IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 14, 2022, accepted April 8, 2022, date of publication April 12, 2022, date of current version April 20, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3166844

Proactive Radar Protection System in Shared Spectrum via Forecasting Secondary User Power Levels

SU P. SONE[1], JANNE LEHTOMÄKI[1], (Member, IEEE), ZAHEER KHAN[1], (Member, IEEE), KENTA UMEBAYASHI[2], (Member, IEEE), AND ZUNERA JAVED[1]

[1]Centre for Wireless Communications (CWC), University of Oulu, 90014 Oulu, Finland
[2]Umebayashi Laboratory, Department of Electrical and Electronic Engineering, Tokyo University of Agriculture and Technology, Tokyo 184-8588, Japan

Corresponding author: Su P. Sone (sone.supyae@oulu.fi)

This work was supported in part by the Infotech Oulu, and in part by the Academy of Finland 6Genesis Flagship under Grant 318927.

ABSTRACT Spectrum sharing in radar bands with interference forecasting for enhanced radar protection can help design proactive resource allocation solutions which can achieve high data rates for wireless communication networks on one hand and help protect the incumbent radar systems. We consider radar spectrum sharing in 5.6GHz where a weather radar operates as a primary system and the dominant secondary system is an enterprise network consisting of access points (APs) in a university campus. Our work models transmit the power of the APs as a time series with multinomial distribution based on real collected data. The aggregated interference due to the transmissions from the APs at the radar is forecasted using a long short-term memory (LSTM) based neural network. Monte Carlo dropout is utilized to generate prediction intervals that capture the uncertainties in the interference from the APs. Finally, by using both average and upper limits of predicted interference time series a cloud-assisted efficient sharing and radar protection algorithm is proposed. Tracking the rotating radar is not required in the proposed system. The results show that the proposed efficient sharing and radar protection system ensures better radar protection and increased throughput for wireless communication users.

INDEX TERMS Aggregated interference, DFS, LSTM, neural networks, radar, real network data, spectrum sharing, time series forecasting, WLAN.

I. INTRODUCTION

Innovative new wireless applications are increasing the spectrum demands of both beyond 5G cellular networks and wide local area networks (WLANs), such as enterprise networks. Spectrum sharing between wireless communications and other wireless technologies is one solution to address the growing spectrum demand [1]. TV White Space (TVWS) is one well-known example of spectrum sharing. Radar bands have generated immense interest in being another candidate for sharing large amounts of spectrum [2]. Radar spectrum in L-band (960-1400MHz), S-band (2700-3650MHz), and C-band (5-5.85GHz) have become good potential candidates for spectrum sharing with different wireless technologies as current networks, such as 4G Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX) and WLAN are also operating in one of these bands [3].

The challenge of using radar bands for spectrum sharing is that most of the radar systems have their critical functions, such as in military radars, air surveillance radars, and meteorological radars. Therefore, it is crucial to know the spectrum usage characteristics of a particular radar to design the appropriate spectrum sharing model to maximize the usage of the shared spectrum while protecting the primary radar operations. Among various radar systems, weather radars can be found in many parts of the countries near urban areas. Despite of the communication benefits to society of the secondary network, the priority of the spectrum sharing mechanism is to protect the main radar operation from any potential interference coming from the secondary network. The dynamic frequency selection (DFS) model is standardized for radar protection by detecting a radar at the user side. However, it is not optimal due to its 1 min channel

The associate editor coordinating the review of this manuscript and approving it for publication was Yiming Huo.

availability check (CAC) time and 30 min channel silence period after detecting a radar signal [4].

The secondary users need to interrupt their transmissions for the instants of time only when the radar signal is detected in temporal DFS (DFS-T) instead of leaving the radar channel as in the conventional DFS [5]. Nevertheless, DFS and DFS-T require sensing the signal and tracking the rotation of a weather radar which is found out to be with quasi-periodic rotation in [6]. Hence, a recent study [7] recommended to use of advanced cloud-based technologies such as a Radio Environment Map (REM) repository with an online database to receive the interference information from sensors and a spectrum manager to execute the dynamic temporal spectrum sharing. Most of the frameworks currently used for radar protection depend mainly on the spectrum monitoring sensors called environmental sensing capability (ESC). ESC equipment is deployed in the vicinity of the protection zones to accurately detect incumbent user transmissions [8]. Moreover, there is an extended version of ESC which can do multi-functions such as detecting the presence of radar, measuring any interference from secondary users for incumbent protection, and measuring airtime utility of secondary users [7]. These sensors can periodically update the interference information at the radar and send an alert to the cloud-based REM repository in case exceeding the interference limit.

However, these radar protection systems cannot guarantee that the aggregated interference at the radar caused by the secondary system will not exceed the tolerable interference threshold of a radar due to the delays involved in the process of sensing, processing, and reporting. One possible solution is to apply an interference forecasting mechanism using machine learning algorithms in a cloud-based REM repository. In general, the interference from the wireless systems can be measured or generated by using realistic models and stored as a time series in the REM repository. Medium-to-short-term interference levels can be forecasted using these historical time series data. Our recent work [9] investigated various time series forecasting techniques for wireless traffic usage in an enterprise network and showed that machine learning methods have many advantages, such as being able to utilize extra feature information. In [10], the forecasting performances of machine learning methods are improved and proved that physical layer data has more predictive power than network layer data in the time series forecasting aspect.

Rather than making only point forecasts, LSTM based neural networks can also estimate the degree of uncertainty in forecasted wireless interference values via the use of prediction intervals (PIs). A PI is a type of confidence interval used with predictions; it is a range of values that predicts the value of a new observation, based on an existing model. In spectrum sharing with radar band, the quality-of-service (QoS) and the data rate of the secondary system are also important to consider, besides being able to accommodate more users in a secondary network. The required QoS and data rate can be provided by combining the main channel outside radar bands and a channel in radar bands using the channel bonding (CB) technique which was introduced to fulfill the IEEE 802.22 requirements on the speed in TVWS cognitive radio systems [11]. There are two main types of CB methods: contiguous CB which aggregates the adjacent available channels to combine as a common larger channel for better data rate, and non-contiguous CB which allows to aggregate the available channels even if they are not adjacent. Non-contiguous CB is widely used in cognitive radio technologies due to its flexibility and higher data rate than contiguous CB [12].

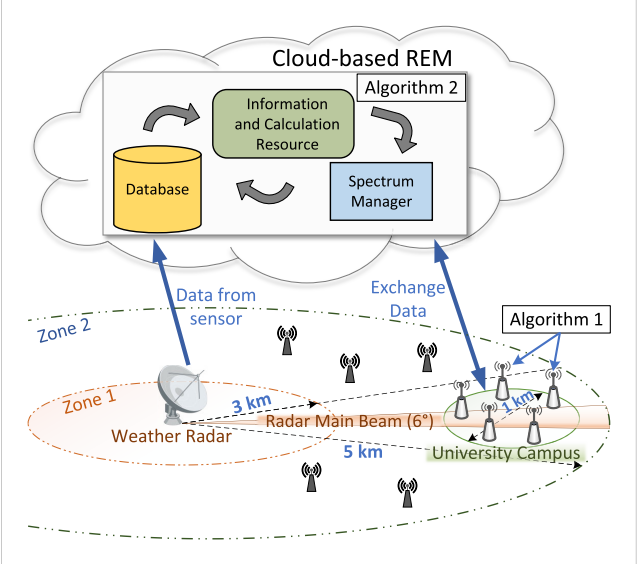


FIGURE 1. Proposed system diagram.

Therefore, we propose an efficient sharing and radar protection system which consists of two parts of algorithms with the aid of cloud-based REM using predicted time series of interference at the radar and non-contiguous channel bonding technique. The novel efficient sharing and radar protection system optimizes the data sharing of an enterprise network and ensures radar protection without requiring tracking the quasi-periodic radar rotation. The overview of the proposed system diagram is shown in Fig. 1. The main contributions of this paper are:

1) The model of transmission power (TP) time series for all access points (APs) is proposed based on real measurements collected from the University of Oulu by mapping the number of connected users to the measured TP data using multinomial based fit.
2) By considering the stochastic nature of neural networks, the upper and lower limits of predicted interference time series are also obtained to utilize in the radar protection system.
3) A novel efficient sharing and radar protection algorithm is proposed and compared with other radar protection mechanisms such as DFS and real-time protection without interference forecasting.

The rest of the paper is organized as follows. Section II provides the previous literature related to the spectrum sharing model of radar systems, time series forecasting, and channel bonding methods. The description of the collected dataset from our enterprise network as well as detailed explanations of time series modeling such as TP mapping and interference at the radar can be seen in Section III. Section IV presents the interference time series forecasting methods and performance metrics used in this paper. The novel efficient sharing and radar protection algorithm is proposed in Section V. The complete simulation system is evaluated by comparing it with others in Section VI. Finally, we conclude in Section VII by discussing the outcomes and the future direction of this paper.

II. RELATED LITERATURE

After several initiatives of spectrum sharing techniques such as TVWS, unlicensed wireless access search for underutilized licensed spectrum bands has increased and radar C-band which operates in 5GHz has become popular for spectrum sharing with enterprise WLAN networks. From various types of radars, weather radars that use C-band can be found widely across the countries near the urban area. For radar channels in C-band, dynamic frequency selection (DFS) is widely used to enable spectrum sharing between a primary system with the licensed spectrum and the unlicensed secondary devices [4]. However, it is not efficient in searching for available spectrum since it requires long sensing periods and long non-occupancy periods. In [6], the characteristics and behaviors of a particular weather radar in Finland are studied. They proved that radar patterns are not always periodic but mostly quasi-periodic which is not reliable for tracking radar rotation and sensing-based temporal spectrum sharing models. Hence, our proposed system is designed to protect the radar without requiring to track the rotation of a weather radar.

In general, the priority of shared spectrum access is to protect the primary user with a licensed spectrum. In zone-based sharing with radar band, REM repository is used to provide the sharing rules to users in secondary network by collecting dynamic information of radar and interference at radar since [6] stated that sensing-based sharing model does not work in a weather radar system. Moreover, the Internet of Things (IoT) has become a huge dynamic global network and the demand for connectivity for IoT devices is rising endlessly [13]. The REM architecture for shared spectrum is also proposed in [14] to increase the connectivity of IoT devices in both 5G networks and enterprise networks. It also explained the facts for the zone-based shared access (SA) suitability, implementation challenges, and spectrum goodness metrics for IoT applications. Therefore, a zone-based sharing system with a cloud-based REM repository is used in this work to collect the data and execute the forecasting algorithm for the prediction of interference at the radar.

The detailed mechanism of the REM elements to utilize for spectrum sharing in radar systems is also investigated in [15]. Instead of channel sensing at the secondary users' side, using a sensor at the radar to measure the interference has more guarantee of radar protection. The detailed implementation of an FPGA-based spectrum monitoring ESC sensor for shared access with rotating radars, which is high-speed and low-cost compared to other ESCs, is proposed in [16]. Upon receiving the alert of interference exceeding the limit from the ESC sensor implemented at the radar, the spectrum manager in the REM repository updates the sharing rules based on the utilized spectrum sharing model [7]. It also introduced two different database-assisted spectrum sharing mechanisms such as a distributed unified channel access (UCA) method and a cloud-based UCA method. In these types of real-time radar protection systems without forecasting interference, there is a drawback that the sharing rules are updated only when the interference at the radar has already exceeded the threshold. To overcome this problem, in this paper, time series of predicted interference at the radar is utilized to help in proactive spectrum assignments for the APs of an enterprise network.

In [5], the authors considered aggregated interference to the radar for interference threshold calculated under temporal DFS (DFS-T), which is the modified version of the DFS system, with a cooperative sharing scheme. They modeled the interference from cognitive users for both radar antenna main lobes and side lobes by using link budget power calculation. A mathematical model for the aggregated interference to the radar by WLAN devices is presented and the WLAN devices are considered uniformly distributed within a circle of radius R in [17]. It also stated that the adverse effect of aggregated interference is only shown in an area with more than 10 WLAN devices per square kilometer. The simulation model of cellular systems sharing the same spectrum with rotating radar can be seen in [18]. The parameters values used for weather radar, such as tolerable interference-to-noise ratio (INR) and so on, are also stated in this literature. However, cognitive users, which are WLAN devices in [5], [17], and [18], still need to sense the radar signal as in conventional DFS system. In our proposed system, the aggregated interference is also considered but the secondary users do not need to sense the radar signal since the sharing rules are updated by the cloud-based REM.

Theoretical and empirical performance comparisons of different forecasting methods for wireless traffic data of an enterprise network can be seen in our recent work [9]. The detailed time series pre-processing, analysis, and stationarity testing steps are also explained. Previous work [10] also proved that physical layer data such as channel utilization or transmit power time series have more predictive power and higher accuracy in forecasting using LSTM than network-level data. For the radar protection system, we need to capture the uncertainty of the forecasting model to ensure that the radar is fully protected. The machine learning models used in [9] and [10] are the standard neural networks that do not

consider the uncertainty of their outputs. To measure the uncertainty range such as upper and lower PIs of forecasting models, the Monte-Carlo dropout (MC-dropout) method is introduced in [19]. MC-dropout is the method that simply applies the Monte Carlo loop, a class of computational algorithms that rely on repeated random sampling to obtain a distribution of some numerical quantity, at testing time. The usages of MC-dropout and its benefits can be seen in [20] and [21]. Hence, LSTM with MC-dropout is used to compute the averaged prediction and PIs of the interference at the radar time series.

To maximize the QoS and the data rate of connected secondary users, the non-contiguous CB technique can be utilized also in the spectrum sharing model of the weather radar system. The recent work [22] proposed distributed and coordinated channel bonding methods under signal-to-interference-noise ratio (SINR) and collision-protocol models. The method called pi-Aut is under the SINR-protocol model and pi-sig is under the collision-protocol model. Both proposed methods are tested in two scenarios such as combining only adjacent channels (contiguous CB) and combining both adjacent or non-adjacent channels (non-contiguous CB). The SINR and collision-protocol models designed in [22] are also suitable for shared access in rotating weather radar systems, and the SINR model with non-contiguous CB is used in our proposed system. The results showed that the non-adjacent channels scenario has a higher averaged sum data rate in [22] and [12] also proved that non-contiguous CB is more flexible and can provide a higher data rate than contiguous CB.

III. NETWORK TIME SERIES DATA MODELS

A. DESCRIPTION OF COLLECTED REAL NETWORK DATA

In our proposed efficient sharing and radar protection system, the collected channel occupancy rate time series, which is the physical layer data of each AP, is used to calculate and predict the total interference level caused by secondary users at the radar. We have access to collect the channel occupancy data from only seven APs operating with high traffic transmissions which are deployed in the student lounge area of the University of Oulu, Finland. Physical layer data represents the occupancy percentage of a radio frequency (RF) channel within a particular period t. The APs were configured to collect the channel occupancy data of a 5.6GHz WLAN channel at every 5-minute interval between January 22 to February 22, 2020. Hence, each physical layer data time series has over 8000 data points. We also collected network layer data from the APs deployed around the Linnanmaa campus of the University of Oulu due to the limitation in physical layer data collection.

The received and transmitted traffic data, the number of connected users, locations, and the names of each AP of a total of 470 APs, including both types of APs using 2.4GHz and 5.6GHz, around the campus are collected as the network layer dataset. There are around 50 APs that are using 5.6GHz in the University campus. Each data point of a total of 5040 of the time series provides the measurement at every 10-minute interval within the period of January 5 to February 22, 2020. The transmitted traffic data, which is known as downlink data, is considered as the network traffic utilization (TU) and it always dominates the received traffic data at every APs. For this reason, we focus only on the interference from downlink transmissions. By assuming that transmission occurs at the maximum allowed power level (P_t), channel occupancy percentage data indicates the power utilization percentage (TP_{per}) of the total transmissions and transmission power from all kinds of sources operating on the same specific channel within period t can be defined as, $\mathrm{TP} = \mathrm{TP}_{per} \times P_t$.

The channels utilized in an enterprise network are shared among multiple wireless technologies so that the usage of other IoT devices excluding users connected to the APs around the campus with the same channel can be included in the measured data. Hence, the TP of secondary users (or APs) mentioned later in this work is considered as downlink transmissions from the APs to the connected users which are mainly dominant, and the other possible transmissions from IoT devices on the same channel. Along with TU data, the number of connected users to each AP is also collected since it is one of the important factors for the enterprise network, and in the next subsection, we show how to stochastically map the number of users to TP data. We focus our investigation on only weekdays (working days) data of both physical layer and network layer data series as in [9].

B. TP MAPPING

As we studied the relation between TU data and the number of connected users time series in our previous work [9], the Pearson correlation between TU and connected users of an AP is significant for highly utilized APs although a small number of users with heavy data usage can contribute most of the traffic in APs. Therefore, we investigate the relation between the TP data and the number of connected users for seven APs that are deployed in the crowded area of the University in this work. Surprisingly, the two time series have a similar pattern and are fitted together for most of the highly utilized APs, an example is shown in Fig. 2. We proved that most of the highly utilized APs have similar traffic and users patterns in [9] and most of the APs using 5.6GHz channels are included in the highly utilized APs category. Hence, we can model the TP time series for other APs with 5.6GHz channels by mapping the numbers of connected users to the TP time series of collected seven APs. It is important to note that the mapping is not one-to-one but stochastic mapping which gives a distribution of TP values for each number of connected users. This reflects reality since channel usage by users varies randomly.

To be able to calculate and predict the total interference caused by the University network, we need to collect the historical data of shared channel occupancy of all APs. Despite being able to collect TP data of only seven APs in the

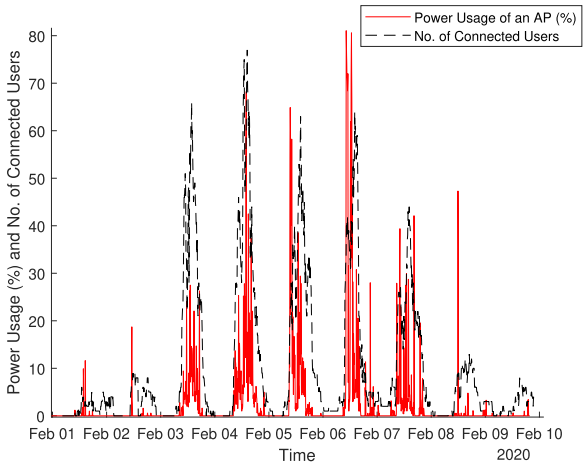


FIGURE 2. The collected power usage percentage and the number of connected users for an AP vs time.

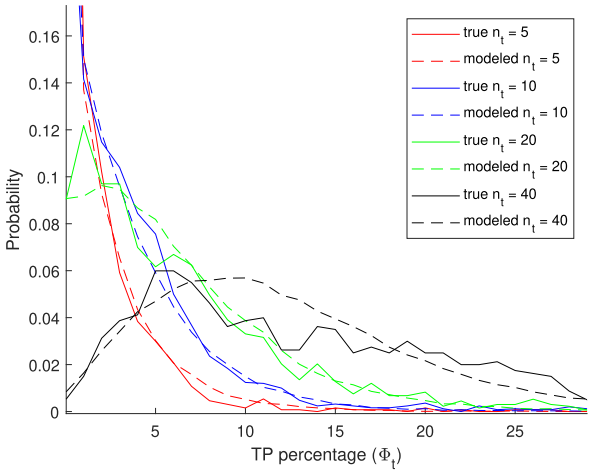


FIGURE 3. Comparison of differences between true TP data and TP data generated from the model for specific n_t values.

University, our investigation shows that it is possible to model the TP time series for others 5.6GHz APs of the University. Since the TP data series have a fitting shape with the number of connected user time series and not all connected users are utilizing an equal amount of power usage level at a time, the TP time series can be modeled as follows. There is also no strict limitation for the maximum TP percentage for a user.

If we define TP percentages $i = 0, 1, \ldots, k$ for each user with k maximum TP per user, no. of total connected users at time t as n_t and set the optimal weights as $P = p_0, p_1, \ldots, p_k$, we can model the number of users $U = u_0, u_1, \ldots, u_k$ using i^{th} TP percentage at time t with multinomial distribution as $U \sim Mult(n_t, P)$. Then, the total TP percentage of all users at time t (for a given AP) can be expressed as:

$$\Phi_t = \sum_{i=0}^{k} i u_i, \tag{1}$$

where $\sum_{i=1}^{k} u_i = n_t$. The weights, $p_0, p_1, \ldots, p_k$, are modeled as natural exponential decaying function since there can be only a few users with heavy usage while others are just connected.

It is modeling with probability p_i that a user is consuming i percentage of the channel in the time domain. Then we use multinomial distribution to get random channel usage from n_t users (where the number of users data is coming from our comprehensive measurements in the University of Oulu). For example, assume that the studied AP has 10 connected users. Now, the multinomial output can be [5 3 2], which means that 5 connected users are not using the channel, 3 users are using the channel with 1% utilization, and 2 users are using the channel with 2% utilization. Total utilization is then $5 \times 0 + 3 \times 1 + 2 \times 2 = 7$ percent. Since the multinomial distribution is random, another realization of the multinomial variable can lead to another output (for example [4 4 2], now the channel utilization would be $4 \times 0 + 4 \times 1 + 2 \times 2 = 8$ percent). This means that the mapping from several connected users to time-domain utilization of the physical channel is stochastic. The idea in the selecting of the weights p_i is to minimize the difference in the observed distribution of the TP data for a given number of users and the distribution coming from the use of the multinomials.

However, brute force optimization to get minimum difference between the true TP data and TP data generated from the model, is very difficult due to computational complexity. To reduce the computational time, one possible solution is to model the natural exponential function with 2^{nd} degree polynomial for each weight value such as

$$p_x = \exp(c_2 x^2 + c_1 x + c_0), \quad x = 0, 1, \ldots, k, \tag{2}$$

where c_0, c_1, c_2 are polynomial coefficients which are the variables to optimize. Now we have reduced the number of variables to optimize from k to only three which makes the problem much simpler.

However, the optimized differences between true TP data and TP data generated from the model with 2^{nd} degree polynomial for each weight value become higher than optimizing all of the k weights. After comparing the weight values from two different optimization schemes, we found out that the slope between p_0 and p_1 is huge and it cannot be modeled with 2^{nd} degree polynomial for the initial weight p_0. The variable p_0 is the probability that a connected user is not using the channel. In fact, by modeling the initial weight p_0 as a separate variable and modeling the rest of the weights with the natural exponential function with 2^{nd} degree polynomial as above, not only the computation time for optimal weights is reduced but also the minimum differences between true TP data and TP data generated from the model as shown in Fig. 3 are smaller than before. The variables p_0, c_0, c_1 and c_2 are optimized using nonlinear minimization method called Nelder-Mead simplex method [23]. The weights c_0, c_1 and c_2 are fed to the polynomial model, equation (2), in order to get the probabilities p_x for $x = 1, 2, \cdots, k$ where k is the assumed maximum time domain utilization per user.

C. INTERFERENCE TO RADAR SYSTEM MODEL

We consider a ground-based meteorological radar operating at 5610 MHz band which is located at certain kilometers away from the Linnanmaa campus of the University of Oulu, Finland. This weather radar is equipped with an extended ESC sensor that can measure the interference around the radar. We define three different zones for the radar [14], such as radar channel will not be used by APs in zone 1, radar channel can be used by certain rules to avoid the interruption of the radar communication in zone 2, and radar channel is free to use in zone 3. A circle with radius R_c km can represent the campus area within the radar zone 2 and a total of N active APs are operating in the 5.6GHz band inside the campus circle. The measured aggregated interference time series from the sensors can also be used in the efficient sharing and radar protection system. In this work, we generated the realistic aggregated interference at the radar time series by using real collected data from an enterprise network and using the model for other possible transmissions.

We mainly consider the downlink transmission of APs with an additive white Gaussian noise (AWGN) channel since it dominates the uplink transmission at every APs inside the campus as we mentioned above. We also consider possible downlink transmissions such as other active WLAN devices using the 5.6GHz band in radar zone 2 which are outside and a bit far from the campus area. With the use of the DFS algorithm, APs have to avoid using the channel in zone 2 when the radar signal is detected, and APs need to track the radar rotation with DFS-T algorithm [5]. However, the considered scenario for our proposed system is that even when the radar main beam is on the campus area, APs operating in the same band as radar will continue operating. This is possible as long as the predicted interference at the radar is not exceeded the pre-calculated interference threshold which can occur without service degradation of the radar. The proposed method can operate without quasi-periodic time-domain gaps leading to more usability of the spectrum sharing as compared to DFS-T.

Assuming the radar main beam is on the campus area, the parameters used in this work are provided in Table 2. If the required INR is set as -10 dB [18], this corresponds to the maximum tolerable interference threshold of -104 dB which is calculated as [24]:

$$Threshold = INR + N, \tag{3}$$

where, $N = -144(dBm) + 10\log_{10}(B_{radar})_{MHz} + \eta(dB)$. We defined path loss model to calculate interference where the received signal power from an i^{th} AP at the radar is:

$$Pr_i = P_0 \left(\frac{d_i}{d_{0i}}\right)^{-\alpha} \tag{4}$$

where, $d_i \geq d_{0i}$ is the distance between i^{th} AP and the radar. The reference received power P_0 at the close-in reference distance $d_{0i} = max\{\frac{2D^2}{\lambda_i}, D, \lambda_i\}$ of i^{th} AP is given by:

$$P_0 = \frac{P_{ti}\lambda_i^2}{(4\pi d_{0i})^2} \tag{5}$$

where P_{ti} is the transmit power of an i^{th} AP. Path loss between an i^{th} AP and the radar is defined as $L_{PL,i} = \frac{P_{ti}}{Pr_i}$. Then, the interference power at the radar caused by the secondary users at time t is [24]:

$$\Omega_{main} = \sum_{i=1}^{N} \frac{P_{ti} \cdot G_{ti} \cdot G_{radar(max)} \cdot B_{radar} \cdot \Phi_t}{B_{AP} \cdot L_{PL,i} \cdot L_{EL}} \tag{6}$$

where L_{EL} is the building entry loss of an AP located in the campus [25], B_{radar} and B_{AP} are bandwidths of radar channel and AP channel, respectively.

While the radar main lobe is on the university campus area, the interference at the radar is not only from the main lobe of radar but also from the side lobes which are directed to the outside of the campus area. To model the simulation, locations of the APs are generated randomly within the campus area (the exact locations of the APs do not significantly affect the aggregated interference at the radar) and we defined uniformly distributed M active WLAN devices outside of the campus area within zone 2 as in [17]. The TP utilization of these WLAN devices at time t, $\Phi_{t(side)}$, is also generated uniformly with a specific value, k, for maximum power utilization of each device. Hence, the interference power at the radar caused by the side lobes is [17]:

$$\Omega_{side} = \sum_{j=1}^{M} \frac{P_{tj} \cdot G_{tj} \cdot G_{radar(min)} \cdot B_{radar} \cdot \Phi_{t(side)}}{B_j \cdot L_{PL,j} \cdot L_{EL}} \tag{7}$$

The total interference from both the main and the side lobes at the radar at time t is $\Omega_t = \Omega_{main} + \Omega_{side}$. Then, the time series of total interference at the radar is generated by using this model.

TABLE 1. Parameters used in radar system model.

Parameter	Notation	Values
TP Percentage per User (Max)	k	30 %
No. of APs (Inside Campus)	N	50
No. of APs (Outside Campus)	M	10
Radius of Radar Zone 1	R_1	3 km
Radius of Radar Zone 2	R_2	5 km
Radius of the Campus Area	R_c	1 km
Radar Channel Bandwidth	B_{radar}	10 MHz
AP Channel Bandwidth	B_{AP}	20 MHz
Center Frequency	f_c	5.6 GHz
Wavelength (in meter)	λ	0.0536 m
Antenna Length	D	0.05 m
AP Transmit Power (Max)	P_t	180 mW
Radar Gain (Max)	$G_{radar(max)}$	44 dBi
Radar Gain (Min)	$G_{radar(min)}$	-21 dBi
AP Gain	G_t	6 dBi
Path Loss Exponent	α	3
Building Entry Loss	L_{EL}	11.5 dB
Noise Figure	η	10
Interference to Noise Ratio	INR	-10 dB

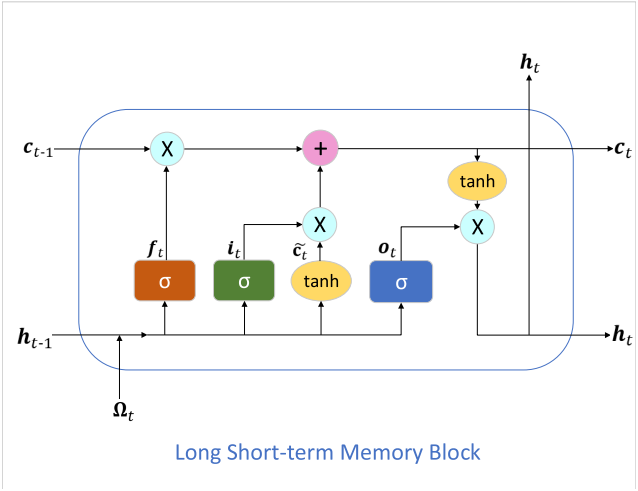


FIGURE 4. The block structure of LSTM.

IV. INTERFERENCE TIME SERIES DATA FORECASTING

A. FORECASTING METHOD

To be able to utilize advantages of machine learning methods we have used long short-term memory (LSTM) neural networks which gave the overall better performances in our previous works for the interference forecasting. LSTM is a variance of recurrent neural networks (RNNs). It is one of the most powerful tools for forecasting time series. LSTM can remember the previous information for a long time as in RNN and can also remove unnecessary data from its memory units. A LSTM block is formed as a cell with 3 main regulation structures which control the amount of information flow such as input gate ($\mathbf{i}_t$) to tell what new information is going to be stored in the cell state, forget gate ($\mathbf{f}_t$) to throw away unnecessary information from the cell state and output gate ($\mathbf{o}_t$) which is used to provide the activation to the final output of LSTM block [26]. One main characteristic of LSTM is that not only the states of the gates but also the candidate cell state ($\tilde{\mathbf{c}}_t$) is computed as the current cell state ($\mathbf{c}_t$) and the final output ($\mathbf{h}_t$). The block structure of LSTM can be seen in Fig. 4. The Sigmoid (σ) activation functions are used in the gates of a cell in LSTM to set the outputs of the gates between 0 and 1 where 0 represents that the gates are blocking everything and 1 represents that the gates allow all data to pass through them. The tanh activation functions which push the values passing through them to be in $[-1,1]$ are used to create a memory vector of the current candidate value ($\tilde{\mathbf{c}}_t$) and used in calculating the final outputs ($\mathbf{h}_t$) of the LSTM block.

The cost function (J) of LSTM model used in our work is the mean absolute error (MAE). If we denote all weights and bias (w, b) of the LSTM layer as w_{lstm}, b_{lstm}, and the dense layer as w_{dense}, b_{dense}, the objective function of LSTM model is defined as [27]

$$(\hat{w}_{lstm}, \hat{w}_{dense}, \hat{b}_{lstm}, \hat{b}_{dense}) = \arg\min_{w,b} J, \\ = \arg\min_{w,b} \frac{1}{N} \sum_{t=1}^{N} |Y_t - \hat{Y}_t|, \quad (8)$$

where N is the number of samples in a predicted period and $\hat{w}_{lstm}, \hat{w}_{dense}, \hat{b}_{lstm}, \hat{b}_{dense}$ are the updated weights and bias of LSTM and dense layers, respectively. Among different optimizers for LSTM model training, the Adam optimizer is selected in our work since it can converge faster than other optimizers [28]. The closed-form expressions for the LSTM layer can be found for example in our previous work [9].

By using our real collected network dataset described in Section III-(A), we generated the TP time series of all APs using 5.6 GHz channels with the TP mapping model introduced in Section III-(B). From equations (6) and (7) in terms of generated TP values, the time series of total interference at the radar at time t is calculated as $\Omega_t = \Omega_{main} + \Omega_{side}$, where Ω_{main} and Ω_{side} are the interference at the main lobe and the side lobe of radar respectively, caused by the secondary users at time t. The total interference at the radar is generated at every 10-minute interval for only weekdays (20 days) between January 22 to February 22, 2020. Hence, the time series dataset has over 2880 data points. The generated dataset used in the LSTM model is divided into a 75% (15 days) training dataset and a 25% (5 days) testing dataset.

We also used the features-like grid training data structure that we introduced in [10]. Moreover, the number of future time periods for which forecasts must be produced is defined as the forecast horizon (FH). Hence, one training input data sample is in the shape of a 6×6 grid for 1-hr FH which is defined as $X_t = \{x_t, x_{t+1}, \ldots, x_{t+5}\}$ where $x_{t+i} = \{\Omega_{t+i}, \Omega_{t+i+1}, \ldots, \Omega_{t+i+5}\}$. The corresponding target sample of training data to compare with predicted values of the model is in the shape of an 1×6 array for 1-hr FH as $Y_t = \{\Omega_{t+12}, \Omega_{t+12+1}, \ldots, \Omega_{t+12+5}\}$ in which the indexes of input and target samples are separated by 2×6 period not to be overlapped. Then, the corresponding predicted output sample can be denoted as $\hat{Y}_t = \{\hat{\Omega}_t, \hat{\Omega}_{t+1}, \ldots, \hat{\Omega}_{t+5}\}$ where $\hat{\Omega}_t$ is the predicted total interference power at the radar at time t.

For neural network learning models selection, it is common to use the K-fold cross-validation approach with K equal parts of randomly separated data. However, this K-fold cross-validation method cannot capture the temporal dependency of considered time series so that it is not suitable for time series forecasting [29]. Therefore, the time series cross-validation method called rolling origin evaluation in which $n-1$ chronological windows are used for training and n^{th} window is used as validation [30] is used in our work. The generated training dataset of total interference time series is split into 3 windows each with 5 days since our time series data is in daily periods and the hyper-parameters which gave the optimal averaged result of all windows are selected for the LSTM model used in our work. Optimizing the hyper-parameters of neural network-based machine learning methods is important. The steps and methods of optimizing the hyper-parameters for wireless network parameters are presented in our previous works [9] and [10].

TABLE 2. The optimal hyper-parameters for LSTM.

Hyper-parameter	Considered values
No. of layers (l)	2
No. of neurons (nn)	32
Dropout (d_p)	0.4, 0.5
Learning rate	0.001
Losses	MAE
Optimizer	Adam
Epochs	5000

For neural network-based machine learning methods, deep and narrow networks can create more complex feature representations of the current input than shallow and wide networks [31]. However, stacking many layers does not always help for time series forecasting. The optimal number of layers also depends on the data, hence, we first started with commonly used parameters for time series forecasting such as $\{1, 2, 3\}$ layers, $\{32, 64\}$ neurons of LSTM in each layer, and dropout value range from $\{0.1$ to $0.9\}$ where value 1 means no dropout is applied. The optimal hyper-parameters of LSTM for our time series optimized by using the time series cross-validation approach are presented in Table 2. The optimized LSTM model consists of 2-layer LSTM each layer with 32 nodes (memory cell size). Each LSTM layer is followed by an MC-dropout layer with a probability of 0.5 to prevent overfitting and to be able to compute the PIs of interference at the radar time series. Then, one dense layer is added as the output layer to directly output the predictions at the end. The linear activation function is used in the dense layer as it does not change the weighted sum of the input of the dense layer and returns the predicted numerical value which is suitable for regression-type predictive modeling problems [29]. In addition, the averaged accuracy values of 200 iterations are presented in this work by considering the stochastic nature of neural network.

B. MC-DROPOUT AND UPPER LIMITS OF FORECASTING

General regression and machine learning methods do not capture the model uncertainty [19]. The Monte Carlo dropout technique is the interpretation of the regular dropout as a Bayesian approximation of the Gaussian process. The regular dropout is applied at both training and testing steps so that the output of the model is no longer deterministic. The main purpose of MC-dropout is to generate the multiple prediction outputs and consider them as random variables of a probabilistic distribution which is called Bayesian interpretation.

By using MC-dropout, the statistical properties of the outputs, such as upper and lower limits of the predictions can be computed. In statistics, the range between actual upper and lower limits of the expected estimate is called prediction interval (PI) and it is associated with a probability with which the true value will be within that interval [32]. For example, the considered PIs vs percentages of true data within the given PI for different dropout values with 1-hr FH is shown in Fig. 5. The benefit of considering upper limits of predictions with high probability PI in the radar protection system is that capturing the wide range of uncertainty in interference predictions guarantees comprehensive protection for a radar.

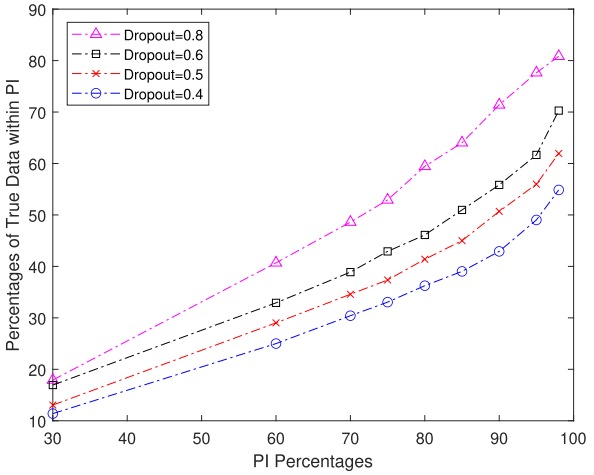


FIGURE 5. True data within forecasted prediction interval vs different dropout values for 1-hr FH.

V. EFFICIENT SHARING AND RADAR PROTECTION ALGORITHM

Previously, temporal DFS or cloud-based system with zone-based shared access dividing three geographical zones is used for radar protection. In zone-based shared access, the secondary operation on the radar channel is strictly forbidden in zone 1 and the radar spectrum is free to use in zone 3 while temporal sharing is allowed with a tolerable interference threshold in zone 2 whenever the radar's main beam is pointing in another direction. The drawback of DFS or temporal DFS with zone-based shared access is that sensing the radar signal at the user side is not optimal for the throughput of secondary users. Moreover, secondary users need to track the radar rotation time while most of the weather radar rotations are quasi-periodic so that comprehensive radar protection is not guaranteed. Our novel efficient sharing and radar protection system aims to achieve optimal temporal sharing while ensuring that radar is almost completely protected and tracking the radar rotation is not required.

The main objective of the proposed system is to maximize the averaged throughput over all connected users over all time periods where the throughput of each user j connected to an AP at time t is defined as:

$$\begin{aligned} Throughput_j &= B_{AP} \cdot \log_2(1 + SINR) \cdot \phi_j, \\ SINR &= \frac{P_R}{P_n + \omega_j}, \\ P_R &= \frac{P_t \cdot G_t}{L_{user}}, \\ P_n &= \eta \cdot N_{0(linear)} \cdot B_{AP}, \end{aligned} \tag{9}$$

while minimizing the aggregated interference points over the tolerable threshold of radar, P_{ot}, which is denoted with the

indicator function at time t, $I_p(t)$, as:

$$P_{ot} = \sum_{t=0}^{T} I_p(t),$$
$$I_p(t) = \begin{cases} 1, & \text{if} \Omega_t^R \geq Threshold, \\ 0, & \text{if } \Omega_t^R < Threshold, \end{cases} \quad (10)$$

where ϕ_j is the TP percentage of the user j, P_R is the received signal power from an AP that user j is connected, ω_j is the interference at the user j caused by other APs, L_{user} is the path loss between user and the connected AP, and P_n is the noise power with -174 dBm reference noise, N_0. Moreover, T is the total number of time instances and Ω_t^R is the total interference at the radar at time t after the radar protection system is applied.

By considering the random nature of radio propagation, the radar protection of the proposed system can be expressed in terms of the probability of total interference which exceeds the tolerable radar interference level and the permissible probability of harmful interference at the radar, ϵ_p, as in [17] and [33]:

$$Pr[\Omega_t^R \geq Threshold] \leq \epsilon_p. \quad (11)$$

The value of ϵ_p varies depending on the operating frequency and the radar type [33]. Reference [17] considered $\epsilon_p = 0.05$ for a weather radar operating in 5.6 GHz.

For simulation, we assumed that the university is inside the zone 2 of a weather radar which is 4 km away from the center of the radar. Instead of sensing the radar or tracking its rotation, the proposed algorithm is designed for the secondary users to be able to use the radar channel even when the main beam of radar is illuminating on them. The aggregated total interference at the radar is calculated based on the real collected data from the university's network. The APs inside the university are operating with the main channel excluding a radar channel and a subordinate channel which is a radar channel. Whenever the radar channel is allowed to be used as a subordinate channel for an AP, the SINR channel bonding model introduced in [22] is used to bond the main and subordinate channel for better throughput for the connected users of an AP. The proposed algorithm makes sure to protect the radar system by denying the access of necessary APs for the subordinate channel usage with the help of cloud-based REM. It is divided into two parts such as AP part (Algorithm part 1) and the Cloud-based REM part (Algorithm part 2).

A. ALGORITHM PART 1

In Algorithm 1 - AP part, all APs are required to register with cloud-based REM to be able to use the radar channel as a subordinate channel. If an AP is in Zone 1 and Zone 3, the rules are the same as before. If an AP is in Zone 2, the radar channel will be assigned as a subordinate channel. The transmission on the radar channel will be stopped for a certain period (10 minutes in our case) only when the notification from REM is received and then, the APs will connect to the radar channel again. On top of the 10-min break period, there is also an option called the silence period. The optional silence period is introduced to use during busy hours (mostly from 10 am to 4 pm during weekdays) of the highly utilized APs from the university's network. As we analyzed in [9], there is a peak utilization period in most of the highly utilized APs, and TP levels will be high all the time during these periods. Therefore, instead of connecting the radar channel again after a 10-min break, AP cannot use the radar channel again once its access is denied as long as the silence period for an AP is on. When the silence period is over for an AP, the radar channel can be assigned and used until receiving further notification from REM again.

Algorithm 1: Part 1 - AP Part

```
Each AP i do
Select: A main channel p ∈ M_p, where M_p is the set of
        available channels excluding radar channels.
Assign a radar channel as subordinate channel for higher
 data rate,
Initialize: Register with cloud-based REM.
Get: Rules for sharing with radar system, zone,
     distances and silence period for an AP i
     information
if zone == 1 or silence period for an AP i is on then
    No Access: for a Radar Subordinate channel, only
               the main channel is assigned.
else if zone == 2 and silence period for an AP i is off
 then
    Select: Utilize a Radar channel as Subordinate
            channel by defined rules.
    for t = start to requested time interval do
        if notification to move channel from REM is
         received then
            Stop: Accessing radar channel for a certain
                  silence period
            Perform: Transmission by using only
                     Primary channel during silence
                     period
        else
            Continue utilizing.
else
    Radar channels are free to use.
    Select: A Radar channel as Subordinate channel.
Perform: Non-contiguous channel bonding with the
         main and subordinate channels.
```

B. ALGORITHM PART 2

The Cloud-based REM collects the necessary information of each APs, calculates the interference data or collects the measured interference data from the ESC sensors at the radar, and decides which APs to remove not to over the tolerable interference threshold of the radar. The Cloud-based REM also computes the average and upper limits of predicted

Algorithm 2: Part 2 - Cloud-Based REM Part

A radar channel is assigned as a Subordinate channel for higher data rate.
Get: TP levels of APs
Set: silence indicator = 0
for *Each time t* **do**
  if *silence indicator > 0* **then**
    Set: silence indicator = silence period - 1
    if *total interference at time t-1 ≥ threshold* **then**
      Set: Reduced Interference = 0
      while *Reduced Interference ≤ Amount of previous Interference over threshold* **do**
        Denied: Access of an AP with highest TP level among updated connected APs list
        Calculate and Update: Reduced Interference and Connected APs list
      Send: Notifications to change channel only at t to APs whose accesses are denied
    else
      Keep: The same connected APs list (do not allow already removed APs to access during silence peroid).
  Silence Period Off: if *silence indicator ≤ 0* **then**
    if *Predicted total interference at time t+1 ≥ threshold* **then**
      Set: Reduced Interference = 0 and silence indicator = silence period
      while *Reduced Interference ≤ Amount of predicted Interference over threshold at t+1* **do**
        Denied: Access of an AP with highest TP level among total connected APs
        Calculate and Update: Reduced Interference and Connected APs list
      Send: Notifications to change channel only at t+1 to APs whose accesses are denied
    else
      Initialize: All APs to use radar channel as usual

total interference at the radar by using collected historical data. The predicted total interference of the next period is compared with the threshold and APs with the highest TP level are removed until the total interference is below the threshold. If an AP is decided to be removed for the next period (10-min), REM sends the notification to the specific AP.

Using silence period is optional for the efficient radar protection system with predicted total interference at the radar. When it is applied, the silence period will be on for certain hours right after the first time removing some APs. Once the silence period is on, the radar channel is not assigned again to the already removed APs in the next period, and the interference at the radar at time $t-1$ (after removing the previous APs) is used to compare with the threshold and decided the numbers of new APs to remove for the current period t. All the APs which are removed during the silence period cannot use the radar channel until the silence period is off again. In Algorithm 2 - Cloud-based REM part, all the steps will be used when the silence period is applied, and only the part after "Silence Period Off" will be used when the silence period is not applied.

VI. SIMULATION SYSTEMS AND COMPARISONS

A. DFS AND TEMPORAL DFS RADAR PROTECTION SYSTEM

In the DFS radar protection system, radar protection is done by detecting a radar at the secondary user side. The DFS requirements standardized by International Telecommunication Union (ITU) are −64 dBm threshold when radiated power higher than 200 mW, 60-sec channel availability check (CAC) time, and 30 min non-occupancy period after detecting a radar signal [4]. For a considered weather radar, the rotation time of the main beam to illustrate on the same area is 60 sec (rotating with 6° per sec) so that radar signal will be always detected at the user side within 60 sec CAC period [34]. It means the DFS system does not allow transmission within zone 2 where the received radar signal is stronger than the standardized threshold. If the DFS system is applied, none of the APs from the university which is located within zone 2 will be able to use the radar channel as the subordinate channel.

Temporal DFS (DFS-T) which is an extended version of DFS utilizing the temporal opportunity for secondary users is also widely used previously. In DFS-T, APs are assumed to know the exact antenna pattern and periodic rotation of the radar and utilize them to calculate the adjusted threshold. In reality, weather radars are quasi-periodic [22] and it is difficult for APs to know the exact antenna pattern and rotation of the radar [34]. The cooperative method with a combination of DFS-T and centralized dynamic threshold proposed in [5] which allows secondary user transmission in zone 2 is only for the secondary users with constant transmission and lower aggregated interference than tolerable interference threshold of a radar which is not suitable for our considered secondary users with stochastic transmission power and higher aggregated interference level. To overcome the drawbacks of DFS and DFS-T systems, one possible way is utilizing the real-time feedback data from the radar to ensure its protection.

B. REAL-TIME RADAR PROTECTION SYSTEM

In a real-time radar protection system, we have assumed that the measured interference at the radar with the help of

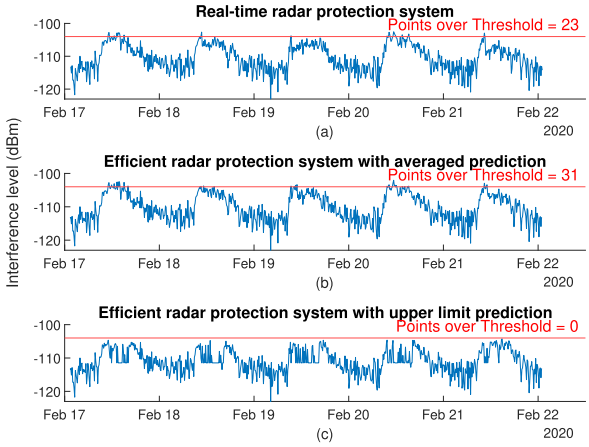


FIGURE 6. The total interference at the radar vs calculated threshold for different radar protection systems.

extended ESC sensor at $t-1$ is fed back to cloud-based REM at every t and it is used to compute the decision for removal of APs at $t+1$. This system provides the near-optimal secondary usage of the radar channel with simple feedback and computing mechanism. However, the drawback of a real-time radar protection system is that there are at least two time-step delays to remove the necessary APs for radar protection although the interference at the radar is already over the threshold. Moreover, it is impossible to keep the current interference level below the threshold using previous values even when the silence period is on due to the stochastic nature of the TP time series of APs. The example of interference at the radar time series vs calculated threshold for real-time radar protection system without predicting interference time series can be seen in Fig. 6 (a).

C. PROPOSED RADAR PROTECTION SYSTEM

Instead of waiting for the real-time feedback data, we used time series of predicted interference at the radar. First, the interference historical data are calculated or collected and the prediction of interference at the radar is computed at the cloud-based REM. The benefit of using predicted interference is that the real-time feedback from the radar is not required anymore at which there can be a delay (which reflects reality) in removing the necessary APs for radar protection. However, the averaged prediction values are not precise enough to protect the radar completely. Especially, the total interference at the radar is over the threshold when the predicted interference is less than the real interference value at time t. Therefore, we also used time series of upper limits prediction of interference for an efficient radar protection system.

The main advantage of using upper limits prediction is ensuring with a high probability that the actual interference will not be over the upper limits of the predicted time series. It provides almost perfect radar protection with the trade-off between lower interference at the radar and higher throughput of the users. Moreover, the silence period is not required

TABLE 3. Comparison for interference forecasting with LSTM and different dropouts for 1-hr forecast horizon.

Dropout	RMSE	NRMSE	MAE	R2 score
0.8	0.5396	0.0375	0.4291	0.9869
0.6	0.4291	0.0294	0.3381	0.9911
0.5	0.38752	0.0257	0.2880	0.9932
0.4	0.3833	0.0262	0.2901	0.9929
Naïve	1.6905	0.1159	1.1326	0.8629

in the efficient radar protection system with Upper limits prediction since the upper limits already provides the guard interval by considering the stochastic nature of interference time series. The examples of interference at the radar time series vs calculated threshold for proposed radar protection system with average and upper limits of predictions with 90% PI are shown in Fig. 6 (b) and (c), respectively.

D. PERFORMANCE COMPARISONS

In this section, performance comparisons of different radar protection systems are presented. Before going to the numerical results of the different radar protection systems, performances of the forecasting method used in the proposed radar protection system are also presented. To be able to utilize the uncertainty range of machine learning methods, we used the LSTM forecasting method with MC dropout to predict the averaged interference time series for a certain number of realizations to capture the stochastic nature of the interference time series.

The best LSTM averaged prediction result is with dropout 0.5 in Table 3 so that using the average and upper limits of predicted interference time series with dropout 0.5 gave the best efficient sharing and radar protection performances, which will be explained in detail later. The performances of predicting the upper limits of interference time series with different PIs are also shown in Fig. 7. Although the upper limits prediction with 99.9% PI captured the highest uncertainty range, using the upper limits predicted time series with 80% PI gives higher throughput per connected user with smaller ϵ_p value than using the average of predicted time series which is also explained in a later paragraph.

The performances of different radar protection systems such as DFS, real-time system and proposed systems with predicted interference are compared based on two metrics: (a) points over the threshold (P_{ot}) for a certain period and (b) averaged throughput of each user j connected to the APs in the university ($Throughout_j$). The ranges of the permissible probability of harmful interference at the radar which is defined as $\epsilon_p = \frac{P_{ot}}{T}$, to represent the radar protection performances for different radar protection systems are also investigated. The comparison of total interference time series and points over threshold for one example realization when different radar protection systems are applied is shown in Fig.6. For the DFS system, points over the threshold will be always zero since none of the APs can use the radar channel. In fact, the number of points over the threshold for

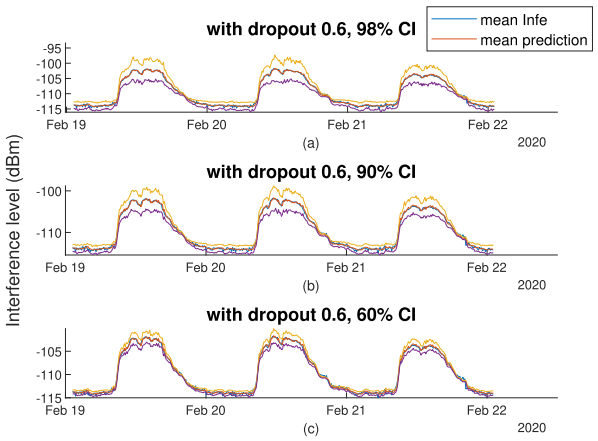


FIGURE 7. Forecasting total interference at the radar using LSTM with 1-hr FH.

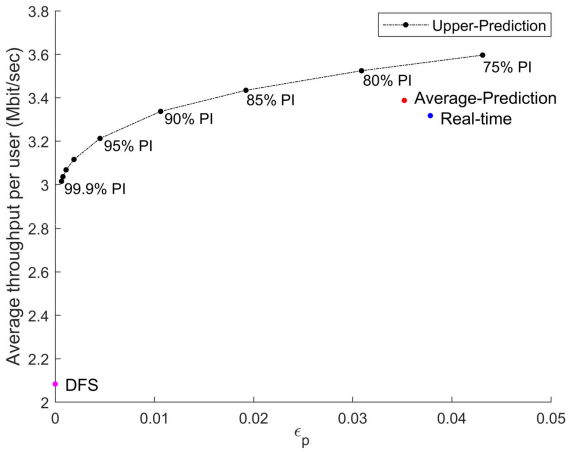


FIGURE 8. Averaged throughput per user connected to each AP for different radar protection systems vs ϵ_p.

different systems presented should also be averaged for a certain number of realizations by considering the stochastic nature of interference time series. The averaged points over the threshold for the real-time system proposed protection with averaged prediction system, and DFS system are 27, 25, and 0, respectively. For proposed protection with the upper limits prediction system, the averaged points over the threshold can vary from 0.45 with 99.9% PI to 22 with 80% PI.

From the results, the DFS system has the best radar protection and our proposed efficient radar protection system with upper limits prediction has higher radar protection performance than the rest. However, comparing the throughput of the users connected to each APs of the university is necessary to optimize the transmission of connected users. The averaged throughputs per user connected to each AP in the university for different radar protection systems are presented in Fig. 8. Due to a trade-off between radar protection and efficient sharing in the weather radar band, the averaged throughput with the DFS system is significantly lower than any other system. The proposed system with averaged prediction has slightly higher averaged throughput per user with better radar protection (lower ϵ_p values) than in the real-time system. The radar protection performance of our proposed system is improved by utilizing the upper limits of different PIs so that lower ϵ_p value is always achieved for the same averaged throughput per user than in the system with averaged prediction and the real-time system. Our proposed scheme with upper limits prediction can be used between $\epsilon_p = 0.0006$ with 99.9% PI and $\epsilon_p = 0.043$ with 75% PI which does not exceed the recommended value, $\epsilon_p = 0.05$, for a weather radar operating in 5.6 GHz [33].

The main advantage of the proposed system with upper limits prediction is that it achieves higher averaged throughput per user with lower ϵ_p value for 85% and 80% PIs compared to the real-time and averaged prediction systems. The radar protection performance of the proposed system with an upper limits prediction for 99.9% PI is also close to the protection performance of the DFS system but with significantly higher averaged throughput per user as shown in Fig. 8. Hence, the proposed efficient radar protection system with upper limits prediction, which has significantly higher averaged throughput per user, ensures the radar protection by even allowing some of the APs to transmit when radar main beam is illustrated on them unlike in the DFS system, which ensures the radar protection by not allowing any APs to transmit.

VII. CONCLUSION AND FUTURE WORK

Spectrum sharing between radars in the 5.6 GHz band and wireless enterprise networks can help in providing higher capacity. However, designing such a sharing scheme is challenging and to address this, we have proposed a machine learning-driven technique which can facilitate efficient sharing. Our proposed technique enables a radar protection system via neural network-based interference prediction which in turn helps in optimizing spectrum sharing. While the proposed technique can be used for sharing with any rotating radar system in various bands, however, our focus in this paper is on radar protection for a weather radar that rotates quasi-periodically in a 5.6GHz band. To model the interference generated to a radar system from an enterprise wireless network, in our work, we studied the stochastic relationship between the number of connected users and physical layer transmit power (TP) data of 7 different APs to model the TP time series for 50 APs operating with 5.6 GHz in the real enterprise network. In simulations, these generated TP time series from the multinomial-based model are used to calculate the aggregated interference at the radar by using appropriate path loss models.

The calculated aggregated interference time series at the radar (which can also be measured by a sensor) are utilized in training the LSTM-based machine learning model which then makes interference-related predictions. To ensure robust radar protection, we also consider the prediction intervals for the predicted interference values by using the MC dropout method. The proposed efficient sharing and radar

protection system consists of two parts of algorithms. In part 1, AP part, APs are listening to the cloud-based REM whether to access the radar channel or not. Once the radar channel is allowed access, the non-contiguous channel bonding is performed by the APs. In part 2, the Cloud-based REM part, the predicted interference at the radar is compared with a tolerable threshold and some APs are removed with certain rules whenever the predicted interference is about to exceed the threshold.

We also compared different radar protection systems in terms of how often the interference is exceeded over the threshold when a particular system is used. Moreover, achieved averaged throughput per user connected to the APs is also utilized to compare with other systems. According to the facts, the secondary users located inside zone 2 of the considered radar will not be able to use the radar channel as a subordinate channel when the DFS system is applied. The real-time radar protection system and the proposed system with averaged predicted interference have higher throughput per user than the DFS system but cannot provide the comprehensive radar protection. To address these limitations, the proposed system is made robust by incorporating a PI-based technique in which an upper limits of predicted interference time series ensures that similar radar protection performance with significantly better throughput per user than conventional DFS system.

Dynamic threshold calculation aims to achieve higher throughput than static thresholds. However, the limitation in previous works considering dynamic threshold calculation (e.g. [5] and [17]) is that they cannot guarantee comprehensive radar protection due to the inefficient radar sensing time and the quasi-periodic weather radar rotations. To address this limitation as a future direction of our work, dynamic tolerable thresholds of the radar can be calculated with the help of neural networks-based radar rotation prediction. With its powerful nonlinear mapping ability, neural networks-based time series predictions can help forecast the quasi-periodic radar rotations which can be used in calculating the dynamic tolerable threshold of the radar to guarantee comprehensive radar protection. Unlike in this work, a sufficient historical radar signal time series obtained using the approach for example in [6], will be required for the radar rotations prediction methods. Dynamic tolerable thresholds calculation with neural networks-based radar rotation prediction can provide the throughput improvement as compared to the current efficient sharing and radar protection system which only considers the threshold of worst-case scenario that the radar main beam is illuminating on the university.

REFERENCES

[1] *Report on Collective Use of Spectrum (CUS) and Other Spectrum Sharing Approaches*, RSP Group, RSPG11-392, Radio Spectr. Policy-Unit B4, Electron. Commun. Netw. Services Directorate, Directorate-Gen. Commun. Netw., Content Technol., Eur. Commission, BU 33 07/65, B-1049, Brussels, Belgium, Nov. 2011.

[2] M. Cotton, M. Maior, F. Sanders, E. Nelson, and D. Sicker, "Developing forward thinking rules and processes to fully exploit spectrum resources: An evaluation of radar spectrum use and management," in *Proc. 12th Annu. Int. Symp. Adv. Radio Technology. (ISART)*, pp. 1–121, 2012.

[3] F. Paisana, N. Marchetti, and L. A. DaSilva, "Radar, TV and cellular bands: Which spectrum access techniques for which bands?" *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1193–1220, 3rd Quart., 2014.

[4] *Dynamic Frequency Selection (DFS) in Wireless Access Systems Including Radio Local Area Networks for the Purpose of Protecting the Radiodetermination Service in the 5 GHz Band*, Standard R. I.-R. M.1652-1, May 2011.

[5] C. de Souza Lima, F. Paisana, J. F. de Rezende, and L. A. DaSilva, "A cooperative approach for dynamic spectrum access in radar bands," in *Proc. Int. Telecommun. Symp. (ITS)*, Aug. 2014, pp. 1–5.

[6] Z. Khan, J. J. Lehtomaki, R. Vuohtoniemi, E. Hossain, and L. A. DaSilva, "On opportunistic spectrum access in radar bands: Lessons learned from measurement of weather radar signals," *IEEE Wireless Commun.*, vol. 23, no. 3, pp. 40–48, Jun. 2016.

[7] Z. Khan, J. J. Lehtomaki, R. Aguilar-Gonzalez, R. Vuohtoniemi, E. Hossain, L. A. DaSilva, and A. Marshall, "Database-assisted distributed and cloud-based access methods for unlicensed and radar bands," *IEEE Trans. Cognit. Commun. Netw.*, vol. 3, no. 3, pp. 404–419, Sep. 2017.

[8] J. Caulfield, "Proposal to administer a environmental sensing capability," Key Bridge Wireless LLC, FCC, Washington, DC, USA, Tech. Rep., 2016. [Online]. Available: https://ecfsapi.fcc.gov/file/60001841831.pdf

[9] S. P. Sone, J. J. Lehtomaki, and Z. Khan, "Wireless traffic usage forecasting using real enterprise network data: Analysis and methods," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 777–797, 2020.

[10] S. P. Sone, J. Lehtomaki, Z. Khan, and K. Umebayashi, "Forecasting wireless network traffic and channel utilization using real network/physical layer data," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 31–36.

[11] L. Deek, E. Garcia-Villegas, E. Belding, S.-J. Lee, and K. Almeroth, "Intelligent channel bonding in 802.11n WLANs," *IEEE Trans. Mobile Comput.*, vol. 13, no. 6, pp. 1242–1255, Jun. 2013.

[12] J. Gao, X. Li, W. Wang, and Y. Bai, "Non-contiguous channel bonding for TV white space usage with NC-OFDM transmission," *Wireless Pers. Commun.*, vol. 86, no. 2, pp. 385–401, Jan. 2016.

[13] A. Ghasempour, "Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1, p. 22, Mar. 2019.

[14] Z. Khan, J. J. Lehtomaki, S. I. Iellamo, R. Vuohtoniemi, E. Hossain, and Z. Han, "IoT connectivity in radar bands: A shared access model based on spectrum measurements," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 88–96, Feb. 2017.

[15] F. Paisana, Z. Khan, J. Lehtomaki, L. A. DaSilva, and R. Vuohtoniemi, "Exploring radio environment map architectures for spectrum sharing in the radar bands," in *Proc. 23rd Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–6.

[16] Z. Khan, J. J. Lehtomaki, E. Hossain, M. Latva-Aho, and A. Marshall, "An FPGA-based implementation of a multifunction environment sensing device for shared access with rotating radars," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 11, pp. 2561–2578, Nov. 2018.

[17] M. Tercero, K. W. Sung, and J. Zander, "Impact of aggregate interference on meteorological radar from secondary users," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2011, pp. 2167–2172.

[18] J. M. Peha, "Cellular systems and rotating radar using the same spectrum," in *Proc. Int. Symp. Adv. Radio Technol.*, Mar. 2012.

[19] Y. Gal and Z. Ghahramani, "Dropout as a Bayesian approximation: Representing model uncertainty in deep learning," in *Proc. Int. Conf. Mach. Learn. (ICML)*, 2016, pp. 1050–1059.

[20] I. Alarab, S. Prakoonwit, and M. I. Nacer, "Illustrative discussion of MC-dropout in general dataset: Uncertainty estimation in bitcoin," *Neural Process. Lett.*, vol. 53, no. 2, pp. 1001–1011, Apr. 2021.

[21] C. J. Holder and M. Shafique, "Efficient uncertainty estimation in semantic segmentation via distillation," in *Proc. IEEE/CVF Int. Conf. Comput. Vis. Workshops (ICCVW)*, Oct. 2021, pp. 520–535.

[22] Z. Khan, J. Lehtomaki, S. Scott, Z. Han, M. Krunz, and A. Marshall, "Distributed and coordinated spectrum access methods for heterogeneous channel bonding," *IEEE Trans. Cognit. Commun. Netw.*, vol. 3, no. 3, pp. 267–281, Sep. 2017.

[23] J. C. Lagarias, J. A. Reeds, M. H. Wright, and P. E. Wright, "Convergence properties of the Nelder-Mead simplex method in low dimensions," *SIAM J. Optim.*, vol. 9, no. 1, pp. 112–147, 1998.

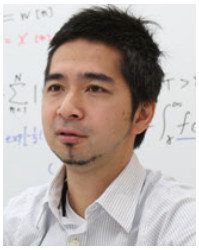
[24] *Procedures for Determining the Potential for Interference Between Radars Operating in the Radiodetermination Service and Systems in Other Services*, document ITU-R M.1461-2, Geneva, Switzerland, 2018.

[25] *Compilation of Measurement Data Relating to Building Entry Loss*, document ITU-R 2346-2, Geneva, Switzerland, 2017.
[26] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Dec. 1997.
[27] Z. Karevan and J. A. K. Suykens, "Transductive LSTM for time-series prediction: An application to weather forecasting," *Neural Netw.*, vol. 125, pp. 1–9, May 2020.
[28] C. Zhang and P. Patras, "Long-term mobile traffic forecasting using deep spatio-temporal neural networks," in *Proc. 18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (Mobihoc)*, Jun. 2018, pp. 231–240.
[29] J. Brownlee, *Deep Learning for Time Series Forecasting: Predict the Future With MLPs, CNNs and LSTMs in Python*. Melbourne, VIC, Australia: Mach. Learn. Mastery, 2018.
[30] R. J. Hyndman and G. Athanasopoulos, *Forecasting: Principles and Practice of Business & Economics*, vol. 2. London, U.K.: OTexts, May 2018.
[31] R. Pascanu, C. Gulcehre, K. Cho, and Y. Bengio, "How to construct deep recurrent neural networks," in *Proc. Int. Conf. Learn. Representations (ICLR)*, Apr. 2014.
[32] V. K. Rohatgi and A. M. E. Saleh, *An Introduction to Probability and Statistics*. Hoboken, NJ, USA: Wiley, 2015.
[33] E. Obregon, K. W. Sung, and J. Zander, "Is spectrum sharing in the radar bands commercially attractive?—A regulatory and business overview," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 3, pp. 428–438, Mar. 2016.
[34] M. Tercero, K. W. Sung, and J. Zander, "Temporal secondary access opportunities for WLAN in radar bands," in *Proc. 14th Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Oct. 2011, pp. 1–5.

SU P. SONE received the B.E. and M.E. degrees in telecommunications engineering from the Asian Institute of Technology, Bangkok, Thailand, in 2016 and 2018, respectively. She is currently pursuing the Ph.D. degree with the University of Oulu, Finland. She was a Research Assistant at the BU-CROCCS Laboratory, Bangkok University, Thailand, from 2015 to 2016. She is a Full-Time Researcher with the Centre for Wireless Communications, University of Oulu. She was a recipient of the Hiromichi Seya Prize and the Wireless Personal Multimedia Communications Prize, in 2018. Her research interest includes traffic modeling in physical layer of wireless communications.

JANNE LEHTOMÄKI (Member, IEEE) received the Ph.D. degree from the University of Oulu, Finland, in 2005. Currently, he is an Adjunct Professor with the Centre for Wireless Communications, University of Oulu. He was a Visiting Scholar at the Georgia Tech, Atlanta, USA, in fall 2013. Currently, he is focusing on spectrum measurements and terahertz band wireless communications. He was a Guest Associate Editor of the *IEICE Transactions on Communications Special Section*, in February 2014 and July 2017, and a Managing Guest Editor of *Nano Communication Networks Special Issue*, in June 2016. He was the General Co-Chair of IEEE Wireless Communications and Networking Conference (WCNC), in 2017 and International Workshop on Smart Spectrum, a TPC Co-Chair of IEEE Wireless Communications and Networking Conference (WCNC), in 2015 and 2016 and International Workshop on Smart Spectrum, and a Publicity/Publications Co-Chair of ACM NANOCOM, in 2015, 2016, and 2017. He has coauthored the paper receiving the Best Paper Award in IEEE Wireless Communications and Networking Conference (WCNC), in 2012. He is the Editorial Board Member of *Physical Communication*.

ZAHEER KHAN (Member, IEEE) received the M.Sc. degree in electrical engineering from University College Borås, Sweden, and the Dr.Sc. degree in electrical engineering from the University of Oulu, Finland, in 2007 and 2011, respectively. He was a Tenure Track Lecturer at the University of Liverpool, U. K., from 2016 to 2017. He was a Research Fellow/Principal Investigator at the University of Oulu, from 2011 to 2016, where he is currently an Adjunct Professor. His research interests include implementation of advanced signal processing and wireless communications algorithms on Xilinx FPGAs and Zynq System-on-Chip (SoC) boards, application of game theory to model distributed wireless networks, prototyping access protocols for wireless networks, the IoT location tracking systems, cognitive and cooperative communications, and wireless signal design. He was a recipient of the Marie Curie Fellowship for 2007-2008.



KENTA UMEBAYASHI (Member, IEEE) received the L.L.B. degree from Ritsumeikan University, Japan, in 1996, and the B.E., M.E., and Ph.D. degrees from Yokohama National University, Japan, in 1999, 2001, and 2004, respectively. From 2004 to 2006, he was a Research Scientist at the Centre for Wireless Communications, University of Oulu, Finland. He is currently a Professor with the Tokyo University of Agriculture and Technology, Japan. He was a Principal Investigator of four grants-in-aid for scientific research projects and three strategic information and communications research and development promotion program projects, including a HORIZON2020 Project. His research interests include signal detection and estimation theories for wireless communications, signal processing for multiple antenna systems, cognitive radio networks, and terahertz band wireless communications. He received the Best Paper Award at 2012 IEEE Wireless Communications and Networking Conference (WCNC) and the Best Paper Award at 2015 IEEE Wireless Communications and Networking Conference (WCNC) Workshop from IWSS.

ZUNERA JAVED received the B.Eng. degree in telecommunication from the Mehran University of Engineering and Technology, Pakistan, in 2014, and the M.Sc. degree in computer science by research from Sunway University, Malaysia, in 2017 (under the dual degree program of Sunway University, Malaysia and Lancaster University, U.K.). She is currently pursuing the Dr.Sc. degree with the University of Oulu, Finland. She worked as a Research Assistant at the Wireless Communication Department, MIMOS Berhad. She is a Full-Time Researcher with the Centre for Wireless Communications, University of Oulu. Her research interests include game theory for wireless networks, applied reinforcement learning, and cognitive radio networks.