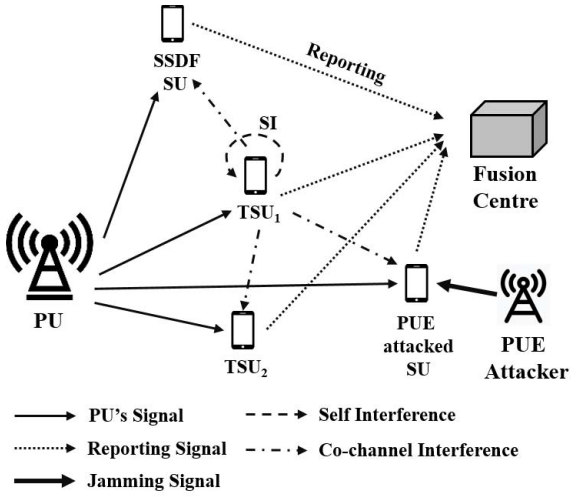

Fig. 1. Structure of the system model.

EL framework by introducing three base learners and one meta learner. In Section IV, we analyse the spectrum waste and collision probabilities in LAT. Simulation and numerical results are presented in Section V. In the end, we draw our conclusion in Section VI.

II. System Model

As shown in Fig. 1, we consider a CRN consisting of one PU-licensed channel, M unlicensed SUs, each of which is equipped with two-antenna FD radio and partial SI suppression (SIS) capability, and an FC. SUs cooperatively sense the channel to detect the status of PU and report to FC. Among all M SUs, we assume there are M_t ($M_t \geqslant 2$) trusted SUs (TSUs), M_p PUE attacked SUs and M_s misbehaving SSDF SUs that report highly unreliable sensing results to the FC. There is a control channel in the secondary network, which is used for reporting sensing results from SUs to the FC. The reporting signal is assumed to be error-free.

A. Primary User's Traffic Model

PU's traffic is modelled as a simple ON and OFF process which contains two instant states: $s_t = 1$ is for busy and $s_t = 0$ is for idle at time slot t. Recent studies indicate that the real-world PU's channel occupancy status is rather time-correlated than completely memoryless [9]. Therefore, we assume random packet arrivals at PU packet arrival rate λ_a (packet/slot). According to the Bernoulli process, PU becomes active with probability $\mathrm{P}(s_{t+1} = 1|s_t = 0) = p$ when its queue is not empty and if it is not transmitting. Considering the common case that PU changes its state sufficiently slow, we assume $\frac{1}{p} \gg 1$. Once activated, PU will keep transmitting until its queue becomes empty with a transmission rate λ_t ($\lambda_t > \lambda_a$). Thus, there is a temporal correlation between the states of previous slots and the current slot.

B. Cooperative Sensing Metrics

In each time slot, local sensing is performed by each SU in the network first. We consider energy-detection based spectrum sensing technique in this paper due to its simplicity and ability to identify spectrum white spaces without requiring any *a priori* information of PU's signal pattern. The sensing result also has two states: $o_t = 1$ is for busy and $o_t = 0$ is for idle at time slot t. The performance of spectrum sensing is judged by two fundamental measures, the false-alarm $P_f = \mathrm{P}(o_t = 1|s_t = 0)$ probability and the detection probability $P_d = \mathrm{P}(o_t = 1|s_t = 1)$. The former refers to the probability that the channel is idle, and SU falsely decides that it is occupied by the PU. The latter is the probability that the PU is occupying the channel and the SU detects it.

We quantify the SIS capability in FD-LAT protocol by χ ($0 \leqslant \chi \leqslant 1$), where $\chi = 0$ corresponds to perfect SIS and $\chi = 1$ indicates no SIS [10]. Without loss of generality, we assume TSU_1 and TSU_2 is the current transmitter and receiver pair with SIS coefficient χ. The false-alarm probability and detection probability for TSU_1 considering SI are given by eq. (9) and (12) in [10], respectively.

The influence of CCI on sensing performance is also critical, especially when the SU transmitter TSU_1 is located nearby the other SUs. The detection and false-alarm probabilities considering CCI are similar to those with SI but replacing the SI terms by CCI terms α_{s_i,s_1}, where α_{s_i,s_1} refers to the SNR transmitted by TSU_1 and received at $\mathrm{SU_i}$.

The local sensing decision for the ith SU is 0-1 binary, determined by comparing the received energy level with its pre-set threshold. The FC collects each SU's sensing result through the control channel. It then makes the final decision according to its fusion rule, and broadcasts the final sensing decision to all SUs by sending control messages.

C. PUE and SSDF Attacks

PUE attackers occasionally send PU-alike signal to nearby SUs to prevent them from observing the spectrum white spaces [6]. Those attacked SUs result in high false-alarm probability. Consider the PUE attacker may occasionally save energy, we define two attack probabilities, which are p_0^{PUE} and p_1^{PUE}, respectively. The former refers to the probability that the PUE attacker sends a jamming signal when PU is absent whilst the latter indicates the probability that it attacks when PU is occupying the channel. Therefore, the sensing error probabilities can be further expressed as:

$$\hat{P}_{d,\mathrm{PUE}}^{(i)} = P_d^{(i)} + p_1^{\mathrm{PUE}}(P_{d,\mathrm{PUE}}^{(i)} - P_d^{(i)}) \tag{1}$$

$$\hat{P}_{f,\mathrm{PUE}}^{(i)} = P_f^{(i)} + p_0^{\mathrm{PUE}}(P_{f,\mathrm{PUE}}^{(i)} - P_f^{(i)}), \tag{2}$$

where $P_{d,\mathrm{PUE}}^{(i)}$ and $P_{f,\mathrm{PUE}}^{(i)}$ are the ith SU's sensing error probabilities under PUE attack, which are calculated by replacing the SI terms by the PUE interference terms $\alpha_{s_i,a}$, where $\alpha_{s_i,a}$ is the SNR transmitted by the PUE attacker a and received at $\mathrm{SU_i}$.

SSDF attack refers to SUs sending modified sensing results in order to "fool" the FC to make highly unreliable final decisions [6]. Unlike PUE attackers who usually aim at preventing SUs from discovering the idles slots, SSDF attackers flip their sensing results for both preventing SUs transmission

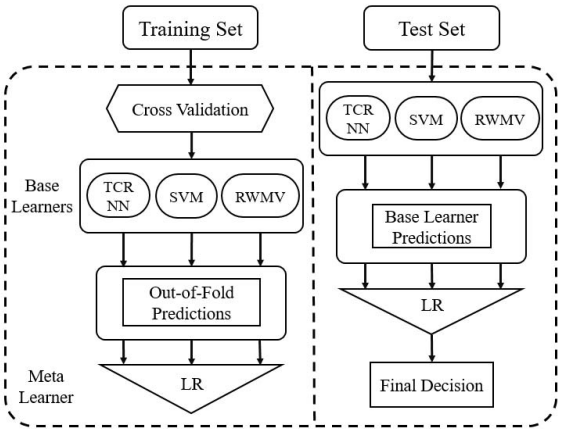

Fig. 2. Training and testing procedure for the proposed ensemble machine learning based robust fusion strategy.

and increasing the collision probability between SUs and PU. We also define two attack probabilities, p_0^{SSDF} and p_1^{SSDF}. The former is the probability that SSDF SUs flip their results when the channel is unoccupied whilst the latter is the probability they flip their results when the PU is not absent. The sensing error probabilities under the SSDF attack are given by:

$$P_{d,\mathrm{SSDF}}^{(i)} = P_d^{(i)}(1-p_1^{\mathrm{SSDF}}) + (1-P_d^{(i)})p_0^{\mathrm{SSDF}} \quad (3)$$

$$P_{f,\mathrm{SSDF}}^{(i)} = P_f^{(i)}(1-p_1^{\mathrm{SSDF}}) + (1-P_f^{(i)})p_0^{\mathrm{SSDF}}. \quad (4)$$

III. Ensemble Machine Learning Based Robust Fusion Strategy

As analysed in Section II, the presence of SI and CCI and malicious attackers significantly degrades SU's local sensing performance, and thus, worsens the global sensing decision made by the FC. Conventional fusion method such as the MV rule has been proven to be ineffective in this kind of complicated scenario since the weight of each SU's result cannot be considered as equal [7]. On the other hand, since the learning capability of a single model is usually limited, we propose an ensemble framework which combines the results from various models in order to increase the decision reliability and also ensure secure and reliable communications in FD-CRNs [11]. The proposed learning and prediction procedure is shown in Fig. 2, and described in the following.

A. Framework Structure

The EL framework contains two levels where the first level is called the base learner level and the second level is called the meta learner level. The base learner level consists of multiple different machine learning methods, which aims at extracting latent representations from different aspects. Studies have proven that the larger difference between base learners leads to better prediction results since the model can learn more different latent expressions of the data [11]. In this paper, we choose three different learning methods as base learners, which are TCRNN, SVM and RWMV. TCRNN learns the temporal

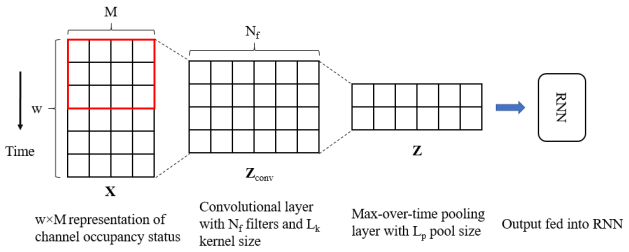

Fig. 3. Structure of temporal convolutional layer with max-over-time pooling in w time slots.

correlation between previous and current slots and the non-linear mapping between inputs and output. SVM extracts high-dimension implicit representations between SUs' local results, and RWMV learns the explicit linear relationships based on their reputations (i.e., whether their sensing results are equal to the label). The meta learner level usually contains one simple linear learner to prevent overfitting. One commonly used meta learner is the LR algorithm.

B. Training and Testing Procedures

The input of EL framework is a local decision vector containing all cooperative SUs' local results whilst the output is either 0 or 1 (i.e., idle or busy). The training procedure is illustrated in the left half of Fig. 2. First, we apply the K-fold cross-validation to split the original training set into K subsets (e.g., $K = 5$ in this paper). The base learners choose $K-1$ subset for training and evaluate their results on the remaining one subset. This cross-validation process continues for K times until all subsets are evaluated. Then the evaluation results, which are called the Out-of-Fold (OOF) predictions, are used as the training set for the meta learner. After the cross-validation is finished, all learners are trained on the entire original training set. The testing procedure is illustrated in the right half of Fig. 2. The base learners predict on the test set and then the meta learner combines their prediction results and makes the final decision.

C. Temporal Convolutional Recurrent Neural Network

Both Temporal Convolutional Network (TCN) and Recurrent Neural Network (RNN) have shown promising capability on time series classification tasks. Thus, we design a hybrid TCRNN structure in this paper to extract the non-linear and temporal feature representations of SUs' local results.

1) Temporal Convolutional Layers: A temporal convolutional layer is added before RNN to pre-extract the temporal features. Figure. 3 illustrates the process of temporal convolutional and max-over-time pooling operations. The input matrix $\mathbf{X}$ has been processed in such a way that each sample contains M SUs' local sensing results over w time slots. Then the convolutional filters extract temporal features and generate a new feature matrix $\mathbf{Z}_{\mathrm{conv}}$. In order to prevent overfitting, the network only keeps a part of generated features by using max-over-time pooling. After max pooling, the size of the feature

Algorithm 1 Reputation Based Weighted Majority Vote

Initialise each SU's reputation to zero
for $j = 1, 2, ..., N$ **do**
  for $i = 1, 2, ..., M$ **do**
    if $d_j^{(i)} == y_j^*$ **then**
      Increase SU_i's reputation: $r_j^{(i)} = r_j^{(i)} + 1$
    else
      Decrease SU_i's reputation: $r_j^{(i)} = r_j^{(i)} - k$
    end if
  end for
end for
The fusion result in probability:
$p_{\mathrm{rwmv}} = \mathrm{P}(\hat{y}^* = 1|\hat{\mathbf{x}}) = \mathrm{sigmoid}(\sum_{i=1}^{M} r^{(i)} \hat{d}^{(i)})$

matrix is reduced. At last, the pooled feature matrix $\mathbf{Z}$ is fed into RNN for recurrent processing.

2) Long Short-Term Memory Layers: RNN is a superior deep learning structure in solving time series prediction problem, which explores the temporal relationship between the previous state to the current state. The input matrix $\mathbf{Z}$, which comes from the output of the convolutional and pooling layers, are fed into the RNN network one vector at each step (e.g., $\mathbf{z}_t$ is the input vector of RNN at step t). The historical information up to the current step is all stored in the hidden states of RNN, by which RNN learns the temporal correlation between previous slots and the current slot. In order to tackle the gradient vanishment problem for traditional RNN cell, the Long Short-Term Memory (LSTM) cell structure is used here.

The mapping function in an LSTM memory cell from the input $\mathbf{z}_t$ to output $\mathbf{h}_t$ at step t is precisely specified by:

$$\begin{aligned}
\mathbf{i}_t &= \mathrm{sigmoid}(\mathbf{W}_i^z \cdot \mathbf{z}_t + \mathbf{W}_i^h \cdot \mathbf{h}_{t-1} + \mathbf{b}_i) \\
\mathbf{f}_t &= \mathrm{sigmoid}(\mathbf{W}_f^z \cdot \mathbf{z}_t + \mathbf{W}_f^h \cdot \mathbf{h}_{t-1} + \mathbf{b}_f) \\
\mathbf{o}_t &= \mathrm{sigmoid}(\mathbf{W}_o^z \cdot \mathbf{z}_t + \mathbf{W}_o^h \cdot \mathbf{h}_{t-1} + \mathbf{b}_o) \\
\tilde{\mathbf{c}}_t &= \tanh(\mathbf{W}_c^z \cdot \mathbf{z}_t + \mathbf{W}_c^h \cdot \mathbf{h}_{t-1} + \mathbf{b}_c) \\
\mathbf{c}_t &= \mathbf{i}_t \odot \tilde{\mathbf{c}}_t + \mathbf{f}_t \odot \mathbf{c}_{t-1} \\
\mathbf{h}_t &= \mathbf{o}_t \odot \tanh(\mathbf{c}_t),
\end{aligned} \tag{5}$$

where the operator $\odot$ refers to the Hadamard product; $\mathbf{W}$ and $\mathbf{b}$ are the corresponding weight matrices and bias vectors, respectively. Since it is a binary classification problem, the output of the last LSTM cell $\mathbf{h}_T$ then passes a dense layer with one neuron to map the output results into a probability:

$$p_{\mathrm{tcrnn}} = \mathrm{sigmoid}(\mathbf{w}_d \cdot \mathbf{h}_T + b_d), \tag{6}$$

where $\mathbf{w}_d$ and b_d are the weight vector and bias, respectively.

D. Support Vector Machine

SVM aims at finding a linearly separable hyper-plane by mapping the features into a higher dimension feature space, with the help of support vectors. It has been proven to be the most effective classification algorithm among all traditional machine learning algorithms for sensing-result fusion in [12]. Let $\phi(.)$ denote the non-linear mapping function, the convex optimisation problem for maximising the margin of classification while minimising the sum of prediction errors can be formulated as:

$$\min \quad \frac{1}{2}||\mathbf{w}||^2 + C_{\mathrm{svm}} \sum_{i=1}^{N} \mathbb{I}_{\{\delta_i > 1\}} \tag{7}$$

$$\text{s.t.} \quad y_i^* \cdot [\mathbf{w} \cdot \phi(\mathbf{x}_i) + b_0] \geqslant 1 - \delta_i \tag{8}$$

$$\delta_i \geqslant 0, \quad \text{for } i = 1, ..., N, \tag{9}$$

where δ_i is the slack variable for measuring the margin classification error; $\mathbb{I}_{\{X\}}$ is the indicator function which is zero if X is false; and is one, otherwise. If a miss-classification appears, δ_i is set to be larger than one. $\mathbf{w}$ is the weight vector and b_0 is the bias. The parameter C_{svm} is used as a soft margin constant for regularisation. The above optimisation problem is is a quadratic programming problem, which can be further solved by using sequential minimal optimisation method. Finally, the Platt scaling method is applied to transforms the classified output into probability. The estimated probability of $\hat{\mathbf{x}}$ is in the class $\hat{y}^* = 1$ is given as follows:

$$p_{\mathrm{svm}} = \mathrm{P}(\hat{y}^* = 1|\hat{\mathbf{x}}) = \mathrm{sigmoid}(a \cdot \hat{y} + b), \tag{10}$$

where a and b are two scaling parameters learnt by fitting the sigmoid function; $\hat{y}$ is the soft decision function calculated by solving the above optimisation problem.

E. Reputation Based Weighted Majority Vote

To find the explicit linear relationship between the output and inputs, we propose a reputation based learning method, which is called RWMV. The weight assigned to each SU is based on its historical reputation. The general steps of our proposed RWMV are given in Algorithm 1. Let $r_j^{(i)}$ denote the ith SU's reputation at jth iteration. First, all SUs' reputations are initialised to zero. Then during training, the RWMV increases $r_j^{(i)}$ by one if SU_i's local sensing result $d_j^{(i)}$ is equal to the label y_j^*, and decreases by a penalty constant k if they are different. During the test phase, the fusion result as a probability is calculated by adding all SUs' weighted local decisions and passed by the sigmoid function to map them into a probability.

F. Logistic Regression

The LR algorithm is a commonly used effective meta learner in EL frameworks. It automatically learns the optimal weights of base learners' prediction results. The advantages of using LR include its simplicity, stability and the ability to prevent overfitting in small-scaled data sets without much hyperparameter tuning.

Let $\mathbf{x}_{\mathrm{base}} = \{p_{\mathrm{tcrnn}}, p_{\mathrm{svm}}, p_{\mathrm{rwmv}}\}$ denote the OOF prediction vector of the base learners, where p_j is the predicted probability of the corresponding base learner j. The output probability of LR is defined as:

$$p_{\mathrm{lr}} = \mathrm{sigmoid}\left(\mathbf{w}_{\mathrm{lr}} \cdot \mathbf{x}_{\mathrm{base}} + b_{\mathrm{lr}}\right), \tag{11}$$

where $\mathbf{w}_{\mathrm{lr}}$ and b_{lr} are learnable weight vector and bias, respectively. The final binary classification decision is determined by comparing the probabilistic output with a threshold (e.g., 0.5).

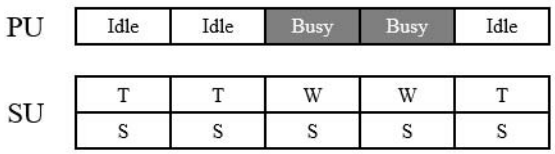

Fig. 4. Listen-And-Talk protocol, where 'S', 'T' and 'W' refer to the sensing period, transmission period and waiting period, respectively.

IV. Performance Analysis of Two Full-Duplex Transmission Protocols

In this section, we study SU's analytical performance of the LAT protocol, as shown in Fig. 4. We first derive the channel idle and busy probabilities, and then the spectrum waste and collision probabilities in LAT. The sensing error probabilities used in the following derivations are all determined by the fusion method applied at the FC.

A. Channel Idle and Busy Probabilities

Let l_0 and l_1 denote the instant length of idle and busy periods, l_1 and its corresponding average length L_1 can be written as:

$$l_1 = \frac{\lambda_a}{\lambda_t - \lambda_a} l_0 + 1, \quad L_1 = \frac{\lambda_a}{p(\lambda_t - \lambda_a)} + 1. \tag{12}$$

Using the Bayes' theorem, PU's idle and busy probabilities $\mathrm{P}(s=0)$ and $\mathrm{P}(s=1)$ are given by:

$$\mathrm{P}(s=0) = \frac{\lambda_t - \lambda_a}{p(\lambda_t - \lambda_a) + \lambda_t}, \ \mathrm{P}(s=1) = \frac{p(\lambda_t - \lambda_a) + \lambda_a}{p(\lambda_t - \lambda_a) + \lambda_t}. \tag{13}$$

B. Spectrum Waste Probability

Since the sensing decision is made one slot ahead in LAT, the spectrum waste probability contains two kinds of time slots: a) the time slots when the channel remains idle and FC falsely alarms it was busy in the last slot, and b) the slots when the channel occupancy status changes from busy to idle while FC correctly decided it was busy in the last slot. Therefore, the spectrum waste probability in LAT is derived as follows:

$$P_w = \frac{(\lambda_t - \lambda_a)(1-p)}{p(\lambda_t - \lambda_a) + \lambda_t} \cdot P_f^{(\mathrm{FC})} + \frac{p(\lambda_t - \lambda_a)}{p(\lambda_t - \lambda_a) + \lambda_t} \cdot P_d^{(\mathrm{FC})}, \tag{14}$$

where $P_f^{(\mathrm{FC})}$ and $P_d^{(\mathrm{FC})}$ are the error probabilities at the FC after sensing result fusion.

C. Collision Probability

The collision probability in LAT also contains two kinds of slots: a) the time slots when the channel remains busy and FC decided it was idle in the last slot, and b) the slots of PU's arrival in which the FC decided the channel was idle in the last slot. The collision probability is then given by:

$$P_c = \frac{\lambda_a}{p(\lambda_t - \lambda_a) + \lambda_t} \cdot \overline{P_d}^{(\mathrm{FC})} + \frac{p(\lambda_t - \lambda_a)}{p(\lambda_t - \lambda_a) + \lambda_t} \cdot \overline{P_f}^{(\mathrm{FC})}, \tag{15}$$

where $\overline{P_f}^{(\mathrm{FC})}$ and $\overline{P_d}^{(\mathrm{FC})}$ are the complimentary probabilities.

TABLE I
AUC Scores for different Number of Training Samples and PU's Active Probability in LAT protocol

Fusion Methods	Number of Training Samples			
	1000		10000	
	$p = 0.05$	$p = 0.1$	$p = 0.05$	$p = 0.1$
EL	0.986	0.976	**(0.988)**	**[0.979]**
TCRNN	0.956	0.941	**(0.983)**	**[0.969]**
SVM	0.958	0.958	**(0.960)**	**[0.959]**
RWMV	**(0.953)**	**[0.956]**	0.952	0.953
MV	**(0.524)**	**[0.523]**	0.511	0.512

V. Simulation Results

Unless stated otherwise, we use the following parameter values for simulation and numerical results. We set $M = 10$, $M_t = 4$, $M_p = 3$, $M_s = 3$, $\chi = 0.1$, $\lambda_a = 2$ packet/slot, $\lambda_t = 6$ packet/slot, SNR received by TSU_1 from itself $\alpha_s = 15$ dB, SNR received by SU_i from PU $\alpha_{s_i,p} = -13$ dB, SNR received by SU_i from TSU_1 $\alpha_{s_i,s_1} \in [-10, 0]$ dB, SNR received by SU_i from PUE attacker $\alpha_{s_i,a} \in [0, 3]$ dB, $p_0^{\mathrm{PUE}} = 0.6$, $p_1^{\mathrm{PUE}} = 0.1$, $p_0^{\mathrm{SSDF}} = p_1^{\mathrm{SSDF}} = 1$, the RNN window size $w = 10$. The number of training and test samples are 5000 and 10000, respectively.

A. Prediction Performance Analysis

One commonly used metric for binary classification methods is the Area Under Curve (AUC) score. AUC score provides an aggregate measure of performance across all possible classification thresholds. A high AUC score demonstrates the classifier has a strong classification capability.

In Table I, we list the AUC scores for the different number of training samples and PU's active probability for each fusion methods. The bold numbers in parenthesis and square brackets refer to the highest AUC score of $p = 0.05$ and $p = 0.1$ in that row, respectively. It can be seen that larger data sets lead to higher AUC scores for EL, TCRNN and SVM, whilst RWMV works better on a smaller data set. Specifically, the AUC score of TCRNN increases dramatically with the size of the training set, which shows the strong capability of deep learning-based methods in a larger data set. However, its results on smaller data sets are worse than traditional machine learning methods such as SVM. Our proposed EL framework leverages the pros and cons of each method and outperforms each of them with a relatively high and stable prediction performance on both small and large data sets. Furthermore, a smaller p results in a higher value of AUC score, which indicates that PU's activity pattern can be predicted more easily if it changes more slowly.

Figure. 5 depicts the detection probability, false-alarm probability and classification time comparison for different fusion methods. We constrain the detection probability at the FC $P_d^{(\mathrm{FC})} \geqslant 0.9$ to protect the communication quality of PU. The decision threshold of each method is accordingly adjusted. From Fig. 5 we can see that the EL gives the lowest false-alarm probability among all methods. The MV method has a

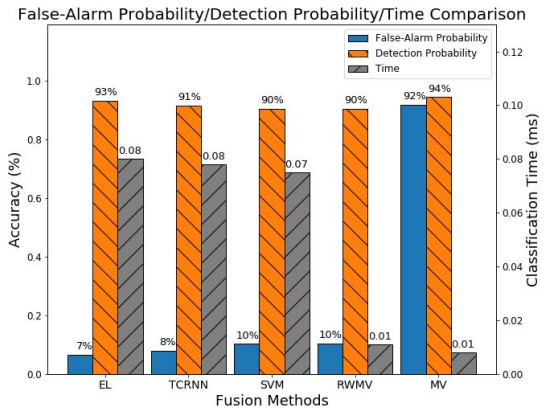

Fig. 5. Detection probability, false-alarm probability and classification time comparison for different fusion methods with constrained detection probability in LAT protocol.

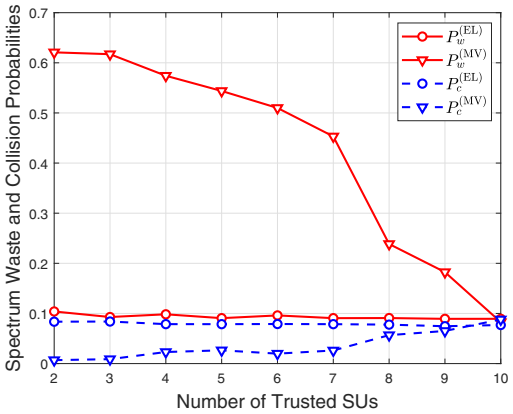

Fig. 6. Spectrum waste and collision probability comparison for EL framework and MV in LAT protocol.

very poor prediction performance in terms of extremely high false-alarm probability in such a complicated scenario.

The prediction time for all fusion methods is much lower than the sensing duration. Since the prediction of base learners can be done in parallel, our proposed EL framework doesn't require a long time whilst it provides an up to 85% reduction of false-alarm probability compared with conventional MV, and 4% reduction compared with three single-model base learners.

B. LAT Performance Analysis

Figure. 6 illustrates the spectrum waste and collision probabilities in LAT for our proposed EL framework and conventional MV. It can be seen that the spectrum waste probability of MV is very high when the number of TSUs is small though its collision probability is low. This indicates that the MV based fusion method can be easily misled to decide that the channel is occupied due to malicious attacks. However, our proposed EL framework is much more stable in both probabilities with any number of TSUs compared with MV method.

VI. Conclusion

In this paper, we proposed a novel EL framework for cooperative sensing decision fusion, which is robust with accuracy against malicious attackers and interference in FD-CRN. First, we designed a deep learning structure, TCRNN, to extract the temporal-correlation features. An SVM learner was applied to figure out the high-dimensional implicit feature representations whilst a learning-based RWMV algorithm was proposed to learn the explicit linear relationships between the inputs and the output. An LR meta learner was then trained to assign weights to the base learners' results. Then we derived the channel idle and busy probabilities, the spectrum waste and collision probabilities in LAT. By testing the classification performance, we demonstrated the superiority of our proposed EL framework in terms of high and robust accuracy, low time cost, low spectrum waste and collision probabilities with any number of TSUs. It outperforms single-model based fusion methods and conventional MV based fusion strategy.

Acknowledgment

This research was supported by the Engineering and Physical Science Research Council (EPSRC) through the SENSE grant EP/P003486/1.

References

[1] J. Mitola, G. Q. Maguire *et al.*, "Cognitive radio: making software radios more personal," *IEEE personal communications*, vol. 6, no. 4, pp. 13–18, 1999.

[2] S. M. Mishra, A. Sahai, R. W. Brodersen *et al.*, "Cooperative sensing among cognitive radios." in *Icc*, vol. 6. Citeseer, 2006, pp. 1658–1663.

[3] D. Teguig, B. Scheers, and V. Le Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks," in *2012 Military Communications and Information Systems Conference (MCC)*. IEEE, 2012, pp. 1–7.

[4] Y. Zhang, J. Hou, V. Towhidlou, and M. Shikh-Bahaei, "A neural network prediction based adaptive mode selection scheme in full-duplex cognitive networks," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2019.

[5] Y. Liao, T. Wang, L. Song, and Z. Han, "Listen-and-talk: Protocol design and analysis for full-duplex cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 656–667, Jan 2017.

[6] Yang Li and Q. Peng, "Achieving secure spectrum sensing in presence of malicious attacks utilizing unsupervised machine learning," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Nov 2016, pp. 174–179.

[7] Yun Liao, Kaigui Bian, Lili Ma, and Lingyang Song, "Robust cooperative spectrum sensing in full-duplex cognitive radio networks," in *2015 Seventh International Conference on Ubiquitous and Future Networks*, July 2015, pp. 66–68.

[8] R. Chen, J. . Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, April 2008, pp. 1876–1884.

[9] P. Zuo, X. Wang, W. Linghu, R. Sun, T. Peng, and W. Wang, "Prediction-based spectrum access optimization in cognitive radio networks," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2018, pp. 1–7.

[10] W. Afifi and M. Krunz, "Exploiting self-interference suppression for improved spectrum awareness/efficiency in cognitive radio systems," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 1258–1266.

[11] T. G. Dietterich *et al.*, "Ensemble learning," *The handbook of brain theory and neural networks*, vol. 2, pp. 110–125, 2002.

[12] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, "Machine learning techniques for cooperative spectrum sensing in cognitive radio networks," *IEEE Journal on selected areas in communications*, vol. 31, no. 11, pp. 2209–2221, 2013.