Newsletter

IEEE ComSoc Technical Committee
on Cognitive Networks (TCCN)

Editor: Prof. Dola Saha

University at Albany, SUNY, USA

December 2022

Contents

1 Chair's Message 2

2 Editor's Note 4

3 Visions of Prof. Kaushik Chowdhury 11

4 Insights of Prof. Rose Hu 21

5 Views of Prof. Walid Saad 40

6 Thoughts of Prof. Yalin Sagduyu 58

1. Chair's Message

Dear TCCN Fellow Members,

Time goes quickly and it has been six years since I served as the Vice-Chair and then Chair of TCCN. This will be my last message to you as the TC Chair.

On behalf all the TCCN officers, I would like to take this opportunity to thank all of you for your strong support of our work during the past two years. I am glad to write to you regarding some of our recent progress as well as future plans of the TCCN.

The scope of cognitive network is broad, and we have been encouraging colleagues to establish SIGs (Special Interest Groups) to promote specific research directions within the TC's scope. In this newsletter, I would like to share with you the recent progress on SIG for AI and Machine Learning in Security, which is a valuable venue for professionals interested in this area.

– **Chair**: Prof. K.P. (Suba) Subbalakshmi, Stevens Institute of Technology, USA

– **Vice-Chair**: Prof. Dola Saha, University at Albany, SUNY, USA

The group is responsible for organizing symposiums, workshops, virtual seminars, and special issues of magazines and journals in this area; influencing telecommunications standards in the area of cognitive networks; and providing opportunities for networking between its members. In the past two years, the SIG has become an active and important platform for TCCN members to exchange research ideas and brainstorm about the future research directions of the TC.

In addition, we will announce the call-for-nominations for the TCCN Publication and Recognition Awards for 2022 soon. These are annual awards. The call-for-nominations usually come out in the summer, and we will announce the awardees at IEEE GLOBECOM 2022.

The term of the current TCCN officers will come to an end by the end of 2022. We have formed a nomination committee and announce the call-for-nominations for the officer candidates. Following the tradition, the voting will be done electronically by all the voting members of the technical committee. The results will be announced at IEEE GLOBECOM 2022. I look forward to having more energetic and dedicated volunteers joining the leadership team.

As always, any suggestions from TCCN members are welcome regarding how to make TCCN a better community. Please feel free to contact me at *lingyang.song@pku.edu.cn* to share your thoughts.

Thanks and best regards,

Lingyang Song,
Fellow of IEEE
Chair, IEEE ComSoc TCCN
Peking University, China

Bio: Lingyang Song received his BS from Jilin University, China, in 2002, and PhD from the University of York, UK, in 2007, where he received the K. M. Stott Prize for excellent research. He worked as a research fellow at the University of Oslo, Norway until rejoining Philips Research UK in March 2008. In May 2009, he joined the School of Electronics Engineering and Computer Science, Peking University, and is now a Boya Distinguished Professor. He is the co-author of a number of best paper awards, including IEEE ComSoc Leonard G. Abraham Prize in 2016, IEEE Communications Society Heinrich Hertz Award in 2021, IEEE ICC 2014, IEEE ICC 2015, IEEE Globecom 2014. He has served as a Distinguished Lecturer of IEEE Communications Society, an Area Editor of IEEE Transactions on Vehicular Technology, an Editor of IEEE Transactions on Communications. He is a Fellow of IEEE, and a Clarivate Analytics Highly Cited Researcher in 2018.

2. Editor's Note

Cognition for Coexistense with Passive Users of Spectrum

Author: Prof. Dola Saha,
University at Albany, State University at New York
Albany, NY, USA,
Email: *dsaha@albany.edu*

The growing need for spectrum to support the next generation (xG) communication networks increasingly generate unwanted radio frequency interference (RFI) in protected bands for passive scientific usage, like radio astronomy and remote sensing [Org20; Nat15]. Radio Astronomy is a discovery-based science, which has revolutionized our understanding of the Universe through scientific observations across the electromagnetic (EM) spectrum. Radio Astronomy services (RAS) aims at collecting the faint emissions of distant astronomical sources at radio frequencies. The sensitivity required to observe astronomical emissions from Earth is achieved through very low noise amplifier technology, and data observations over wide bandwidth (100s of MHz) and long integration times (minutes to hours long). These received emissions are counted in units of Janskys (1 Jy = $10^{-26}\mathrm{Wm}^{-2}\mathrm{Hz}^{-1}$), and are many orders of magnitudes below the typical transmit power of most active services, which have the potential to compromise the conduct of an astronomical observation. Similarly, passive remote sensing detects natural energy radiated or reflected from the scene being observed. Radiometer is an instrument that measures the intensity of electromagnetic

radiation, converts that to microwave brightness temperature (BT), which is translated to measures of various geophysical parameters, like ice cover, soil moisture, sea surface salinity, etc., based on well-established radiative models. Radiometers require high sensitivity, in the order of 1K (Kelvin) or less. The weakest sources of interference can mask or mimic a signal of interest, and the strongest can saturate the receivers (amplifier or analog-to-digital converters) preventing any scientific observations.

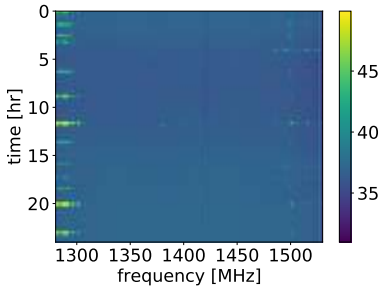
This necessitates stringent interference mitigation techniques to continue scientific research in presence of challenging RFI. Generally, researchers in communication area strive to reduce noise from artificially generated signal, whereas passive sensing community focuses on removing communication signals from the scientific signal. This seemingly opposing requirement is pushing the two communities farther away. Both communities use the electromagnetic spectrum, one for transmission to keep people connected in a virtual world, the other for understanding the Universe through the RF window. Both are equally essential and are designed to overcome a common bottleneck: *Interference*. Hence, it is crucial for future cognitive communication networks [Mit00] to address this issue and improve its cognition capabilities beyond detection and avoidance of primary users to morph the RF environment for coexistence with passive users. The rest of the article focuses on radio astronomy, although the discussions presented here can be generalized for any passive services.

2.1 Collaborative Interference Cancellation

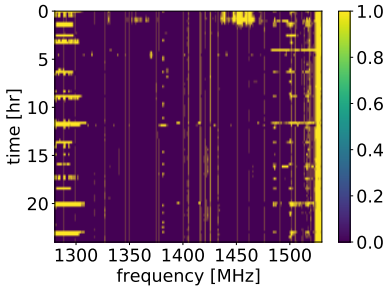
Radio telescopes are generally located in geographically isolated areas farther from communication networks and monitor astronomical signals in the protected bands, which should ideally have no RFI. However, Doppler shifts in the spectral lines observed by the telescopes are common due to movement of the observed cosmic objects relative to the Earth. This is the most interesting scenario that radio astronomers would like to study to understand the structure and changes to the Universe. However, this shift often reaches unprotected frequency bands, where RFI can be even more prominent. Current RFI mitigation techniques use statistical signal analysis to detect RFI and remove the associated time and frequency bins when detected, called excision. So, any astronomical signal of interest will be lost if it is persistently contaminated with RFI.

Figure 2.1 illustrates the excision problem with data collected with the Deep Synoptic Array DSA-110 [Hal+19] located at the Owens Valley Radio Observatory. It is one of the largest university-operated radio observatories in the world and hosts DSA-110 [Hal+19]. Deep Synoptic Array-110 (DSA-110) is a radio interferometer built for fast radio burst (FRB) detection and direct localization. It is under development to create an array of 110×4.65m dishes, which will continuously survey for FRBs. The data in Figure 2.1b spanning 1300-1500MHz is corrupted with the three types of RFI encountered in radio astronomy: continuous in time and narrow in frequency; intermittent in time and narrow in frequency; and impulsive in time and wide in frequency. Figure 2.1c shows the same data after identification and excision of the RFI-corrupted time-frequency bins. This flagging and excision approach is usually tuned to minimize the probability of non-detection of the RFI and leads to a significant data loss, sometimes as high as 40% at L-band (1-2 GHz), 30%

(a) Deep Synoptic Array-110 (DSA-110).



(b) RFI from GNSS



(c) Flags include H1 line

Figure 2.1: RFI flagging and excision with data from OVRO [Hal+19]

at S-band (2-4 GHz) and 20% at X-band (4-8 GHz) [RSE19], impacting the recovery of the astronomical signal of interest.

Therefore, full recovery of an astronomical signal corrupted by RFI cannot be achieved without prior knowledge of the source of interference. Fortunately, artificial signals can be characterized and made available to the telescope through collaboration. Then, the contribution of the RFI can be accurately cancelled from the telescope data to reveal the astronomical signal. In our recent work [Car+21], we proposed to decompose the RFI at the cellular BS into a compact yet accurate eigenspace that is periodically shared with the radio telescope over the Internet. At the telescope the composite signal is decomposed using the same method revealing its eigenspace that contain the RFI subspace, ideally orthogonal to the astronomical signal space. The shared RFI eigenspace is used to cancel the RFI from the composite eigenspace via complimentary orthogonal projections. Since the cancellation happens in the eigenspace, a final step to convert the eigenspace to the corresponding time-domain signal will reveal the RFI-free astronomical signal. Figure 2.2 shows

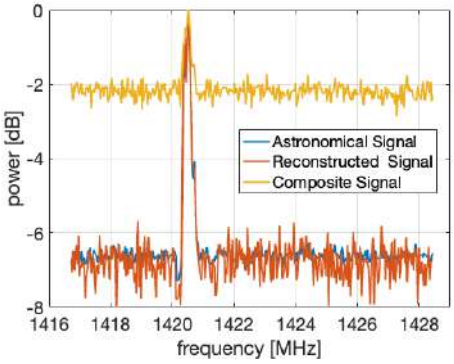


Figure 2.2: Reconstructed space signal compared to the true astronomical and the composite signal.

true astronomical signal (blue) captured using DSA-110, an RFI contaminated astronomical signal (yellow), which is used in our methodology to remove RFI and reconstruct the rectified astronomical signal (orange). The power levels are relative with measured noise floor at the telescope (-174 dBm) as the baseline. We achieved a Reconstruction Quality Factor (RQF) of 24.6944 dB for this reconstructed signal, which is much higher than the theoretical lower bound of RQF=10.0007 dB. Much work remains to be done in this domain and are not limited to issues like minimizing the overhead of communication and removing RFI from multiple base stations as well as multiple small cells.

2.2 Interference Cancellation through Intelligent Reflections

RAS has been allocated [Bur13] only 1.3% frequency of fully protected bands in which all emissions are prohibited that are sparsely distributed under 30 GHz, as well as 1.2% and 0.5% of shared bands as a primary and secondary user, respectively. Most astronomical emissions are however wideband by nature (e.g. thermal or synchrotron emissions), and observatories often have to operate opportunistically outside the allocated bands to reach the required sensitivity of their observations. Continuous transmitters can be avoided, either spatially by locating the radio observatories in remote areas with low population densities [Ser21], through filtering in the frequency domain [CLJ10], or even through active collaboration with the transmitting service [Car+21]. Mobile transmitters, however, cannot be spatially avoided and active collaboration through wireless media induces more RFI in Radio Astronomy Services (RAS). These mobile transmitters may include aircraft, satellite, handheld devices, automotive radars and UAVs that can cause significant interference to radio astronomy observations. But, they are transient and offer frequent down times in their occurrence of transmission that can often be exploited for astronomical observations. Figure 2.3 shows one such example of aeronautical activity in 1090 MHz from January to April 2022 around the Owens Valley Radio Observatory (OVRO) in California. The next generation of radio telescope, DSA-2000 will be even larger with 2000 dishes. Both DSA-110 and DSA-2000 suffer significantly from airborne RFI. Hence, it is essential to innovate techniques that can intelligently detect and track RFI in real time and accurately cancel it at the radio telescope to preserve scientific observations in those electromagnetic bands.

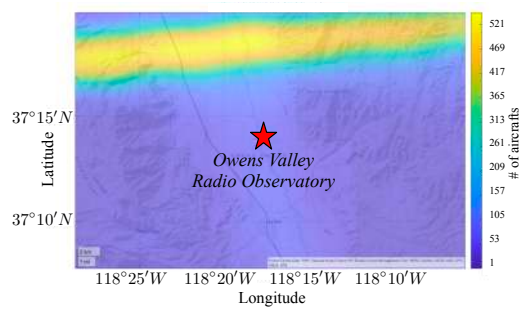


Figure 2.3: Air traffic density around OVRO (red star). The aeronautical signals are observed as RFI at the Telescope.

In our recent work [Zou+22], we introduced `SCISRS`: Signal Cancellation using Intelligent Surfaces for Radio Astronomy Services, which cancels incident RFI at the telescope receiver through creation of a destructive wavefront using a Reconfigurable Intelligent Surface (RIS). The proposed system is the first of its kind where RIS is used to cancel the energy of an RFI wavefront for a radio telescope. It allows the removal of the RFI before it reaches the ADCs of the telescope, thus facilitating scientific broadband observations across the electromagnetic spectrum.

Given a direction of arrival (DoA) of an RFI, SCISRS changes the phases of the RIS elements to steer the incident RFI towards telescope in order to cancel the incident interference at the telescope, thus dynamically creating a *EM quiet zone* around the receiver of the radio telescope. To realize this idea, we focus on the aeronautical signals from aircraft (960-1215 MHz) in L-band due to growing interest in observing the lower frequencies by the radio astronomy community. Figure 2.4 shows the system architecture with three entities: the telescope receiver, the RFI DoA Estimator and the RIS, which are together used to cancel the RFI transmitted by an airborne transmitter. The direct path of RFI (aeronautical signals) is incident on the telescope receiver, which undergoes flat fading channel, propagation loss and antenna sidelobe gain. Similarly, another direct path of the transmitter signal reaches the RIS unit. The reflected signal at the telescope is the collective sum of all signals reflected by multiple RIS cells, which has undergone a cascaded channel of Transmitter-RIS and RIS-Telescope. The RFI is cancelled at the radio telescope when both *the magnitude and phase response* of the RIS array exactly equals the channel and antenna gains of the direct path. Essentially, SCISRS makes passive radio telescope a cognitive system that can reflect incident RFI, dynamically creating an EM quiet zone to coexist with other important active wireless communications around it.

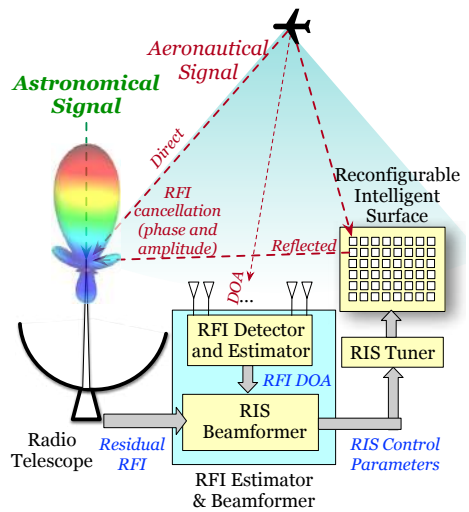


Figure 2.4: SCISRS: Cancelling RFI from airborne transmitters at the radio telescope by reconfigurable intelligent surfaces.

2.3 Future Directions for Cognitive Communication Networks

Wireless technology has changed our lives and has enormous potential to change the way we live over the next several decades. Wireless signals have helped connect people across the globe, communicate beyond the Earth, sense signals originating from outer space or the Earth for understanding the Universe or our world through the window of radio frequency (RF). However, the exponential growth of active wireless services has brought forth new challenges due to increased requirement for spectrum usage. But, the electromagnetic (EM) spectrum is a constant and limited resource and needs to be appropriately shared among all wireless systems and applications, including both active and passive uses. Hence, it is essential to induce "cognition" in both active and passive users for seamless coexistence of multiple services that improve effective spectrum utilization. This newsletter includes four articles by eminent researchers in the area of cognitive wireless communication. Their vision will pave the path for future research in next generation cognitive wireless systems.

References

[Org20] International Astronomical Organisation. *Dark and Quiet Skies for Science and Society*. 2020. URL: *https://www.iau.org/static/publications/dqskies-book-29-12-20.pdf*.

[Nat15] National Academies of Sciences, Engineering, and Medicine. *A Strategy for Active Remote Sensing Amid Increased Demand for Radio Spectrum*. Washington, DC: The National Academies Press, 2015. ISBN: 978-0-309-37305-0. DOI: *10.17226/21729*. URL: *https://www.nap.edu/catalog/21729/a-strategy-for-active-remote-sensing-amid-increased-demand-for-radio-spectrum*.

[Mit00] Joseph Mitola. "Cognitive Radio An Integrated Agent Architecture for Software Defined Radio". In: 2000.

[Hal+19] Gregg Hallinan et al. "The DSA-2000–A Radio Survey Camera". In: *arXiv preprint arXiv:1907.07648* (2019).

[RSE19] Urvashi Rau, Rob Selina, and Alan Erickson. *RFI Mitigation for the ngVLA: A Cost-Benefit Analysis ngVLA Memo# 70*. 2019.

[Car+21] Maqsood Careem et al. "Spectrum Sharing via Collaborative RFI Cancellation for Radio Astronomy". In: *2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 2021.

[Bur13] ITU-R Radioecommunications Bureau. *ITU-R Handbook on Radio Astronomy*. Switzerland, Geneva: ITU-R Radioecommunications Bureau, 2013.

[Ser21] RA Series. *Characteristics of radio quiet zones*. Technical report. Technical report, International Telecommunication Union (ITU), Geneva ..., 2021.

[CLJ10] Alonso Corona-Chavez, Ignacio Llamas-Garro, and Michael J. Lancaster. "A high temperature superconducting quasi-elliptic notch filter for radioastronomy". In: *Microwave and Optical Technology Letters* 52.1 (2010), pages 88–90.

[Zou+22] Zhibin Zou et al. "SCISRS: Signal Cancellation using Intelligent Surfaces for Radio Astronomy Services". In: *2022 IEEE Global Communications Conference (GLOBECOM)*. 2022, pages 1–6.

The Author

Dola Saha is an Assistant Professor in the Department of Electrical & Computer Engineering at University at Albany, SUNY. She co-directs the Mobile Emerging Systems and Applications (MESA) Lab at UAlbany. She was a faculty fellow at Jet Propulsion Laboratory, Caltech, NASA in summer of 2022. She was a visiting faculty at the Air Force Research Laboratory in summers of 2020 and 2021. She is the Vice Chair of the IEEE ComSoc TCCN SIG for AI and Machine Learning in Security and has been appointed a member of the SUNY Innovations Policy Board. Prior to that, she was a Research Assistant Professor in the Department of Electrical & Computer Engineering at Rutgers University. Before that, she was a Researcher in the Mobile Communications and Networking group at NEC Laboratories America. She received her Masters and Doctorate degrees from the Department of Computer Science in the University of Colorado Boulder. She is the recipient of Google Anita Borg Scholarship for her academic credentials. Her research interests lie in the crossroads of Machine Learning for Wireless Communication, Wireless Security, Digital Communication, Wireless Networks, Wireless Signal Processing, and Architecture of Software Defined Radios with focus on systems design and practical evaluation.

3. Visions of Prof. Kaushik Chowdhury

"Cognition" for Next Generation Wireless Technologies

Author: Prof. Kaushik Chowdhury,
Institute for the Internet of Things, Northeastern University
Boston, MA, USA,
Website: *https://genesys-lab.org*
Email: *krc@ece.neu.edu*

3.1 Introduction

Wireless engineers have attempted to empower radios with cognition and ability to make independent decisions that optimize a defined network utility over the past two decades. The goal of early efforts towards designing so called "cognitive radios" is captured in the definition proposed by the US Federal Communications Commission [FCC03]:

> A "Cognitive Radio" is a radio that can change its transmitter parameters based on interaction with the environment in which it operates.

While the definition is broad, most research efforts have focused on spectrum sharing and access under different priority levels for primary and secondary users of the spectrum. Over the past two decades, this body of work has laid the foundation for the next stage of

evolution of cognitive radios, which will indeed become transformative in the next decade. Along these lines, this article attempts to capture two emerging directions in the general area of imbibing intelligent operation within radios and how they will impact the future of wireless. Specifically, it describes a vision for (i) building trust in the operation of such radios, and (ii) shaping the environment, going beyond merely reacting to it. The definition of the term "cognitive radio" above narrows its functions to self-reconfiguration. Instead, this article advocates for "intelligent interacting" (I^2) radios. I^2 radio operation is built on two key abilities: The first involves leveraging the power of connections whenever needed, be it among peer-radios or radios and humans. The second involves radios co-working with other configurable entities in the environment, which leads to interesting decisions on when to self-reconfigure (along the lines of the existing vision for cognitive radios) and when to reconfigure the environment itself.

3.2 Building trust in I^2 radios

Intelligent radio operation often relies on machine learning (ML), which is used to control the 'knobs' of radio operation. As an example, several approaches involving reinforcement learning and Bandit algorithms have been used to solve problems of which spectrum to access and when, based on assumptions of unknown activity patterns of the primary incumbents. For such methods, our understanding of crafting utility functions and rewards for radio operation has made rapid strides. More recently, deep neural networks have been shown to be remarkably successful for inference tasks when the underlying causes of an otherwise observable effect are unknown. As an example, models like VGG [SZ14] and ResNet [He+16] can classify one out several dozens of modulation classes or identify a particular emitter among several devices that of the same make/manufacturer/model and advertise bit-similar addresses. There are many other examples of such networks being used in beam selection, code-book generation, underlay signal detection, among others. Despite these success stories, a vexing question remains:

> How can we rely on such radios, if their operation relies on mathematical computations within a black box neural network?

Indeed, deep neural networks models have so far been resistant to interpretation and an elegant mathematical formulation that explains their inner workings has proven to be elusive. A possible way to break this impasse is to develop a notion of trust that is divorced from that of interpretability. Drawing an analogy from flying in an airplane, a passenger happily enjoys the in-flight food and entertainment for hours on end, well knowing that the plane is largely flying by itself. Control loops take in data from hundreds of different parameters, analyze them for context and then actuation decisions are made in split-second intervals by the flight computer. There may be an unexpected event that the algorithms have not been designed for, which can lead to catastrophic consequences if left to the machine alone. For these reasons, there is always a human pilot on hand, who can assume control and recover from machine errors. Thus, the passenger trusts the combined human pilot and autopilot system that can potentially check and guide each other. The overall

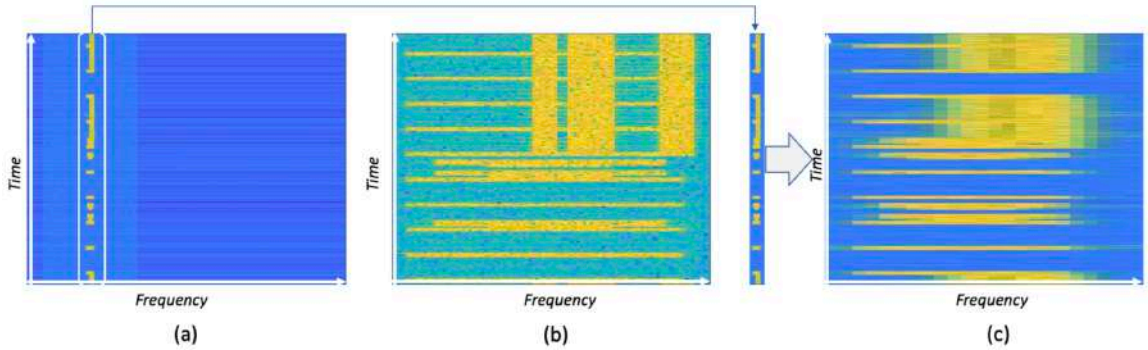


Figure 3.1: Sample spectrograms for training an ML model to detect the presence of LTE signals (shown by yellow color) for different sampling rates. Spectrograms in (a) and (b) are obtained at a sampling rate of 100MHz and 12.5MHz, respectively. Spectrogram (c) is constructed by artificially "stretching and interpolating" a sliver of spectrogram (a), which now resembles the lower frequency spectrogram (b).

system is far too complex for a lay passenger to be interpretable and yet there is a notion of trust.

We need to revisit our expectations of intelligent radios, especially in the context of problems that require deep learning models not amenable to full interpretation. For mission-critical systems, the radio should be able to interact with (again the motivation for I^2 radios becomes relevant here) and query a human expert or even a deterministic model of the system. These gentle guiding efforts may allow the I^2 radios to perform better over time. Thus, the notion of trust here does not stem from the expectation that the radio will always perform optimally, but rather from the belief that it will know to seek help from an external expert when needed. There are several open challenges that must be addressed to realize this goal.

3.2.1 Knowing When Past Learning Falls Short

Test performance of a radio running an ML model depends on whether the training data is sufficiently representative of test conditions. As an example, consider the case when a radio is trying to identify the presence of an unauthorized LTE signal in the 3.5GHz Citizens Broadcast Radio Service (CBRS) band. If the machine learning model for detecting the LTE signal is trained on spectrograms obtained at a high sampling rate (see Fig 3.1 (a)), it will not perform well if the test signal is obtained at a lower sampling rate (see Fig 3.1 (b)). This scenario can be addressed locally by the radio, by data augmentation methods. The training dataset can be sliced and stretched with pixel interpolations to resemble a lower sampling rate spectrogram (see Fig 3.1 (c)), even if such data is not available at training time. The radio needs to distinguish cases like this from others wherein local augmentation is not possible. The latter cases arise when new signals need to be detected, or equivalently, new classes are introduced, requiring a completely new dataset. As shown in Fig 3.2 (a-b), detecting signals after introducing a new class, i.e frequency hopping spread spectrum signal (FHSS) needs external support for the radio. Prior works that examine whether the

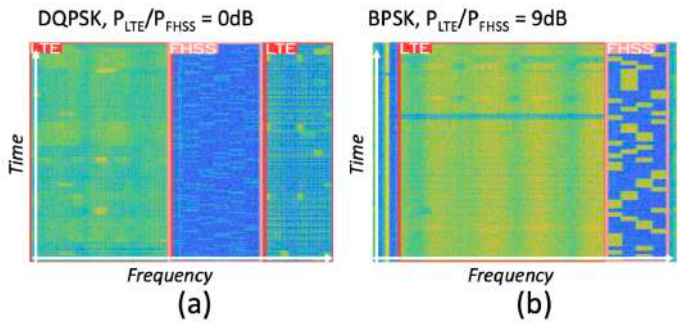


Figure 3.2: Apart from LTE discussed in Fig 3.1 earlier, a new FHSS signal is introduced. To detect this new class, a new dataset needs to be created followed by another round of training. Two different spectrograms are shown for different modulations of the FHSS signal and relative powers of the LTE and FHSS signals.

test data comes from out-of-distribution (i.e., may contain classes not seen during training time) are an excellent starting point [Gri+19; Kat+22]. This step can then trigger expert-led (the expert here can be either human or machine) efforts for minimal new data collection in the unseen environment and/or selective labeling of previously data collected in new environments by the expert. In these cases, the overhead associated with data collection (in the former case, using meta learning [FAL17]) and data labeling (in the latter case, using active learning [ZKN22]) is minimized. In all of these, there is on-demand interaction between the deployed ML and the remote expert, and this coordination is an integral part of the I^2 radio vision.

3.2.2 Analyzing the Cost of Querying the Expert

The cost of querying the expert is the price of trust. Consider real-time and non-real time costs in the following examples. There is an increasing trend towards swapping classical deterministic signal processing blocks with their corresponding machine learning-based models. In a recent paper [Sol+22], we showed that indeed a modular NN-based receiver improves bit error rate of the traditional non-ML receiver (implemented in MATLAB) by 61% and 10% for simulated and over-the-air collected datasets, respectively, for certain low signal-to-noise ratio (SNR) conditions. However, in the process of establishing trust in these ML models, there is no option for offline querying, as the receiver must process millions of IQ samples per second. Thus, if the expert is situated closeby, possibly on the same chip itself that executes the NN models, then the cost of querying in terms of time can potentially become negligible (see Fig 3.3). An intriguing concept of 'cost' may arise from seeking the output of the deterministic algorithm that is licensed by a patent holder. More the number of queries that are sent to the expert, more is the billing incurred. In a future era where ML-based 'black boxes' are poised to circumvent core-technology IP held by major companies, this could be a possible revenue model for the latter.

On the other hand, querying a remote expert may be possible for longer-time scales for problems such as network slicing for resource allocation at the base station, scheduling policy selection, among others. The expert may reside remotely, at the network edge or a

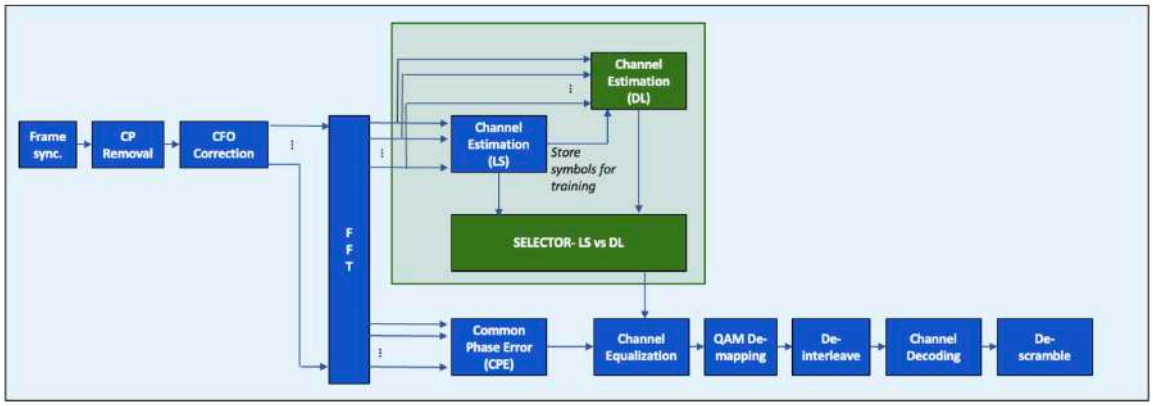


Figure 3.3: A typical OFDM receiver chain with the traditional signal processing blocks (blue) and the additional machine learning related blocks (green) using deep learning (DL) co-existing within the same chip. The DL module can learn the outcomes based on traditional least-square based channel estimation by querying the pure signal processing LS block.

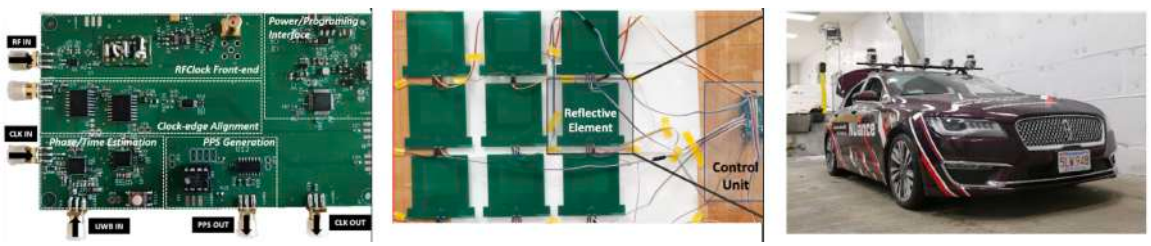


Figure 3.4: (a) Custom designed time/phase/frequency synchronization circuit, (b) 9-element RIS design, each of which can set , and (c) car mounted LiDAR, camera and directional beamforming arrays

centralized cloud; in fact, many related problems form the core focus interest of the US NSF indeed AI-Edge Institute [NSF]. Thus, the cost in this case is the impact on the wireless link efficiency and the overall end to end latency for sending the control data to the expert and the decision back to the radio. To fully characterize this, more research is needed on whether some of the queries can be pre-emptive, the wireless/wired standard used for control, and the frequency of such queries: possibly, early on, the queries are more frequent and then taper off with time as the ML model gains more experience. Again, all these metrics depend highly on interaction with the I^2 radio.

3.3 Shaping the Environment

3.3.1 Using RF Sources

Future I^2 radios will proactively interact with each other as well as with other passive embedded technology like reconfigurable intelligent surfaces (RIS) to force changes in the wireless propagation environment. Proactive interaction among radios can take several

forms, as we describe below with examples. Consider a situation where the receiver is located in a high interference or in a non-line-of-sight (NLOS) environment which considerably reduces the signal to interference and noise ratio (SINR). This increases the bit error rate at the receiver. Here, multiple transmitter radios that share the same information to be transmitted can coordinate their actions to ensure their respective signals align at the same time with constructive phases to increase the SINR at the receiver. However, radios will need to synchronize their clocks, generate a common timing pulse reference as well as start their transmissions with suitable delays (depending on their respective locations) to ensure that all signals arrive at the same instant. While this form of coordinated beamforming is challenging enough for line-of-sight (LOS) conditions, identifying suitable reflecting paths for each radio in NLOS conditions for the desired effect at the receiver is yet to be addressed. We demonstrated such distributed coordinated beamforming for software defined radios in static and mobile scenarios for LOS conditions. Central to enable such a desired outcome is contact-free synchronization, for which we designed a customized hardware circuit to exchange control signals among all the radios in the network, [Ale+21] (see Fig. 3.4 (a)). Thus, the overheads are considerable, requiring specialized synchronization hardware and then incurring the cost of sharing the information to be communicated among the entire group of transmitters. Several other interesting scenarios have been proposed by the research community that include radios working together by injecting specially constructed RF signals in the shared wireless medium to cancel out undesired interference at the receiver to intentionally introducing signal transformations that result in incorrect classifying of waveform features like the modulation class [Kim+22].

A new and exciting paradigm that is being actively investigated by the community involves setting the reflection properties of the surrounding surfaces through RIS. This allows a fine-grained control over the signal propagation path, allowing the signals to overcome blocking obstacles and increase directivity. Different from the proactive coordination between radios described earlier, the RIS are generally considered as passive elements in the sense that they do not radiate energy. By carefully adjusting the reflection phase of each element, the entire surface becomes programmable. There are a number of challenges in such interactions:

1. *Configuring RIS in real time*: Radios transmit specially designed preambles that may be used for channel estimation at the receiver side. However, for passive RIS, adapting to changing wireless conditions is a challenge since they do not explicitly emit signals. Furthermore as the wireless channel changes over time, setting the optimal reflection phases of each of the RIS element must be completed within the coherence time of the channel. For ubiquitously deployed RIS that can have thousands of individual elements, clearly exhaustive search is not feasible. If the phases of each element can be changed on a continuous scale, then the entire network need not operate under the limitations of a fixed size codebook. While such a capability may allow the RIS to accurately track the motion of a target receiver, it increases the difficulty in setting the parameters of the RIS. Our prototype design (see Fig. 3.4 (b)) allows for selecting 4-different phases for each RIS element in a 9-element RIS surface by activating the delays in a transmission line. Even under such limited systems design, the computational challenges involved is setting the correct phases under different channel conditions imposes real-time operational challenges.

2. *Protocols for RIS to I^2 radio links*: There is no standardized protocol today for I^2 radios to discover the presence of RIS, identify the transmitter-RIS-receiver positional constraints and harness computational support from a local edge compute service and then issue control directives in near-real time. Without such a dedicated control channel for these tasks, the promise of shaping the wireless environment in real time cannot be achieved.

3.3.2 Using non-RF Sources

Shaping the environment can involve interacting with more than just RF devices. We are surrounded by a number of sensors that capture data in the form of camera images, LiDAR and radar to name a few. These sensors can be mounted statically in public spaces as well as on vehicles, and the resulting data stream can be fused to obtain contextual information of the environment in which the radios operate. In recent work, we explored how such information could be utilized through deep learning models to guide beam selection for car and road-side base station mounted radios [Sal+22] through datasets collected on actual autonomous cars (see Fig 3.4 (c)). Akin to human cognition that relies on information obtained via different senses, future I^2 radios will rely on non-RF sources, requiring new ways to think about obtaining such information and processing them at the network edge.

This novel form of cognition will require shaping the environment in context of where to place such multimodal sensors and how to design efficient control channels that can work reliably during network congestion and in the rich multipath observed in urban canyons. There are a number of tools for creation of virtual environments, from open-source to cutting-edge industry products. For example, the Raymobtime dataset [Kla+18] captures a virtual deployment with high fidelity in the urban canyon region of Rosslyn, Virginia for different traffic patterns. A static roadside base station is placed at a height of 4 meters, alongside moving buses, cars, and trucks. The image and LiDAR sensor data are collected by Blender, and Blender Sensor Simulation (BlenSor) [Gsc+11] software, respectively. Such a tool can be utilized to create virtual worlds, populate it with radios, sensors, movement and traffic patterns and examine the effects of how multimodal data can be best utilized by the I^2 radios. This can then be utilized to create the real world with similar performance characteristics once several possible options are explored in the digital domain. Technology companies like NVIDIA and Meta will soon release platforms like the Omniverse [NVI] and products like the Metaverse navigating headsets [Met], which will enable how the real world is eventually shaped and how radios and humans interact within them.

3.4 Conclusion

We are at an opportune moment when wireless technologies are poised to make a transformative jump. Radios will soon continuously interact with themselves and the environment, not only to reconfigure themselves but also active emitters and passive reflectors that will be ubiquitously deployed. They will utilize vast amounts of multimodal data that will be generated by thousands of sensors in the environment. Driven by advances in edge computing, radios will gain contextual knowledge of the environment in which they operate, and some of this can also be used to iteratively improve the real world by careful

placement of all the proactive and passive interacting devices. While the benefits are many, there are also some concerns on what the underlying ability of interaction between I^2 radios will entail: Could such radios form groups and display emergent behavior that is at least unfair if not malicious towards non I^2 radios? Are we, as humans, prepared to give up our need for interpretability and elegant mathematical representations of underlying wireless behavior for performance gains shown by a 'black box' neural network? What new economic models must be designed for traditional wireless processing blocks to co-exist within future wireless transceivers that are progressively being replaced module by module? While we will certainly advance the science and formulate solutions to the above seemingly vexing problems, at core, we need to retool ourselves. The lines between the physics of signal propagation, signal processing, computation, learning, device fabrication, sensors and networks protocols are blurring. Cross-disciplinary knowledge and considering the environment and its many interactions holistically through the I^2 concept, as opposed to operation of a single and isolated radio, is a promising way forward.

References

[FCC03] FCC. *Notice of proposed rulemaking and order, ET Docket No. 03-222*. December 2003.

[SZ14] Karen Simonyan and Andrew Zisserman. *Very Deep Convolutional Networks for Large-Scale Image Recognition*. 2014. DOI: *10.48550/ARXIV.1409.1556*. URL: *https://arxiv.org/abs/1409.1556*.

[He+16] Kaiming He et al. "Deep Residual Learning for Image Recognition". In: *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. 2016, pages 770–778. DOI: *10.1109/CVPR.2016.90*.

[Gri+19] Andrey Gritsenko et al. "Finding a 'New' Needle in the Haystack: Unseen Radio Detection in Large Populations Using Deep Learning". In: *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 2019, pages 1–10. DOI: *10.1109/DySPAN.2019.8935862*.

[Kat+22] Julian Katz-Samuels et al. "Training OOD Detectors in their Natural Habitats". In: *Proceedings of the 39th International Conference on Machine Learning*. Edited by Kamalika Chaudhuri et al. Volume 162. Proceedings of Machine Learning Research. PMLR, 17–23 Jul 2022, pages 10848–10865. URL: *https://proceedings.mlr.press/v162/katz-samuels22a.html*.

[FAL17] Chelsea Finn, Pieter Abbeel, and Sergey Levine. "Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks". In: *Proceedings of the 34th International Conference on Machine Learning - Volume 70*. ICML'17. Sydney, NSW, Australia: JMLR.org, 2017, pages 1126–1135.

[ZKN22] Jifan Zhang, Julian Katz-Samuels, and Robert Nowak. "GALAXY: Graph-based Active Learning at the Extreme". In: *Proceedings of the 39th International Conference on Machine Learning*. Edited by Kamalika Chaudhuri et al. Volume 162. Proceedings of Machine Learning Research. PMLR, 17–23 Jul 2022, pages 26223–26238. URL: *https://proceedings.mlr.press/v162/zhang22k.html*.

[Sol+22] N. Soltani et al. "Neural Network-based OFDM Receiver for Resource-Constrained IoT Devices". In: *IEEE Internet of Things Magazine*. 2022.

[NSF] NSF AI-Edge. *AI Institute for Networking Research*. URL: *https://aiedge.osu.edu*.

[Ale+21] Kubra Alemdar et al. "RFClock: Timing, Phase and Frequency Synchronization for Distributed Wireless Networks". In: *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. MobiCom '21. New Orleans, Louisiana: Association for Computing Machinery, 2021, pages 15–27. ISBN: 9781450383424. DOI: *10.1145/3447993.3448623*. URL: *https://doi.org/10.1145/3447993.3448623*.

[Kim+22] Brian Kim et al. "Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers". In: *IEEE Transactions on Wireless Communications* 21.6 (2022), pages 3868–3880. DOI: *10.1109/TWC.2021.3124855*.

[Sal+22] Batool Salehi et al. "Deep Learning on Multimodal Sensor Data at the Wireless Edge for Vehicular Network". In: *IEEE Transactions on Vehicular Technology* 71 (2022), pages 7639–7655.

[Kla+18] Aldebaro Klautau et al. "5G MIMO Data for Machine Learning: Application to Beam-Selection Using Deep Learning". In: *2018 Information Theory and Applications Workshop (ITA)*. 2018, pages 1–9. DOI: *10.1109/ITA.2018.8503086*.

[Gsc+11] Michael Gschwandtner et al. "BlenSor: Blender Sensor Simulation Toolbox". In: *Advances in Visual Computing*. Edited by George Bebis et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pages 199–208. ISBN: 978-3-642-24031-7.

[NVI] NVIDIA. *Omniverse*. URL: *https://www.nvidia.com/en-in/omniverse/*.

[Met] Meta. *Immersive Learning*. URL: *https://about.meta.com/immersive-learning/*.

The Author

Kaushik Chowdhury is Professor in the Electrical and Computer Engineering Department, Associate Director of the Institute for the Wireless IoT at Northeastern University, Boston and co-PI on The Ohio State University-led NSF AI-Edge Institute from Northeastern. He is the winner of the U.S. Presidential Early Career Award for Scientists and Engineers (PECASE) in 2017, the Defense Advanced Research Projects Agency Young Faculty Award in 2017, the Office of Naval Research Director of Research Early Career Award in 2016, and the National Science Foundation (NSF) CAREER award in 2015. He is the recipient of best paper awards at IEEE GLOBECOM'19, DySPAN'19, INFOCOM'17, ICC'13,'12,'09, and ICNC'13. He serves as area editor for IEEE Trans. on Mobile Computing, Elsevier Computer Networks Journal, IEEE Trans. on Networking, and IEEE Trans. on Wireless Communications. He co-directs the operations of Colosseum RF/network emulator, as well as the Platforms for Advanced Wireless Research project office. Prof.Chowdhury has served in several leadership roles, including Chair of the IEEE Technical Committee on Simulation, and as Technical Program Chair for IEEE INFOCOM 2021, IEEE CCNC 2021, IEEE DySPAN 2021, and ACM MobiHoc 2022. His research interests are in applied machine learning for wireless communications and networks, data-centric IoT architectures, and large-scale experimentation.

4. Insights of Prof. Rose Hu

Machine Learning in Spectrum Sharing and Its Security and Privacy

Author: Prof. Rose Qingyang Hu,
Utah State University
Logan, UT, USA,
Email: *rose.hu@usu.edu*

The rapid growth of internet connected systems has generated numerous challenges, such as spectrum shortage issues, which require efficient spectrum sharing (SS) solutions. Complicated and dynamic SS systems can be exposed to various potential security and privacy issues, requiring protection mechanisms to be intelligent, adaptive, reliable, and scalable. Machine learning (ML) based methods have been deemed promising in addressing those demands. This point article provides a survey on recent developments of ML based SS methods, some critical security issues, and corresponding ML based defense mechanisms. The article elaborates the state-of-the-art methodologies for improving the performance of SS communication systems for various vital aspects, including ML based cognitive radio networks (CRNs), ML based database assisted SS networks, ML based LTE-U networks, ML based ambient backscatter networks, and other ML based SS solutions. It also presents security and privacy issues, mainly from physical layer perspectives and corresponding defending strategies based on ML algorithms.

4.1 Introduction

The explosion of data traffic growth, massive number of devices, and commercialization of the 5G wireless communication networks impose great challenges on spectrum usage as well as data security [Wan+22][Sun+18]. On the one hand, in order to meet requirements in the 5G communication system, the future wireless solutions should provide a $10-100$ times higher data rate and support a $10-100$ times higher density of connected devices. On the other hand, the spectrum fragmentation and the crowed spectrum occupation, especially below 6GHz, can potentially hamper the progress of achieving these capacity and connectivity goals. Furthermore, the complicated communication environments and data driven usage scenarios can leave users and systems to potential attacks. Thus security and privacy issues have become one of the primary concerns in future wireless networks.

SS networks can effectively help relieve the shortage of spectrum resources. Different from traditional exclusive frequency allocations, SS by definition involves multiple entities to use the spectrum in a shared or nonexclusive way in order to increase the efficiency of the limited spectrum resources.

One of the technical challenges in the SS system is how to guarantee the performance of different users while achieving the efficient spectrum usage. Towards that end, spectrum access mechanism, interference control, resource allocation, and fairness need to be tackled in a dynamic and collaborative way. Since the concept of SS was first introduced, different SS frameworks based on various usage scenarios have been developed by researchers.

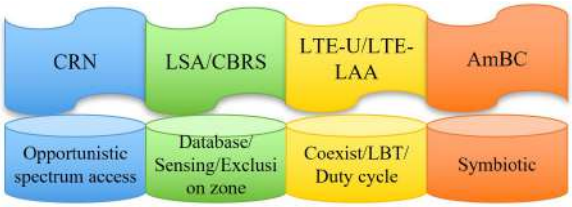


Figure 4.1: Spectrum sharing paradigm.

As shown in Fig. 4.1, spectrum sharing was originated from the concept of opportunistic access. Database-supported access frameworks on a specific licensed frequency band were then developed to connect new users to the unused licensed band without degrading the performance of IUs to improve the SE. As the number of devices as well as the demands for the network capacity quickly increase, extending services based on the licensed band to the unlicensed band was adopted. LTE-U uses the unlicensed band to improve the licensed users' performance. Furthermore, symbiotic schemes such as AmBCs can help meet the needs from the massive growth of IoT devices that normally have power and resource limitations, providing a new paradigm for spectrum sharing. Although these different mechanises share some overlapping features such as sensing and access control, each has its distinctive focuses. 5G has a very broad technical scope and needs to address a variety of communication goals. Therefore, investigating SS under different frameworks can provide very instrumental views for future wireless communication system development.

Nevertheless, to fully exploit the great potentials of SS, users need to interact intelligently with complex and dynamic radio environments to gain high quality channel access and

control, the interference. Relying only on traditional radio access technologies will not be able to tackle such a level of complexity. With the advancements of computing technologies and algorithmic development, ML has garnered tremendous motivations and recently has demonstrated great potentials for tackling large-scale, highly dynamic, very complicated problems that traditional techniques may not readily handle. Many studies have demonstrated that ML algorithms are very powerful and effective in handling tasks such as data classification, decision-making, facial recognition, etc [BLJ13].

The combination of ML with SS networks is very appealing given that SS decisions are normally based on data collected through sensing and measurements. For all the frameworks mentioned above, users in the SS network need to observe the spectrum resource usage and make corresponding decisions in accordance with three major actions, i.e., perception, learning, and reasoning [BLJ13]. In ML, a user first senses the surrounding environment and internal states through perception to obtain information. It further transforms that information into knowledge by using different classification methodologies and generalizes the hypothesis. Based on the obtained knowledge, it then makes decisions through reasoning.

The development of SS techniques can help relieve spectrum scarcity. However, due to the dynamic sharing of spectrum resources by many different users, SS systems can be exposed to various malicious attackers. Firstly, the lack of ownership of the spectrum leaves unlicensed users highly susceptible to malicious attacks. Therefore, it presents more challenges to protect their opportunistic spectrum access from adversaries. Secondly, the dynamic spectrum availability and distributed network architecture make it more difficult to implement coordinated security countermeasures. Moreover, in some SS systems, PUs may contain sensitive information, which can be effortlessly obtained by malicious SUs during the SS process. Thirdly, new technologies such as ML may also be exploited by attackers to launch some new attacks. This article mainly focuses on the threats and mitigation strategies in the physical layer of the SS network. It first investigates works related to two classical spectrum sensing attacks in the SS network, i.e., PUE attacks and SSDF attacks, which aim to disturb the spectrum observation and users' access to the system. It also studies methods of preventing two attacks that exist in wireless communication networks, i.e., jamming attacks and eavesdropping attacks. Yet the special features of the SS network provide new defense solutions for these common wireless attacks. When PUs share their licensed spectrum with multi-type users in some SS frameworks, privacy issues can also arise. While, application of ML in security countermeasures yield effective solutions potentially, it also gives attackers new opportunities and intelligence to disturb system operations.

4.2 ML-based Methodologies for SS

4.2.1 ML Based CRN

In a CRN, unlicensed SUs need to identify vacant or unoccupied licensed frequency bands (or spectrum holes) owned by licensed PUs [Hos+20]. After detecting the spectrum holes, SUs can access them without visibly interfering with any PUs. If a PU's activity reappears, SUs must vacate the corresponding spectrum immediately. This dynamic and uncertain

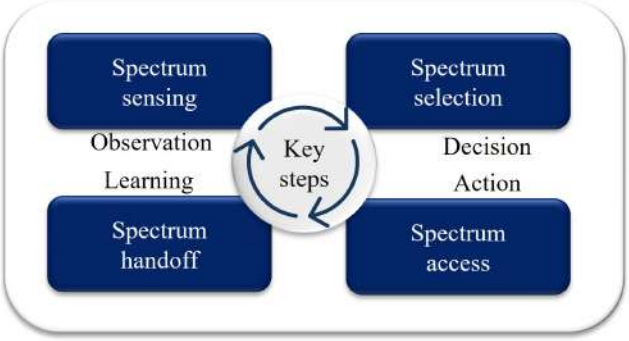


Figure 4.2: Key steps in CRN.

spectrum access creates unique and complex challenges. ML algorithms offer unique advantages in dealing with such challenges.

As shown in Fig. 4.2, the major steps in CRN can be summarized as spectrum sensing, spectrum selection, spectrum access, and spectrum handoff [Aky+06]. A CR agent first uses the sensing function to monitor the unused spectrum and search for possible access opportunities for SUs. Based on the sensing results, the spectrum selection function helps SUs select the best available channels. The spectrum access mechanisms provide fair spectrum scheduling among vying SUs. Since a channel must be vacated when the PU reappears, the corresponding SU must perform a spectrum handoff function to switch to another available channel or wait until another channel becomes idle. Most of the existing SS approaches adopted these four steps in their frameworks.

Spectrum Sensing

Before an SU accesses the licensed channel, it needs to first observe and measure the state of the spectral occupancy (i.e., idle/busy) by performing spectrum sensing. During this procedure, the SU needs to distinguish the PU signals from background noise and interference. As such, spectrum sensing can be formed as a classification problem.

A new approach, as shown in Fig. 4.3, to training data augmentation and domain adaptation was presented in [DS18]. A Generative Adversarial Network (GAN) with DL structures was employed to generate additional synthetic training data to improve classifier accuracy and adapt training data to spectrum dynamics. This approach can be used to perform spectrum sensing when only limited training data is available and no knowledge of spectrum statistics is assumed.

Spectrum Selection

The spectrum selection is performed to capture the best available spectrum to meet user needs based on the sensing outcomes. As a decision-making problem, it requires the system to adaptively select the optimal choice based on observations of the environment. RL algorithms are appealing tools for designing systems that need to perform adaptive decision-making.

As shown in Fig. 4.4, at the beginning of the RL cycle, the agent receives a full or partial

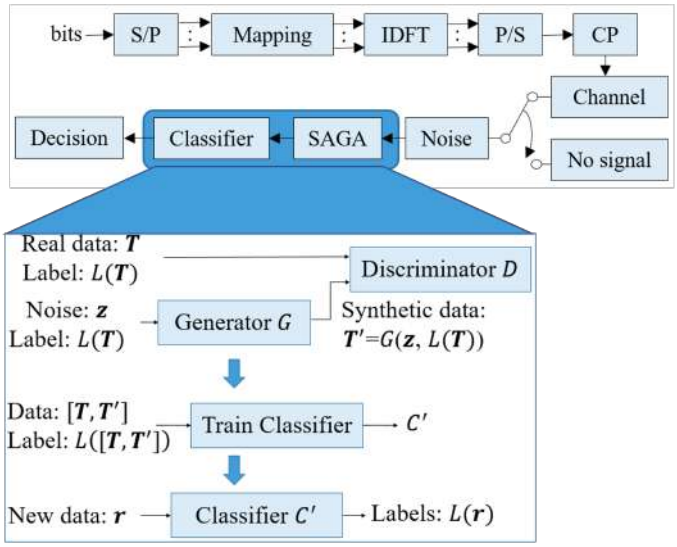


Figure 4.3: OFDM transmitter and receiver structure with SAGA for spectrum sensing and workflow for training data augmentation. [DS18].

observation of current states and the corresponding reward. Combining those states and rewards, the policy is updated by each agent during the learning stage. Then the agent performs a certain selection action based on the updated policy at the decision stage. With RL, CRN can be modeled as a distributed self-organized multi-agent system in which each SU or agent performs spectrum selection by efficiently interacting with the environment through a learning policy. In this approach, other SUs' decisions can be considered as a part of the responses of the environment for each SU.

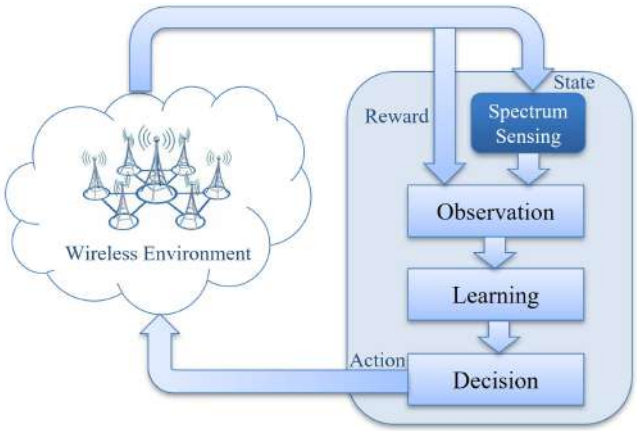


Figure 4.4: The reinforcement learning cycle.

Spectrum Access

One important question in CRN spectrum access is related to how to assign limited resources, such as available spectrum channels and transmit powers, to maximize the system

throughput and efficiency.

An RL-based resource allocation approach entitled Q-Learning and State-Action-Reward-State-Action (SARSA) was proposed in [KK20]. It mitigates interference without the requirements of the network model information. Users in this method act as multiple agents and cooperate in a decentralized manner. A stochastic dynamic algorithm was formed to determine the best resource allocation strategy. It was shown that the energy efficiency could be significantly improved by the proposed approach without sacrificing user's other QoS metrics.

Spectrum Handoff

Spectrum handoff is intended to maintain seamless communication during the transition to a better spectrum. However, enabling spectrum handoff for multimedia applications in a CRN is challenging due to multiple interruptions from PUs, contentions among SUs, and heterogeneous Quality-of-Experience (QoE) requirements. Although an SU may not know exactly when the PU comes back, it always wants to achieve reliable spectrum usage to support the QoS requirements. If the quality of the current channel degrades, the SU can make one of the following three decisions:

(1) Stay in the same channel and wait for it to become idle again (called stay-and-wait).
(2) Stay in the same channel and adapt to the varying channel conditions (called stay-and-adjust).
(3) Switch to another channel that meets the QoS requirement (called spectrum handoff).

In [Wu+14], a learning-based and QoE-driven spectrum handoff scheme was proposed to maximize the multimedia users' satisfaction. A mixed preemptive and non-preemptive resume priority (PRP/NPRP) M/G/1 queueing model was designed for the spectrum usage behaviors of prioritized multimedia applications. The RL-assisted QoE-driven spectrum handoff scheme was developed to maximize the quality of video transmissions in the long term. Their proposed learning scheme could adaptively perform spectrum handoff based on the variation of channel conditions and traffic loads.

4.2.2 ML Based LTE-U/LTE-LAA

LTE-U has emerged as an effective technique for alleviating spectrum scarcity. Using LTE-U along with some advanced techniques such as carrier aggregation can boost the performance of existing cellular networks. However, LTE was initially designed to operate in the licensed spectrum exclusively and was not for harmonious coexistence with other possible co-located technologies [Tan+20]. For this reason, introducing LTE into the unlicensed spectrum leads to possible coexistence issues with other well-established unlicensed technologies such as Wi-Fi, IEEE 802.15.4, or Bluetooth. To enable fair spectrum sharing with other technologies operating in the unlicensed spectrum, in particular with Wi-Fi, new schemes to allow coexistence are needed. On the other hand, not much research attention has been given to studying cooperation across different technologies. Networks that participate in a cooperation scheme can exchange information directly or indirectly (via a third-party entity) to improve the efficiency of spectrum usage in a fairway.

To standardize LAA technology in the 5 GHz spectrum, the Third-Generation Partnership

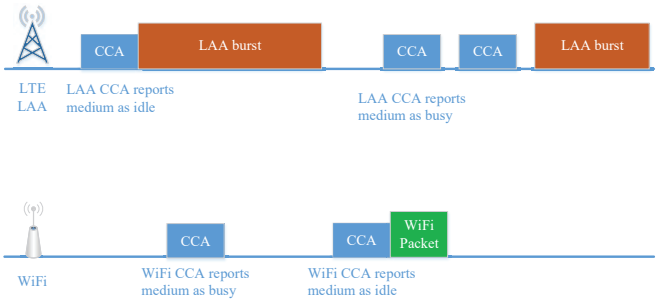


Figure 4.5: LBT based method.

Project (3GPP) standardization group aims to develop a single global framework of LTE in the unlicensed bands. The framework should guarantee that the operation of LTE does not critically affect the performance of WiFi networks. The works started with the downlink LTE-A (LTE Advanced) Carrier Aggregation (CA) in the unlicensed band. This was later expanded to operate downlink and uplink simultaneously[Par+16]. The LTE LAA employs a Listen Before Talk (LBT) mechanism to avoid collision and interference among users.

LTE-U is another option for operating LTE in an unlicensed spectrum, where LTE base stations exploit transmission gaps to facilitate coexistence with WiFi networks. The development of LTE-U technology has been led by the LTE-U Forum, an industry alliance. LTE-U has been designed to operate as an unlicensed LTE in countries where the LBT technique is not mandatory. LTE-U defines the operation of primary cells in a licensed band with one or two secondary cells (SCells), every 20 MHz in the 5 GHz unlicensed band: U-NII-1 and/or U-NII-3 bands, spanning 5150–5250 MHz and 5725–5825 MHz, respectively [Par+16].

Here are some specific ML based schemes.

- ML Based LBT Methods
  According to LTE LAA standards in 3GPP Release 13, the LTE system must perform the LBT procedure (also known as Clear Channel Assessment, CCA) and sense the channel prior to a transmission in the unlicensed spectrum. As shown in Fig. 4.5, when the channel is sensed to be busy, the LTE system must defer its transmission by performing an exponential backoff. If the channel is sensed to be idle, it performs a transmission burst with a duration from $2 - 10$ ms, depending on the channel access priority class.
- ML based Duty Cycle Methods

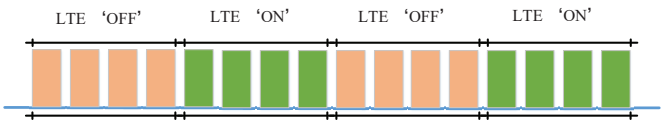


Figure 4.6: Duty cycle based method.

Carrier Sensing Adaptive Transmission (CSAT) is a technique that can enable coexis-

tence between LTE and Wi-Fi based on minor modifications of the 3GPP LTE Release 10/11/12 Carrier Aggregation protocols. As shown in Fig. 4.6, CSAT introduces the use of duty cycle periods and divides the time into LTE "ON" and LTE "OFF" slots. During the LTE "OFF" period, also known as the "mute" period, LTE remains silent, giving other coexisting networks, such as Wi-Fi, the opportunity to transmit. During the LTE "ON" period, LTE accesses the channel without sensing it before transmission. Moreover, CSAT allows short transmission gaps during the LTE "ON" period to allow for latency-sensitive applications, such as VoIP in co-located networks. In CSAT, eNB senses the medium during a time period ranging from 10 to 100 ms and according to the observed channel utilization (based on the estimated number of Wi-Fi APs) defines the duration of the LTE "ON" and LTE "OFF" periods [Tan+20].

- The existing work of LTE-U mainly focuses on using different RL algorithms to adjust the duty cycle and other network resources to maintain fairness between LTE and WiFi users, as well as to seek for a higher system capacity performance [Tan+20; Su+18; Cai+16; Zha+17].

4.2.3 Ambient Backscatter Networks

A technology named AmBC has received significant attention as a new SS framework [Liu+13]. In backscatter communication (e.g., RFID), a device communicates by modulating its reflections of an incident RF signal without generating its own radio waves. Hence, it is significantly more energy-efficient than conventional radio communication. AmBC system enables two devices to communicate using ambient RF as the only source of power.

In particular, in an AmBC system as illustrated in Fig. 4.7, the backscatter transmitter can transmit data to the backscatter receiver by modulating and reflecting surrounding ambient signals. Hence, the communication in the AmBC system does not require dedicated frequency spectrum. Based on the received signals from the backscatter transmitter and the RF source or carrier emitter, the receiver then can decode and obtain useful information from the transmitter. By separating the carrier emitter and the backscatter receiver, the number of RF components is minimized at backscatter devices and the devices can operate actively, i.e., a backscatter transmitter can transmit data without initiation from receivers when it harvests sufficient energy from the RF source [Van+18]. Therefore, AmBC systems can share spectrum with existing systems and achieve better spectral efficiency than that of RFID systems.

The existing ML based works for AmBC systems are mainly focused on the information extraction and mode selections.

Information Extraction

Since ambient backscatter uses uncontrollable RF signals that already have information encoded in them, it needs a different mechanism to extract the backscattered information. In an AmBC system, the readers receive the backscattered signal from the backscatter device (BD) and the Direct-Link Interference (DLI) from the RF source simultaneously. Due to the randomness of ambient RF sources, it is challenging to distinguish backscatter symbols from DLI. Furthermore, the existence of DLI can further cause the conventional Energy Detector (ED) to fall into severe error floor problems. [Guo+19] developed a novel

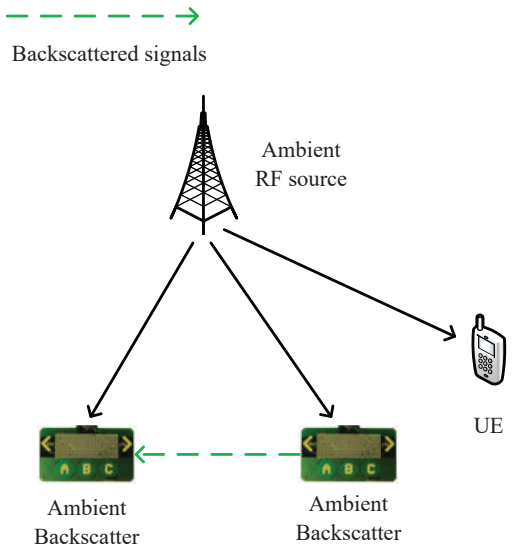


Figure 4.7: AmBC network.

error-floor free detector by using multiple receive antennas at the reader side. Based on this, a novel statistical clustering framework was designed for joint CSI feature learning and backscatter symbol detection.

Operating Mode Selection and User Coordination

Due to its passive nature, Backscatter Devices (BDs) in AmBC systems must harvest energy to power operations such as circuit power consumption, transmission, and sensing. Moreover, although the BD can perform the backscatter and energy harvesting simultaneously, it is impractical and inefficient when the amount of harvested energy is relatively small and can only supply internal operations. Therefore, how to efficiently determine the tradeoff between energy harvesting and backscattering RF signals is critical in a dynamic environment. By adaptively selecting the operating mode in a fading channel environment, the throughput maximization problem of the AmBC system was solved in [Wen+19]. A Q-learning algorithm was employed to explore a suboptimal strategy through repeated interactions with the environment. The efficacy of their proposed Q-learning method showed that close-to-optimal throughput performance could be achieved.

4.3 ML in Security and Privacy of SS Systems

While the ML-based SS networks can help improve the performance, they can also be a double-edged sword to be exploited by the attackers. The dynamic access frameworks introduce more security and privacy risks into the system. As shown in Fig. 4.8, when SUs observe the activity of PUs, the sensing procedure can be disturbed by the malicious attackers by launching the PUE attacks or SSDF attacks. The attackers may also exploit these

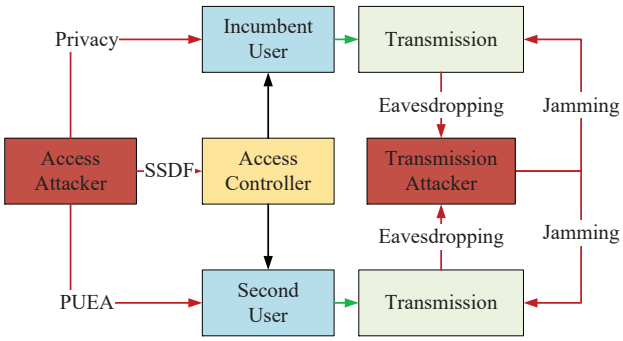


Figure 4.8: Secure and privacy issues in SS network.

opportunities to harm the privacy of PUs. The system also suffers the same security issues found in traditional wireless communications, such as jamming attacks and eavesdropping attacks. Besides launching attacks based on the SS framework, attackers can also attack the ML models.

4.3.1 Primary User Emulation Attack

In CRN, a PUE attack denotes a PU-like signals sent by an attacker during the spectrum sensing period that can exclude legitimate SU access to the channels. The attackers may be selfish users who want to use the spectrum exclusively or malicious attackers who want to disrupt the normal operation of the system. PUE attacks can cause service degradation, denial of service (DoS), connection unreliability, and bandwidth waste.

A typical PUE attack is illustrated in Fig. 4.9. In defending against such attacks, the most important step is to distinguish malicious attackers from legitimate PUs. This can be achieved using specific features extracted from received signals. Distinct features may reflect the transmitters' characters, rendering them unique and differentiable. User location based method is a common and easy way to differentiate between attackers and PUs. Since the received signal strength (RSS) varies by location, it can be adopted to identify location and user type. Some other methods are based on statistical analysis. They use features such as signal power, spectrum occupancy time, and cyclostationarity extracted from received signals to analyze transmitters. Finally, the physical layer approaches uses the hardware behaviors of transmitters or channel behaviors to detect attackers. For example, phase and frequency shifts are commonly used as transmitter fingerprints. A detection problem based on received signals is a classification problem, which ML is particularly good at solving [AU20; MFG20; IK20; Alb+19; Don+18; Fur+20; Elg20; CKN11; SS15; SSM19].

4.3.2 Spectrum Sensing Data Falsification Attack

A group of SUs can collaborate to perform the spectrum sensing by exchanging locally-collected information. An SSDF attack (also known as the Byzantine attack) is launched by sending false local spectrum sensing results to others, leading to flawed spectrum sensing decisions. SSDF attacks aim to decrease detection probability and disturb normal operations

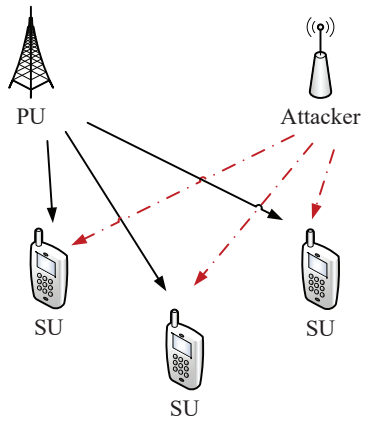


Figure 4.9: Illustration of PUE attacks.

of the primary system. It may also seek to increase the probability of false alarms in order to deprive honest SUs of access opportunities . SSDF attacks harm the system's integrity and

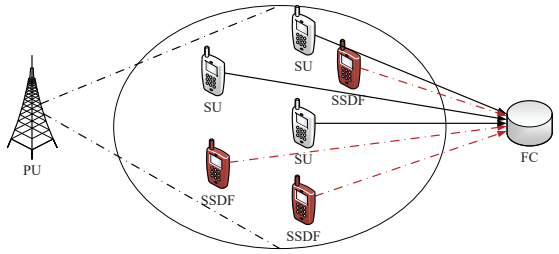


Figure 4.10: Illustration of SSDF attack.

Cooperative Spectrum Sensing (CSS) can help overcome the fading environments and improve the system sensing performance. Different from single-user-based SS, each SU needs to transmit the sensing results to a Fusion Center (FC) in CSS. FC then combines those results and makes a final decision about the PU's presence. SSDF is the most common attack in CSS. As shown in Fig. 4.10, sending falsified sensing data to the FC can lead to an incorrect fusion result, cause interference with PUs, and cause DoS to SUs. To defend against SSDF attacks, the most important step is to differentiate attackers from legal SUs. The existing defense methods fall into two groups, namely outlier detection approaches and reputation-based approaches [FAB11; Nie+17; Huo+15; STM20]. In outlier detection methods, the abnormal user is excluded from the network. In reputation-based methods, on the other hand, SUs are assigned a reputation degree that reflects their detection performance. Since SUs are not eliminated and their reports are not excluded, reputation-based methods can use the collected information more thoroughly than outlier detection techniques.

4.3.3 Jamming Attacks

The open and broadcasting nature of wireless channels leaves them vulnerable to various attacks. One commonly seen attack in wireless communications is jamming attack. Attackers transmit signals to interfere with the victims' communications in order to cause a DoS and compromise availability of communication links. Traditional anti-jamming methods in wireless communications include sequence-based frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). However, the fixed transmission patterns of these methods hamper their effectiveness against dynamic jamming attacks.

ML enabled techniques can provide more adaptive channel selection ability to systems tp tackle jamming attacks. They also give the system the ability to learn and predict the behaviors of jammers and increase anti-jamming channel selection efficiency. On the other hand, the attackers may also use different ML based methods to improve their attack strategies rendering the study of advanced jamming attacks and corresponding countermeasures of vital importance to the SS system.

Most jamming countermeasures focus on how to enable users to efficiently escape the invaded channel. AmBC opens the possibility fighting against the malicious jammers. As shown in Fig. 4.11, a method that allows wireless nodes to fight against a jamming attack instead of escaping was proposed in [Van+19]. By first learning the adversary's jamming strategy, the users could decide whether or not to adopt the rate or backscatter modulated information on the jamming signals. A dueling neural network architecture-based DRL algorithm was developed to deal with unknown jamming attacks such as jamming strategies, jamming power levels, and jamming capability. The proposed algorithm allowed the transmitter to effectively learn about the jammer and conceive optimal countermeasure actions such as adapting the transmission rate, backscattering, harvesting energy, or staying idle. The system performance in terms of learning speed, throughput, and packet loss were all significantly improved by the proposed algorithm.

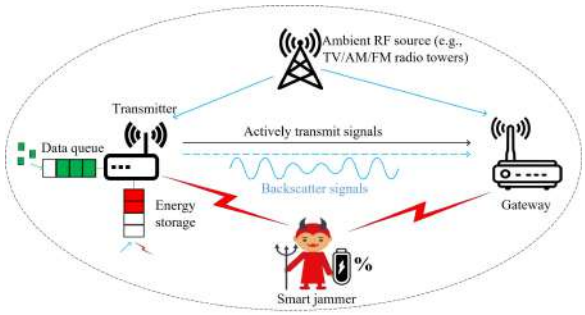


Figure 4.11: Anti-jamming attack in AmBC-CRN [Van+19].

4.3.4 Intercept/Eavesdrop

Eavesdropping is another common attack in wireless communications. Due to the broadcasting nature of radio propagation, any active transmissions operated over the shared spectrum by different wireless networks are extremely vulnerable to eavesdropping. It is therefore important to investigate the confidentiality protection of SS communications

against eavesdropping attacks.

There are two major categories of secure communication techniques that guard against eavesdropping. One focuses on traditional cryptographic techniques and the other one is based on the physical layer security. Cryptographic techniques involve encryption and decryption of information at the transmitter and receiver. In the physical layer security method, the secrecy rate can be achieved by the mutual information difference between the legitimate user and the eavesdropper. However, the security rate can be limited since it depends on the difference between the channel condition from the transmitter to the legitimate receiver and that from the transmitter to the eavesdroppers. Many promising techniques have been proposed to address this issue, including artificial noise (AN) and cooperative jammer (CJ). The advantage of physical layer security over cryptographic is that it can achieve secure communications without extra overhead caused by protecting the security key and can therefore be used in relatively simple communication systems.

As shown in Fig. 4.12, nondirectional forms of communication in AmBC networks are prone to information leakage. Reducing the side lobe level is therefore crucial to preventing eavesdropping. To this end, an ML-based antenna design scheme was proposed in [HLK19] that achieved directional communication between transceivers by combining patch antenna with Log Periodic Dual-dipole Antenna (LPDA). Aiming to limit the number of large side lobes and reduce the Side Lobe Level (SLL), a multi-objective genetic algorithm was proposed to optimize the antenna side lobe, gain, standing wave ratio, and return loss. It was shown the proposed method could significantly reduce information leakage while guaranteeing communication quality.

Figure 4.12: Influence of antenna side lobes on communication. [HLK19].

4.3.5 Privacy Issues in SS Systems

Security normally refers to unauthorized/malicious access, change, or denial of data while privacy normally refers to the unintentional disclosure of sensitive information from some open-access data. The former is usually the work of malicious attackers who wish to disturb the system. In the latter, malicious users usually only collect information that does not immediately cause direct harm to the system. A seemingly harmless open dataset may

contain clues to an individual's private information in real life.

The protection of PUs privacy may not be addressed by strictly controlling access to the database, since each SU must access it to enable the spectrum sharing process. One possible solution might be to reveal obfuscated information instead of the original information to SU queries. By doing this, the system can use the obfuscated information to help determine the channel status while reducing leakage of PU's privacy information.

ML algorithms require massive amount of data to train their models. These data usually include a lot of user-specific sensitive info and need to be exchanged in some distributed systems. Sensitive information may leak out during the training process that would have remained secure using the above spectrum sensing procedure. Three main strategies may be used to maintain privacy in ML work flow: differential privacy, homomorphic encryption and Secure Function Evaluation (SFE)/Secure Multi-party Computation (SMC) [Li+20]. In the differential privacy method, publicly shared dataset information describes the patterns of groups within the dataset but withholds information about individuals. In homomorphic encryption, the operation on encrypted data can be used to secure the learning process by computing on encrypted data. When user-generated data are distributed among different data owners, SFE can enable multiple parties to collaboratively compute an agreed-upon function without leaking input information regarding any party other than what can be inferred from the output.

4.3.6 Attacks on ML model

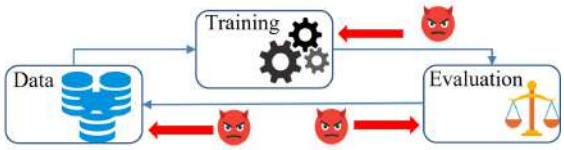


Figure 4.13: Illustration of attacks to ML model.

Besides launching attacks based on the SS framework, attackers can also attack the ML models. As shown in Fig. 4.13, a typical ML using data to train a model and then evaluating the trained model with the test data can expose its workflow to various types of attacks: Exploratory attacks, Evasion attacks, Poisoning attacks, Backdoor attacks, etc. [Shi+18a].

Exploratory attacks, also called inference attacks, discover how the underlying ML works for an application. It usually maintains a surrogate model to mock the victim ML system with the same input and output data types. Exploratory attacks aim to infer sensitive and proprietary information of victim systems to launch vast subsequent attacks to it. There are limited existing works that studied exploratory attacks for CRN networks and corresponding defense methods [Shi+18b]. The attackers can sense the victims' activities to build an ML model, and defenders can also deliberately mislead the attackers' model.

Evasion attackers might trick the ML algorithm into making wrong decisions, such as fooling a security algorithm into accepting an adversary as legitimate. It can be achieved by manipulating the test data to mislead the model. Existing research on evasion attacks in SS communication systems mainly focuses on misleading the classifier at the receiver side by launching the spectrum poisoning attacks during the sensing phase. It aims to change

the channel status features and forces the system to make wrong transmission decisions. It should be noted that this attack differs from SSDF attacks because the attackers mainly focus on injecting adversarial perturbations over the air to the channel instead participated in CSS [Shi+18a] [SSE19].

Poisoning attacks, also called causative attacks, provide incorrect information such as training data to the ML to cause the ML model to perform poorly. The poisoning attacks in the context of SS networks have been investigated in [Luo+20], which can be achieved by fooling the classifiers with spectrum data falsifications during the CSS phase, similar to SSDF attacks.

Backdoor attackers train the ML model by deliberately misclassifying any input with an added trigger to a specific target label. The attackers need to first construct the backdoored data that contains a trigger within a subset of clean data and change their labels to the target one. They then mix this backdoored data with clean data to train the model to learn the original tasks and backdoor behaviors [Sal+20]. Backdoor attacks can be exploited to help the attackers to pass the authentication system and grant unauthorized access right. This can cause severe security and privacy consequences for ML-based SS networks, such as ML-based database-assisted SS systems and distributed ML models-based defense approaches.

4.4 Conclusions

This article investigates various technologies and mechanisms in applying ML in spectrum sharing and its related security and privacy. Four SS application scenarios were first investigated, i.e., opportunistic access-based CRNs, database-assisted SS systems, LTE-U/LTE-LAA networks, and symbiotic SS mechanism-based AmBC networks. A comprehensive investigation of state-of-the-art ML-based ML based SS solutions and their performance gains were discussed. However, it has been noted that the dynamic access and sharing paradigms of SS networks, as well as using ML in SS, may open the system to many security and privacy concerns. Correspondingly two typical spectrum sensing attacks were discussed, i.e., PUE and SSDF. Two common wireless attacks, i.e., jamming and eavesdropping, during wireless access and transmission in the context of the SS network were also discussed. Furthermore, connecting a large number of users and the application of ML all require massive information exchanges, generating tremendous concerns about privacy. The article further presented the state-of-art research on privacy protection for SUs and PUs, as well as the use of ML mechanisms. Finally the article discussed possible attacks on ML models and corresponding defending mechanisms.

References

[Wan+22] Qun Wang et al. “When Machine Learning Meets Spectrum Sharing Security: Methodologies and Challenges”. In: *IEEE Open Journal of the Communications Society* 3 (2022), pages 176–208. DOI: *10.1109/OJCOMS.2022.3146364*.

[Sun+18] H. Sun et al. "Wearable Communications in 5G: Challenges and Enabling Technologies". In: *IEEE Vehicular Technology Magazine* 13.3 (2018), pages 100–109. DOI: *10.1109/MVT.2018.2810317*.

[BLJ13] M. Bkassiny, Y. Li, and S. K. Jayaweera. "A Survey on Machine-Learning Techniques in Cognitive Radios". In: *IEEE Communications Surveys Tutorials* 15.3 (2013), pages 1136–1159. DOI: *10.1109/SURV.2012.100412.00017*.

[Hos+20] M. A. Hossain et al. "Comprehensive Survey of Machine Learning Approaches in Cognitive Radio-Based Vehicular Ad Hoc Networks". In: *IEEE Access* 8 (2020), pages 78054–78108.

[Aky+06] Ian F. Akyildiz et al. "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey". In: *Computer Networks* 50.13 (2006), pages 2127–2159.

[DS18] K. Davaslioglu and Y. E. Sagduyu. "Generative Adversarial Learning for Spectrum Sensing". In: *2018 IEEE International Conference on Communications (ICC)*. 2018, pages 1–6.

[KK20] A. Kaur and K. Kumar. "Energy-Efficient Resource Allocation in Cognitive Radio Networks Under Cooperative Multi-Agent Model-Free Reinforcement Learning Schemes". In: *IEEE Transactions on Network and Service Management* 17.3 (2020), pages 1337–1348.

[Wu+14] Y. Wu et al. "A Learning-Based QoE-Driven Spectrum Handoff Scheme for Multimedia Transmissions over Cognitive Radio Networks". In: *IEEE Journal on Selected Areas in Communications* 32.11 (2014), pages 2134–2148.

[Tan+20] J. Tan et al. "Intelligent Sharing for LTE and WiFi Systems in Unlicensed Bands: A Deep Reinforcement Learning Approach". In: *IEEE Transactions on Communications* 68.5 (2020), pages 2793–2808.

[Par+16] Imtiaz Parvez et al. "CBRS spectrum sharing between LTE-U and WiFi: A multiarmed bandit approach". In: *Mobile Information Systems* 2016 (2016).

[Su+18] Y. Su et al. "LTE-U and Wi-Fi Coexistence Algorithm Based on Q-learning in Multi-Channel". In: *IEEE Access* 6 (2018), pages 13644–13652.

[Cai+16] F. Cai et al. "Spectrum sharing for LTE and WiFi coexistence using decision tree and game theory". In: *2016 IEEE Wireless Communications and Networking Conference*. 2016, pages 1–6.

[Zha+17] N. Zhang et al. "QoE Driven Decentralized Spectrum Sharing in 5G Networks: Potential Game Approach". In: *IEEE Transactions on Vehicular Technology* 66.9 (2017), pages 7797–7808.

[Liu+13] Vincent Liu et al. "Ambient Backscatter: Wireless Communication out of Thin Air". In: *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*. SIGCOMM '13. Hong Kong, China: Association for Computing Machinery, 2013, pages 39–50. ISBN: 9781450320566.

[Van+18] N. Van Huynh et al. "Ambient Backscatter Communications: A Contemporary Survey". In: *IEEE Communications Surveys Tutorials* 20.4 (2018), pages 2889–2922.

[Guo+19] H. Guo et al. "Exploiting Multiple Antennas for Cognitive Ambient Backscatter Communication". In: *IEEE Internet of Things Journal* 6.1 (2019), pages 765–775.

[Wen+19] X. Wen et al. "Throughput Maximization for Ambient Backscatter Communication: A Reinforcement Learning Approach". In: *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. 2019, pages 997–1003.

[AU20] S. Arun and G. Umamaheswari. "An Adaptive Learning-Based Attack Detection Technique for Mitigating Primary User Emulation in Cognitive Radio Networks". In: *Circuits, Systems, and Signal Processing* 39.2 (Feb. 2020), pages 1071–1088. ISSN: 1531-5878.

[MFG20] Mohsen Mahmoudi, Karim Faez, and Abdorasoul Ghasemi. "Defense against primary user emulation attackers based on adaptive Bayesian learning automata in cognitive radio networks". In: *Ad Hoc Networks* 102 (2020), page 102147. ISSN: 1570-8705.

[IK20] M. A. Inamdar and H. V. Kumaraswamy. "Accurate Primary User Emulation Attack (PUEA) Detection in Cognitive Radio Network using KNN and ANN Classifier". In: *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*. 2020, pages 490–495.

[Alb+19] A. Albehadili et al. "Machine Learning-based Primary User Emulation Attack Detection In Cognitive Radio Networks using Pattern Described Link-Signature (PDLS)". In: *2019 Wireless Telecommunications Symposium (WTS)*. 2019, pages 1–7.

[Don+18] Q. Dong et al. "Explore Recurrent Neural Network for PUE Attack Detection in Practical CRN Models". In: *2018 IEEE International Smart Cities Conference (ISC2)*. 2018, pages 1–9.

[Fur+20] Haji M. Furqan et al. "Primary user emulation and jamming attack detection in cognitive radio via sparse coding". In: *EURASIP Journal on Wireless Communications and Networking* 2020.1 (July 2020), page 141. ISSN: 1687-1499.

[Elg20] Sally M. Elghamrawy. "Security in Cognitive Radio Network: Defense against Primary User Emulation attacks using Genetic Artificial Bee Colony (GABC) algorithm". In: *Future Generation Computer Systems* 109 (2020), pages 479–487. ISSN: 0167-739X. DOI: *https://doi.org/10.1016/j.future.2018.08.022*. URL: *http://www.sciencedirect.com/science/article/pii/S0167739X17321246*.

[CKN11] T. C. Clancy, A. Khawar, and T. R. Newman. "Robust Signal Classification Using Unsupervised Learning". In: *IEEE Transactions on Wireless Communications* 10.4 (2011), pages 1289–1299.

[SS15] Y. Sharaf-Dabbagh and W. Saad. "Transfer learning for device fingerprinting with application to cognitive radio networks". In: *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2015, pages 2138–2142.

[SSM19] Sundar Srinivasan, KB Shivakumar, and Muazzam Mohammad. "Semi-supervised machine learning for primary user emulation attack detection and prevention through core-based analytics for cognitive radio networks". In: *International Journal of Distributed Sensor Networks* 15.9 (2019).

[FAB11] F. Farmani, M. Abbasi-Jannatabad, and R. Berangi. "Detection of SSDF Attack Using SVDD Algorithm in Cognitive Radio Networks". In: *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*. 2011, pages 201–204.

[Nie+17] G. Nie et al. "Byzantine Defense in Collaborative Spectrum Sensing via Bayesian Learning". In: *IEEE Access* 5 (2017), pages 20089–20098.

[Huo+15] Y. Huo et al. "Three-layer Bayesian model based spectrum sensing to detect malicious attacks in cognitive radio networks". In: *2015 IEEE International Conference on Communication Workshop (ICCW)*. 2015, pages 1640–1645.

[STM20] Rupam Sarmah, Amar Taggu, and Ningrinla Marchang. "Detecting Byzantine attack in cognitive radio networks using machine learning". In: *Wireless Networks* (July 2020). ISSN: 1572-8196.

[Van+19] N. Van Huynh et al. "Jam Me If You Can: Defeating Jammer With Deep Dueling Neural Network Architecture and Ambient Backscattering Augmented Communications". In: *IEEE Journal on Selected Areas in Communications* 37.11 (2019), pages 2603–2620.

[HLK19] Tao Hong, Cong Liu, and Michel Kadoch. "Machine learning based antenna design for physical layer security in ambient backscatter communications". In: *Wireless Communications and Mobile Computing* 2019 (2019).

[Li+20] T. Li et al. "Federated Learning: Challenges, Methods, and Future Directions". In: *IEEE Signal Processing Magazine* 37.3 (2020), pages 50–60. DOI: *10.1109/MSP.2020.2975749*.

[Shi+18a] Y. Shi et al. "Spectrum Data Poisoning with Adversarial Deep Learning". In: *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*. 2018, pages 407–412.

[Shi+18b] Y. Shi et al. "Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies". In: *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2018, pages 1–6.

[SSE19] Yalin E. Sagduyu, Yi Shi, and Tugba Erpek. "IoT Network Security from the Perspective of Adversarial Deep Learning". In: *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 2019, pages 1–9. DOI: *10.1109/SAHCN.2019.8824956*.

[Luo+20] Zhengping Luo et al. "When Attackers Meet AI: Learning-empowered Attacks in Cooperative Spectrum Sensing". In: *IEEE Transactions on Mobile Computing* (2020), pages 1–1. DOI: *10.1109/TMC.2020.3030061*.

[Sal+20] Ahmed Salem et al. "Dynamic backdoor attacks against machine learning models". In: *arXiv preprint arXiv:2003.03675* (2020).

The Author

Rose Qingyang Hu (Fellow, IEEE) received the B.S. degree from the University of Science and Technology of China, the M.S. degree from New York University, and the Ph.D. degree from the University of Kansas. Besides a decade academia experience, she has more than 10 years of R&D experience with Nortel, Blackberry, and Intel as a Technical Manager, a Senior Wireless System Architect, and a Senior Research Scientist, actively participating in industrial 4G technology development, standardization, system level simulation, and performance evaluation. She is currently a Professor with the Electrical and Computer Engineering Department and Associate Dean for research of College of Engineering at Utah State University. She also directs Communications Network Innovation Lab at Utah State University. Her current research interests include next-generation wireless system design, Internet of Things, Cyber Physical system, Mobile Edge Computing, V2X communications, AI/ML in wireless networks. She has published over 300 papers in leading IEEE journals and conferences and also holds 30 issued patents. She is an IEEE Communications Society Distinguished Lecturer Class 2015-2018, IEEE Vehicular Technology Society Distinguished Lecturer Class 2020-2022, and a recipient of prestigious Best Paper Awards from the IEEE GLOBECOM 2012, the IEEE ICC 2015, the IEEE VTC Spring and the IEEE ICC 2016. She is currently an IEEE ComSoc BoG member serving as the Chief Information Office and also a member of Phi Kappa Phi Honor Society.

5. Views of Prof. Walid Saad

The Path to Cognition in Wireless Networks: Which AI do We Need?

Authors: Walid Saad and Christina Chaccour,
Bradley Department of Electrical and Computer Engineering,
Virginia Tech, Arlington, VA, USA,
Emails: {walids, christinac}@vt.edu

Abstract: Cognition has been a holy grail of artificial intelligence (AI) since more than a decade. Simultaneously, the seminal works of Mitola and Haykin had articulated the need to design so-called cognitive wireless networks that can mimic the human brain. However, remarkably, to date, neither the AI nor the wireless communities have achieved this much coveted "cognition" goal. In this position paper, we opine that achieving cognition requires fundamental advances in the AI tools that are used today, particularly in the wireless community. Towards this end, we first identify the key characteristics needed to build next-generation AI frameworks that can achieve certain levels of cognition suitable for wireless networks. These characteristics include reasoning faculties, generalizability, lifelong learning, sustainability, explainability, and distributed, collective learning. We then discuss the challenges and opportunities associated with deploying AI algorithms that can meet those characteristics in wireless networks, while pinpointing recent advances in this space within the wireless domain. In a nutshell, this position paper charts out a roadmap

for designing next-generation AI frameworks that are apropos for building next-generation AI-native wireless networks with concrete cognition abilities.

5.1 Introduction

The concept of a "cognitive" network emerged nearly two decades ago through the seminal works of Mitola [MM99] and Haykin [Hay05] that envisioned the proliferation of human intelligence into wireless networks, through machine learning (ML) and artificial intelligence (AI) techniques. In these seminal contributions, that created the whole field of *cognitive radio networks*, the primary function of ML and AI was to enhance the observation and management of the radio spectrum. Yet, despite the significant progress that cognitive radio research has ushered in, the use of AI in real-world wireless systems remained insipid for many years due to various barriers, some technical and others regulatory. However, the massive advances in computing technologies, that led to the emergence of deep learning, rekindled the interest in the design of AI-driven techniques to solve a plethora of problems in the wireless networking domain, that go well beyond the classical AI-based spectrum sharing and spectrum management techniques that were the major focus of cognitive radio networks. This trend culminated in the emergence of the concept of *AI-native* wireless systems in which the entire set of network functions, protocols, and processes are designed from the ground up using AI-based algorithms. Indeed, academia, industry, and standardization bodies are now working on defining the requirements needed to design next-generation 6G wireless cellular systems as AI-native systems from the get-go.

However, remarkably, despite this massive interest in the use of AI for wireless system design, existing efforts remain limited in a number of ways. First, recent efforts on AI-native wireless systems (e.g., [Hoy+21]) primarily provide qualitative discussions on how such systems could like, with the focus being on explaining how ML algorithms could replace existing wireless functions. However, these works do not really specify the properties and features that the AI algorithms must meet in order to effectively design the functions of the wireless system. Meanwhile, the broad range of works that apply AI to wireless networks, such as those in [Ayo+18; OH17; Che+21a; Zha+21; YC10] (and references therein), primarily use existing ML and AI tools, such as deep Q reinforcement learning or autoencoders, to either reproduce a wireless function (e.g., modulation) or solve complex optimization problems (e.g., for resource management). Although these results significantly contributed to advancing our understanding of the potential of AI for wireless systems, they are limited in the following ways:

- *Reliance on Big Data:* Existing AI for wireless approaches still require significant amounts of data for training. This reliance on "big data" hinders the adoption of the designed algorithms in real-world wireless networks. Indeed, even if operators may own or have access to sufficient datasets, designing algorithms that require massive amounts of data to be trained and adapted will not be a scalable solution.
- *Centralized Training:* Many of the existing works require centralized training of the ML frameworks and algorithms. Even some of the solutions that use distributed multi-agent reinforcement learning may also adopt an offline, centralized training of the agents before their deployment. This reliance on centralized training introduces

an additional overhead that cannot be tolerated for future networks. As such, it is necessary to go towards truly distributed solutions that can create collective intelligence in the network.

- *AI Latency:* Existing AI algorithms, particularly those that rely on reinforcement learning and computationally complex artifical neural networks (ANNs), can introduce significant latency when deployed in real-world networks. This latency can stem from many aspects: a) the time needed for the algorithm to perform the prediction or converge to a solution, b) the time needed for training; if done online, c) the computational time, and d) the time needed to adapt to new, unseen environments. This additional latency components will render to use of AI-based protocols unsuitable for low-latency applications such as extended reality, the metaverse, and many others.
- *Reactive Protocols:* Most of the existing AI frameworks operate in a reactive fashion. This is particularly problematic when attempting to minimize any security threats to the wireless network. Here, one needs to go from a reactive mindset to a proactive one that can scrutinize and detect the root-causes of the problems.
- *Associational and Statistical Logic:* Today's AI frameworks are heavily reliant on ANNs which model statistical relationships in the data and attempt to perform decision making based on such relationships. Nonetheless, statistical relationships often fail to to unravel the underlying structure of the data [Cha+22]. Given that such frameworks fail to consider *causality* in the data, they fail to extract the root-causes of specific events and data points that might have a crucial effect on performance.
- *Limited Adaptation to Unseen or New Environments:* Most existing AI algorithms used in wireless systems are primarily tailored to one environment and a single ML task. In order to adapt to new environments or new tasks, existing solutions typically require a re-training phase or a significant latency overhead to adapt to new, unseen environments. As such, existing solutions are mostly unreliable in face of unknown/unseen environments and data points, which makes it difficult to adopt them in real-world wireless networks.
- *Catastrophic Forgetting:* Standard ANN architectures suffer from the problem of catastrophic forgetting, whereby the ML system completely and abruptly forgets previously learned information when it is presented with new information. For a wireless network whose operation must be continuous and whose environments change rapidly and often, such catastrophic forgetting significantly limits the effectiveness of AI-based protocols that rely heavily on standard ANNs.
- *Lack of Performance Guarantees:* Existing solutions for AI-based wireless designs often lack the ability to provide performance guarantees for the designed algorithm, this, in turn, has created a barrier of adoption in real-world systems.
- *Traditional siloed and rigid use-case approach:* Existing solutions that adopt AI to predict, optimize, and automate services while being "application-aware" are rigid and siloed. Such approaches cannot be scaled to the versatile needs of the networking stack. Each requirement or process is mostly managed and delivered through a separate process [Sha+19; Che+19; TP18], which makes the deployed AI agent unaware of potentially conflicting requirements.

The goal of this position paper is to revisit these limitations in existing AI algorithms and chart out a path towards a next-generation of AI frameworks that meet several of

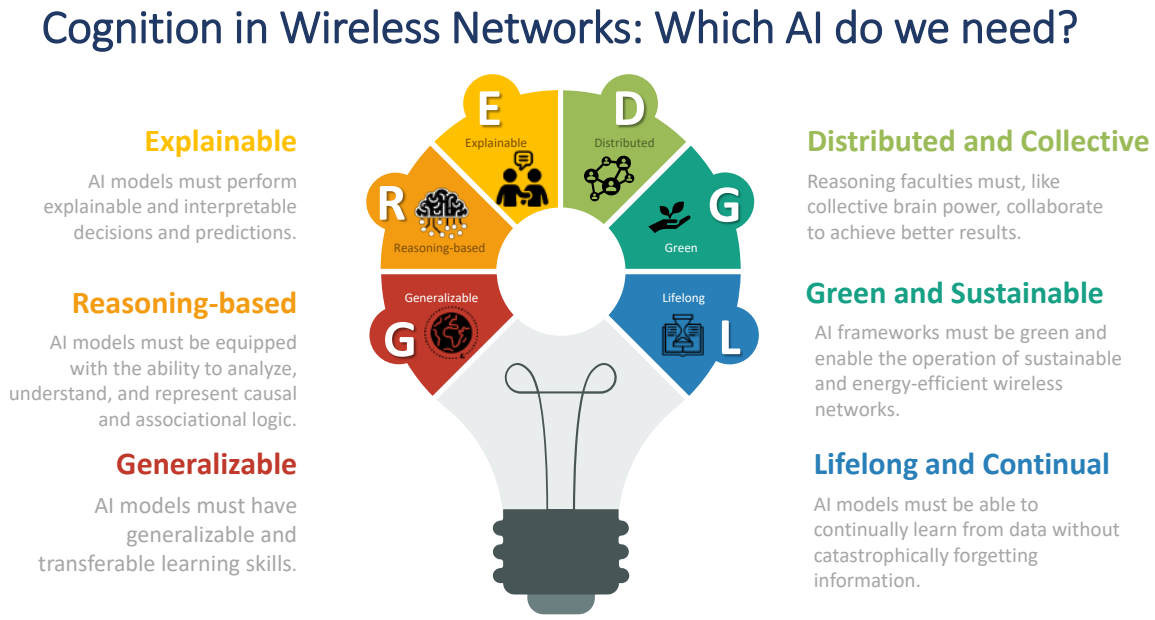


Figure 5.1: Illustrative figure showcasing the six key characteristics of next-generation AI frameworks for future wireless networks.

the requirements of future wireless systems, including the need for real-time distributed operation, low latency, performance guarantees, reliability in face of unseen events, generalizability, and effective adaptation to new environments. In particular, we opine that bringing true "cognition" to wireless systems requires fundamentally novel AI algorithms and frameworks that can overcome the aformenetioned challenges. In the next section, we provide a quick overview on the desiderata for next-generation wireless-centric AI algorithms. Then, we delve into the details of each requirements, while outlining the challenges, open problems, and early results.

5.2 Next-Generation AI for Next-Generation Wireless Systems: An Overview

The holy grail in AI research has always been the ability to design AI algorithms that can mimic the human brain cognitive functions. In fact, this is where the term "cognitive" came to be in the context of cognitive radio networks. There has been many recent attempts at designing such brain-like AI algorithms, ranging from the whole area of artificial general intelligence [GP07] which is the ability to create AI agents that can grasp and understand any intellectual task that the human brain can, to the research that attempts to link AI designs to the so-called System 2 brain model of Daniel Kahneman [Kah13].

Although these attempts provide meaningful analogies that are appealing for defining future goals of AI, most of them remain within the realm of speculation and qualitative discussions. However, from this rich literature, we can potentially draw a number of human brain features that can be useful for designing a next-generation AI framework that can overcome the challenges faced in the wireless domain, as outlined next.

5.2.1 Which AI Do We Need?

To mitigate the previously outlined challenges faced in the wireless domain, it is necessary to create the following desiderata that map the brain to the AI, as shown in Fig. 5.1:

- *Reasoning Faculties:* Reasoning faculties mainly stem from the ability to scrutinize causal and associational relationships in the data. The duality of *causal and associational* logic ultimately contributes to a *knowledge base* that mimics the human brain.
- *Transferability and Generalizability:* As a byproduct of reasoning faculties and causality, a learning agent must be able to consolidate the logic acquired from a particular *task*, and leverage this logic to a completely *new and unseen task*. This generalizability must be invariant to the distribution or domain of the data points.
- *Continual Lifelong Learning:* Given a wireless problem that requires learning from continuous datastreams over the course of time (e.g. mobility data, time series, etc) it is necessary to acquire a *robust* knowledge base without falling into the caveat of *catastrophic forgetting*. It is thus, necessary to study continual and lifelong learning mechanisms from the lense of *memory retention* in order to eliminate catastrophic forgetting [VT19].
- *Explainability:* Given that AI frameworks perform critical decision making (e.g. remote surgery), the rationale behind such decision making must be backed with explainability and interpretability. This explainability further enables improving the trustworthiness of the end-user and industrial bodies in AI for critical wireless services.
- *Collective Brain Power:* Reasoning faculties through causal and associational logic are reflected via a knowledge base hinging at the end of every learning agent. To reach a higher level of reasoning, given that a knowledge base mimics the human brain, knowledge bases too like humans could brainstorm together, execute collective tasks. Such a process enables learning agents and their corresponding knowledge bases to acquire generalizable and specialized learning skills[Ngu+20].

5.3 Generalizable and Transferable Learning Skills for Wireless Networking

One of the most important brain-like features that next-generation wireless systems must acquire is *generalizable* intelligence and transferable learning skills. In essence, when learning a particular task (e.g. beamforming, association scheme, network optimization, etc), the reasoning faculties of a learning agent, in a wireless network, must be able to use the knowledge acquired, and transfer it to different settings. In essence, the knowledge accumulated must enable the learning agent to have a directive that is invariant to: a) the domain, b) the distribution, and c) the context of the task. For instance, a learning agent that has acquired learning a beamforming scheme for millimeter-wave (mmWave) frequency band channel, must be able to generalize and transfer their knowledge to a terahertz (THz) or a visible light communication channel. Therefore a fundamental question that the wireless research community must answer in the next few years is the following: How can we design generalizable AI frameworks that can learn with “small data” and acquire learning and reasoning skills rather than being biased towards a single learning task?

5.3.1 Challenges and Open Problems

Naturally, to answer this fundamental question and achieve this ultimate generalizability for next-generation AI systems, we must overcome multiple challenges when considering wireless communication tasks, as discussed next.

- *How to Define a Learning Task?* The AI literature has recently witnessed a surge in works on meta-learning, transfer learning, and multi-task learning [FAL17; Yu+20; Sun+19]. While such works have seen a success in static, supervised learning, and well-defined use-cases outside the wireless domain such as robotics and image recognition; extending such concepts to wireless settings remains challenging and non-trivial. In essence, these existing solutions hinge on gaining a generalizability on a task domain. In robotics, for example, tasks such as opening a bottle, opening the door and many other rotational tasks share a large similarity. Nonetheless, in wireless settings, multiple parameters are intertwined and the objective of one learning task is often correlated with others. Thus, the very definition of a learning task within a wireless setting is much more challenging than the computer vision counterpart. Second, understanding the breadth and depth of the generalizability that can be achieved with respect to one learning task depends on the level of dynamics surrounding the task, as well as the intertwined objectives.
- *Time-critical Generalizability:* On top of the stringent generalizability requirement, a large number of wireless tasks, particularly those at lower layers, require a high time-criticality in the decision making process. Thus, if generalizability is achieved in a non-timely manner, then the prediction performed or the decision made becomes *obsolete* for the network. In fact, this requirement becomes of a higher significance when migrating towards extremely high frequency bands like mmWave and THz, where the coherence time of the channel is particularly small. In such cases, the deployed learning agent must be *fast and generalizable*. Here, on the one hand, computing advances must take place so that today's AI frameworks can be executed in a faster manner. On the other hand, novel out-of-the box AI frameworks that have a seamless training period and near-real time inference time must be deployed. For instance, the work in [Kas+20] proposed a generative adversarial network (GAN) approach to pre-train a deep-reinforcement learning framework using a mixture of synthetic and real datasets thus enabling the agent to assimilate a broad range of network conditions. We called this pre-training "experience" since it mimics how humans gain experience when meeting different tasks. This work has showcased a lower trial-and-error period and can be deployed for time-critical services. For instance, in Fig. 5.2 from [Kas+20], we showed how our proposed experienced deep reinforcement learning algorithm can quickly adapt to sudden changes in the network conditions (a traffic surge at epoch 100 in this figure), and this adaptation is much faster than that of an agent that has no experience, and agents that have a limited experience (with only synthetic or only real data, without using GAN). This showcases how reliability can be instilled into the learning process itself through a simple GAN-based training that can help overcome data scarcity by merging real datasets with synthetic datasets using GAN. Clearly, this approach remains in its infancy given its reliance on a single centralized learning agent and inability to learn versatile knowledge from multiple learning agents.

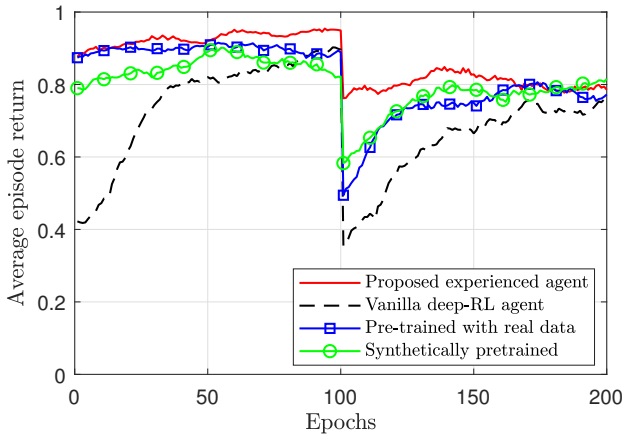


Figure 5.2: Reliability of experienced deep reinforcement learning in face of a sudden surge in traffic at epoch 20. [Kas+20]

5.3.2 Opportunities and Potential Solutions

- *From Statistical Learning to Causal Reasoning:* Today's AI frameworks are mostly focused on ANNs, which characterize the behavior of mechanisms based on the statistical relationships that govern the observed data points. Nonetheless, the behavior of wireless networks is not solely governed by statistical logic. In fact, similar to our daily life problems, one must unravel the *causal* relationships in the data. That said, today's AI state-of-the-art on causal learning is limited to causal graphs and causal discovery. Here, one must consider the concept of *structural causal models* and extend such concepts to characterize the behavior of wireless learning tasks. In [Cha+22], we have shown that causality is a necessary ingredient in establishing a solid reasoning faculty in semantic communication networks. We have also shown in [Cha+22] the role of structural causal models in establishing generalizable, efficient, and minimal semantic representations to ultimately communicate a robust and mature semantic language. Moreover, under such causal-based analysis, one can potentially derive performance guarantees, an aspect that is critical for wireless networks and that is not possible with classical ANNs.
- *Towards Neurosymbolic AI:* Understanding the behavior of a certain mechanism can be performed via two different perspectives. On the one hand, connectionist AI (the bigger umbrella that engulfs ANNs) postulates that learning associations from data (with little or no prior knowledge) is necessary. Here, learning is centered around understanding patterns of activation over the large connectionist network established. On the other hand, symbolic AI postulates that learning must be centered around symbol manipulation (e.g. graph algorithms, natural language processing, etc). That said, a more comprehensive view must be able to capture these two perspectives *simultaneously*. Neuro-symbolic AI is one form of integrating symbolic and connectionist systems. In [TS22], we have shown that causality-based neuro-symbolic AI can indeed help achieve minimal representations, create symmetric communication channels, enable generalizability, and reduce the amount of data

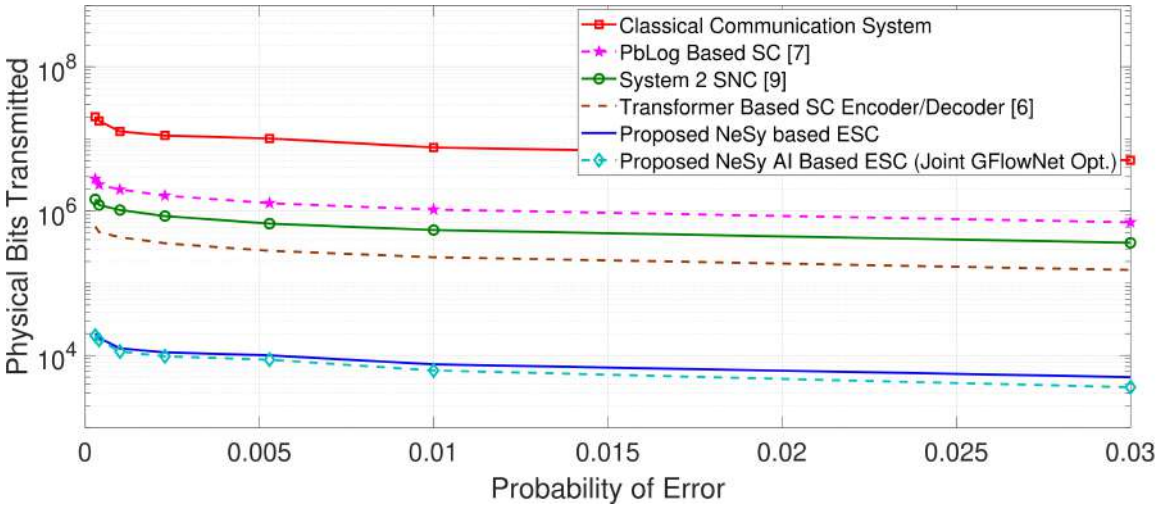


Figure 5.3: Neuro-symbolic (NeSy) AI as an effective tool for generalizability and improved transmission efficiency in the context of emergent semantic communication (ESC) systems. [TS22]

transmitted (see Fig. 5.3 which shows how neuro-symbolic AI outperforms System 2 AI and probabilistic logic AI, ProbLog). Indeed, next-generation AI frameworks for wireless systems must exploit the benefits of both connectionist and symbolic AI, and one fertile area for this exploration is that of semantic communication [Cha+22; TS22].

5.4 Continual Lifelong Learning

Across the networking stack, multiple wireless problems occur in which continuous datastreams over the course of time (e.g. mobility data, time series, etc) must be analyzed and used for prediction, optimization, or automation. Nonetheless, neural networks tend to suffer from the caveat of catastrophic forgetting when learning multiple tasks sequentially. Thus, it is necessary to propose new algorithms that can continually accumulate, organize, and act on knowledge *robsutly*, without any *gaps* in the knowledge.

5.4.1 Challenges and Open Problems

- *Breadth vs. Depth:* Deploying continual learning (and its variants) to solve particular wireless problems, enables gaining robustness versus the time domain, and a flavor of *time-variant generalizability*. In fact, in [HCS22], we have shown that adopting a variant of the elastic weight consolidation (EWC) technique enables digital twins (DTs) to maintain accurate and synchronous representations of their physical application, while preserving the history-aware nature of DTs and overcoming any increase in the de-synchronization time. In particular, as shown in our sample result in Fig. 5.4 from [HCS22] the model's robustness with respect to *catastrophic forgetting* is the best when deploying continual learning. This is verified by measuring the model's accuracy on the first episode after training on each episode successively. Moreover, our continual learning approach in [HCS22] can be further extended to optimize time-critical Internet of Everything (IoE) services (e.g., connected autonomy, robotics,

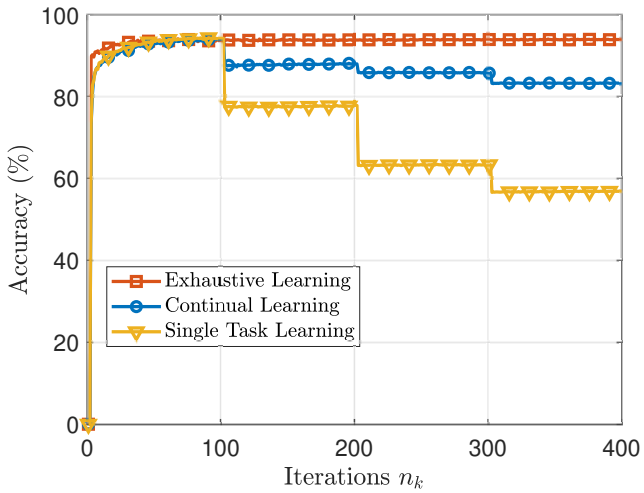


Figure 5.4: Accuracy (%) over the first episode versus iterations n_k [HCS22]

metaverse, and the likes) while addressing their various stringent quality-of-service requirements. However, remarkably in continual learning, the knowledge of the learning agent has evolved with respect to *depth* in the time domain. Here, to expand the learning agent's capability, one must investigate the design of new techniques that can achieve a high generalizability (breadth) while simultaneously improving their lifelong learning capabilities (breadth and depth simultaneously).

- *Storage Requirements:* The need for larger computing resources grows exponentially with the emergence of AI for wireless. Nonetheless, on top of dynamic memory, continual learning requires large amount of storage to *intelligently memorize* the history and mitigate catastrophic forgetting [CL18]. Here, it is necessary to explore minimalist techniques to store knowledge and historical memories. This is particularly challenging when dealing with resource-limited wireless network devices.

5.4.2 Opportunities and Potential Solutions

- *Hyper-game Continual Learning for Spectrum Sharing:* The problem of spectrum sharing in cognitive radio systems consists of a primary and a secondary user that interact in a non-cooperative manner. Here, *history-awareness* is necessary for each of the users, and thus, the AI model of each user must depend on a continual learning model. That said, it is necessary to orchestrate the decision making process between these users in a smooth, dynamic, and flexible scheme. Here, one can resort to game theory [Han+12], in general, and *hypergame theory* [KGL15], in particular. Essentially, hypergame theory is the amalgamation of game theory and decision theory, and it provides a set of tools that can be used to characterize the interaction between different users attempting to share the common spectrum. Clearly, this is a novel and unexplored research direction that could help enhance the AI performance when multiple noncooperative agents are interacting.
- *Self-Attention Continual Learning for IoE Services:* Equipping a learning agent with *breadth and depth* simultaneously is necessary for future IoE services. Here, one

approach that enables increasing the depth of continual learning mechanisms, is to first attempt to tune the *prior knowledge* that can help in learning a sequence of tasks continuously. This prior knowledge must have a *good generality* [SMP21; WKP21] that enables improving the decision making respect vis-a-vis various dimensions (time, domain, distribution). This can done via self-attention meta learning, which attempts to initiate priors by fine-tuning attention models in the knowledge, so as to learn general and specific representations as done in [SMP21]. Clearly, self-supervised and self-attention learning is a nascent avenue that should be further researched so as to mitigate the *breadth vs depth* dilemma in continual learning.

5.5 Distributed, Collective Intelligence

As already discussed, the next-generation of AI systems for wireless networks must be able to operate in a fully distributed manner. In fact, collective intelligence itself requires distributed sharing among multiple reasoning or learning agents that can work together towards an end goal in the network. There has been two popular tools used to enable distributed learning in wireless networks: federated learning (FL) [Kon+16] (and its variants) and distributed multi-agent reinforcement learning (MARL). One the one hand, FL has been a very popular tool for enabling distributed learning. FL essentially enables a group of agents to collectively learn one or more tasks of interest, by exchanging some sort of representation of their individual learning frameworks (e.g., neural network weights). There has been a surge of literature that exploited FL for various wireless networking contexts in recent years [Che+20a; Che+21b; Yan+21; Che+21c; Zho+22; Le+21; Don+21]. These include the use of FL to enhance data-driven learning of network parameters [Che+20a; Zho+22; Le+21; Don+21] as well as the design of FL algorithms that can operate over real-world wireless networks [Che+21b; Yan+21; Che+21c]. Meanwhile, MARL has been a popular tool for solving challenging optimization problems in a distributed way. The key advantage of MARL is that it enables a group of agents to execute either a common task or multiple, interdependent tasks, in a distributed way. Therefore, MARL is a very appealing solution for addressing a broad spectrum of wireless networking problems ranging from network optimization to distributed coordination and control over wireless networks.

5.5.1 Challenges and Open Problems

Clearly, FL, MARL, and their variants are promising tools to instill distributed operation into wireless networks, however, there are a number of challenges and open problems that must be addressed:

- *From distributed FL to swarm AI:* Despite its advantages in distributed learning, FL was primarily motivated by privacy considerations, and its distributed nature was only a "nice-to-have" feature. In fact, in its original form, FL still relied on a parameter server that centrally controlled the process. A key challenge here is to design fully distributed FL algorithms that can move from server-guided collaborative learning, in which a group of agents can preserve their privacy while relying on a centralized server to coordinate their learning towards collective, swarm intelligence in which there are no central coordinators and, thus, agents can setup, on-the-fly, collaborative

learning networks that can dynamically change. We took one step towards this end in [Che+20b] whereby device-to-device links are leveraged to create local FL networks. This prior work can be used as a stepping stone to design a fully distributed FL framework that is closer to swarm AI. Naturally, fully distributed swarm AI can potentially help address many important wireless problems. Those range from spectrum sharing problems among massive number of devices, each owned by different operator, to the optimization of large-scale networks (e.g., swarms of drones, massive deployment of small cells or reconfigurable surfaces, etc.).

- *Complexity, Latency, and Reliability of MARL:* One of the biggest challenges facing the deployment of MARL in real-world wireless networks is the associated complexity in coordinating the agents and enabling them to work together. Indeed, as the number of agent increases, complexity increases significantly since the rewards will now depend on the joint actions of all players and the computational complexity needed to converge to an outcome also increases. In addition, when deployed in wireless networks, issues of latency and reliability come into the picture. For instance, a wireless network cannot afford a slow-to-converge MARL framework (e.g., for managing resources, designing beamforming algorithms, etc.) that cannot react in time to changes in the environment. Meanwhile, when supporting applications such as extended reality or autonomous robotics, it is essential for the wireless system to maintain reliable communication, i.e., connectivity must remain available even when the system suffers extreme events (e.g., a deep fade or a surge in traffic). Existing MARL solutions are not tailored towards such complexity, latency, and reliability requirements and, thus, there is a need for new wireless-tailored MARL designs.

5.5.2 Opportunities and Potential Solutions

- *Distributed and Generalizable Learning:* As already outlined in previous sections, generalizability is quintessential for designing AI solutions that are fit for addressing key problems in wireless networks. Generalizability can, in fact, help address some of the latency and reliability challenges of existing distributed learning techniques (including MARL and FL) by enabling fast out-of-domain, out-of-distribution, or out-of-context generalization. In this regard, remarkably, most of existing FL solutions remain restricted to classical learning tasks that do not exhibit generalizable properties (with a few exceptions that merged FL with domain adaptation [She+22]). Thus, a key open problem here is to investigate the design of FL systems that are both fully distributed and generalizable. Similarly, beyond some works on multi-task MARL, there are very few works that incorporated generalizability with reinforcement learning. In [Hu+21], we studied how meta-learning can be combined with MARL in order to enable generalization across distributions of tasks, within the context of wireless networks serviced by drone base stations (DBSs). As shown in Fig. 5.5, generalizability through meta-learning can significantly reduce the convergence time of the proposed algorithm (called meta-trained value decomposition reinforcement learning, meta-trained VD-RL) compared to several baselines including an independent actor critic (IAC) algorithm. However, this prior work was only limited to meta-learning whose generalizability is limited. In contrast, there is a need for potentially integrating more advanced tools, such as causality and/or neuro-symbolic AI within a MARL

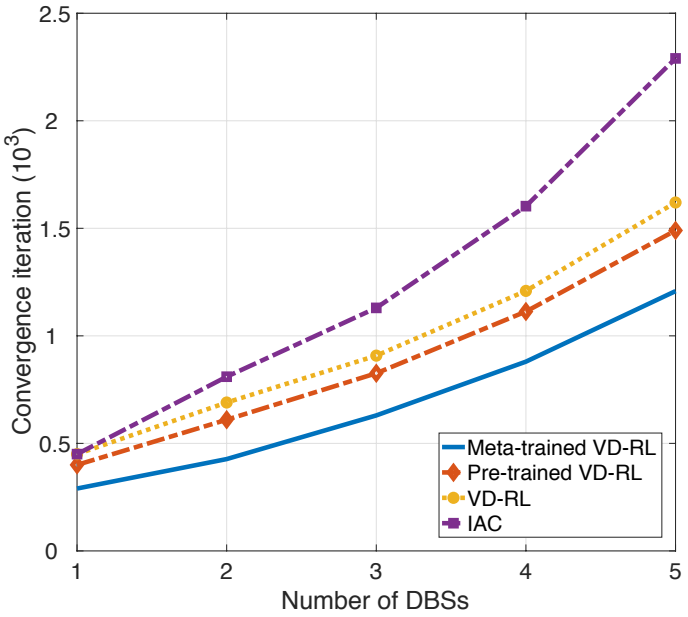


Figure 5.5: Meta-MARL for trajectory design in drone-assisted wireless networks [Hu+21]

framework. Naturally, such a generalizable MARL system will put forward important convergence, optimality, and complexity questions, as already shown in our prior work. In short, for future wireless systems to truly exploit the potential of AI, there is a need for marrying distributed AI frameworks with generalizability concepts.

- *MARL meets FL:* To date, most prior works on MARL or FL in wireless have studied these two frameworks separately. However, a key opportunity, that can pave the way towards true swarm intelligence and that can help address some of the complexity challenges of reinforcement learning, is to combine FL and MARL within a single framework. This can be done in at least two ways. First, one can use a two-step solution in which the FL process is used to train the deep learning architecture of the MARL process. We have explored this solution in [Che+20a], and we showed that it can enhance the quality-of-experience (QoE) of extended reality services, compared to using classical, centralized training of MARL. This early work can be used to build more sophisticated two-step FL and MARL solutions. Second, one can directly design a federated MARL process in which the FL learning task is a reinforcement learning task and not a classification or regression task. This is typically known as federated reinforcement learning (FRL) in the literature, and we have shown in [Abd+22] that it can be used to effectively enable cooperative perception among vehicles. FRL is definitely a fertile area that must be investigated, and its potential application to wireless networks is still under-explored.
- *Distributed, Green AI and Resource Constraints:* Implementing any distributed solution, including FL and MARL, will require computing, energy, and memory resources resources at the devices. In a wireless network, many devices are resource-constrained, and they may not be able to run sophisticated learning architectures or neural networks. Moreover, even at data centers, recent works have shown that AI algorithms may consume significant energy and, thus, there is a need for green AI designs that are sustainable and that can be deployed at real-world edge devices. In this regard,

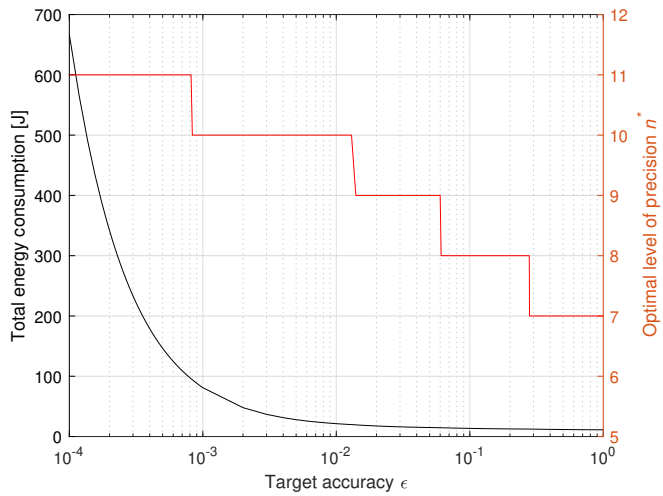


Figure 5.6: On the tradeoff between precision, accuracy, and energy in green FL [Kim+22]

a key opportunity is to investigate the fundamental question of finding an optimal distributed learning architecture (within FL, MARL, or other frameworks) that can not only maximize accuracy, but also minimize energy consumption and resource usage at the end-devices. In [Kim+22], we have taken a first step towards this goal by exploring the use of quantized FL architectures, and we have evaluated the associated tradeoffs between precision, accuracy, and energy. However, quantization alone is not sufficient, and it has its own disadvantages. As shown in Fig. 5.6 from [Kim+22], a higher accuracy level requires larger total energy consumption and more bits for data representation to mitigate the quantization error. However, quantization alone is not sufficient to minimize energy efficiency and resource usage, and other approaches must still be considered. Therefore, this area remains rich in opportunities for future research.

- *Scaling Distributed Learning:* As already mentioned, a key challenge in distributed learning is complexity, when the number of agents increases. This is more pronounced for MARL, but it is also a challenge for FL. In this regard, in order to deploy distributed AI architectures in a real-world wireless system it is necessary to understand how to scale those algorithms to ultra dense networks with massive numbers of devices. Here, tools such as mean-field theory can play a key role in enabling such scalability.

5.6 Conclusions

In this position paper, we have charted a roadmap towards achieving cognition in wireless systems – a target that has been set since nearly a decade ago. In particular, we have studied how next-generation AI frameworks must meet a number of important characteristics that mimic the human brain. These include the need for generalizable intelligence, transferable learning skills, continual learning, and collective intelligence. We have defined each such characteristic and outlined key challenges and opportunities. For example, when it comes to generalizability and transferability, we have investigated how causal learning

and neurosymbolic AI, which constitute key pillars in achieving solid reasoning and generalizability, will play a pivotal role for future wireless systems. We have also discussed the challenges of continual lifelong learning and we highlighted the necessity of efficient AI frameworks in breadth and depth for wireless. Subsequently, we discussed novel concepts from hyper-game theory and self-attention learning. Such concepts open the door for novel opportunities for continual learning in spectrum sharing and IoE services. Then, we outlined the challenges and opportunities surrounding the design of fully distributed collective intelligence in future wireless systems, while expanding upon known frameworks such as FL and MARL. In a nutshell, this position paper laid the necessary foundations for creating truly "cognitive" and AI-native wireless systems.

References

[MM99] J. Mitola and G.Q. Maguire. "Cognitive radio: making software radios more personal". In: *IEEE Personal Communications* 6.4 (Aug. 1999), pages 13–18.

[Hay05] S. Haykin. "Cognitive radio: brain-empowered wireless communications". In: *IEEE J. Select. Areas Commun.* 23.2 (Feb. 2005), pages 201–220.

[Hoy+21] Jakob Hoydis et al. "Toward a 6G AI-native air interface". In: *IEEE Communications Magazine* 59.5 (May 2021), pages 76–81.

[Ayo+18] Sara Ayoubi et al. "Machine learning for cognitive network management". In: *IEEE Communications Magazine* 56.1 (Jan. 2018), pages 158–165.

[OH17] Timothy O'Shea and Jakob Hoydis. "An Introduction to Deep Learning for the Physical Layer". In: *IEEE Transactions on Cognitive Communications and Networking* 3.4 (2017), pages 563–575. DOI: *10.1109/TCCN.2017.2758370*.

[Che+21a] Y. Chen et al. "Reinforcement Learning Meets Wireless Networks: A Layering Perspective". In: *IEEE Internet of Things Journal* 8.1 (Jan. 2021), pages 85–111.

[Zha+21] Y. Zhang et al. "DeepWiPHY: Deep Learning-Based Receiver Design and Dataset for IEEE 802.11ax Systems". In: *IEEE Trans. Wireless Commun.* 20.3 (Mar. 2021), pages 1596–1611.

[YC10] S. Yun and C. Caramanis. "Reinforcement Learning for Link Adaptation in MIMO-OFDM Wireless Systems". In: *Proc. IEEE Global Communication Conference*. Miami, FL, USA, Dec. 2010.

[Cha+22] Christina Chaccour et al. *Less Data, More Knowledge: Building Next Generation Semantic Communication Networks*. Nov. 2022. arXiv: *2211.14343* [cs.AI].

[Sha+19] Haya Shajaiah et al. "Application-Aware Resource Allocation based on Channel Information for Cellular Networks". In: *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*. Marrakesh, Morocco, Apr. 2019, pages 1–6. DOI: *10.1109/WCNC.2019.8885591*.

[Che+19] Mingzhe Chen et al. "Data Correlation-Aware Resource Management in Wireless Virtual Reality (VR): An Echo State Transfer Learning Approach". In: *IEEE Transactions on Communications* 67.6 (Feb. 2019), pages 4267–4280. DOI: *10.1109/TCOMM.2019.2900624*.

[TP18] Punnarumol Temdee and Ramjee Prasad. *Context-aware communication and computing: Applications for smart environment*. Springer, 2018.

[GP07] B. Goertzel and C. Pennachin. *Artificial General Intelligence*. Springer, 2007.

[Kah13] D. Kahneman. *Thinking, Fast and Slow Paperback*. Farrar, Straus and Giroux, 2013.

[VT19] Gido M Van de Ven and Andreas S Tolias. "Three scenarios for continual learning". In: *arXiv preprint arXiv:1904.07734* (2019).

[Ngu+20] Minh NH Nguyen et al. "Self-organizing Democratized Learning: Towards Large-scale Distributed Learning Systems". In: *arXiv preprint arXiv:2007.03278* (2020).

[FAL17] Chelsea Finn, Pieter Abbeel, and Sergey Levine. "Model-agnostic meta-learning for fast adaptation of deep networks". In: *Proc. of International Conference on Machine Learning*. PMLR. 2017, pages 1126–1135.

[Yu+20] Tianhe Yu et al. "Meta-world: A benchmark and evaluation for multi-task and meta reinforcement learning". In: *Conference on robot learning*. PMLR. Osaka, Japan, Nov. 2020, pages 1094–1100.

[Sun+19] Qianru Sun et al. "Meta-transfer learning for few-shot learning". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. Long Beach, CA, June 2019, pages 403–412.

[Kas+20] Ali Taleb Zadeh Kasgari et al. "Experienced deep reinforcement learning with generative adversarial networks (GANs) for model-free ultra reliable low latency communication". In: *IEEE Transactions on Communications* (Oct. 2020).

[TS22] Christo Kurisummoottil Thomas and Walid Saad. "Neuro-Symbolic Causal Reasoning Meets Signaling Game for Emergent Semantic Communications". In: *arXiv preprint arXiv:2210.12040* (2022).

[HCS22] Omar Hashash, Christina Chaccour, and Walid Saad. "Edge Continual Learning for Dynamic Digital Twins over Wireless Networks". In: *Proc. of the 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC)*. Oulu, Finland, June 2022, pages 1–5.

[CL18] Zhiyuan Chen and Bing Liu. "Continual learning and catastrophic forgetting". In: *Lifelong Machine Learning*. Springer, 2018, pages 55–75.

[Han+12] Zhu Han et al. *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge university press, 2012.

[KGL15] Nicholas S Kovach, Alan S Gibson, and Gary B Lamont. "Hypergame theory: a model for conflict, misperception, and deception". In: *Game Theory* 2015 (2015).

[SMP21] Ghada Sokar, Decebal Constantin Mocanu, and Mykola Pechenizkiy. "Self-attention meta-learner for continual learning". In: *arXiv preprint arXiv:2101.12136* (2021).

[WKP21] Haiping Wu, Khimya Khetarpal, and Doina Precup. "Self-supervised attention-aware reinforcement learning". In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Volume 35. 12. Feb. 2021, pages 10311–10319.

[Kon+16] J. Konečnỳ et al. "Federated optimization: Distributed machine learning for on-device intelligence". In: *arXiv preprint arXiv:1610.02527* (2016).

[Che+20a] M. Chen et al. " Federated Echo State Learning for Minimizing Breaks in Presence in Wireless Virtual Reality Networks". In: *IEEE Trans. Wireless Commun.* 19.1 (Jan. 2020), pages 77–191.

[Che+21b] M. Chen et al. "A Joint Learning and Communications Framework for Federated Learning over Wireless Networks". In: *IEEE Trans. Wireless Commun.* 20.1 (Feb. 2021), pages 269–283.

[Yan+21] Z. Yang et al. "Energy Efficient Federated Learning Over Wireless Communication Networks". In: *IEEE Trans. Wireless Commun.* (to appear 2021).

[Che+21c] M. Chen et al. "Convergence Time Optimization for Federated Learning over Wireless Networks". In: *IEEE Trans. Wireless Commun.* (to appear 2021).

[Zho+22] Ruikang Zhong et al. "Mobile reconfigurable intelligent surfaces for NOMA networks: Federated learning approaches". In: *IEEE Transactions on Wireless Communications* 21.11 (June 2022), pages 10020–10034.

[Le+21] Tra Huong Thi Le et al. "An incentive mechanism for federated learning in wireless cellular networks: An auction approach". In: *IEEE Transactions on Wireless Communications* 20.8 (Mar. 2021), pages 4874–4887.

[Don+21] Igor Donevski et al. "Federated learning with a drone orchestrator: Path planning for minimized staleness". In: *IEEE Open Journal of the Communications Society* 2 (Apr. 2021), pages 1000–1014.

[Che+20b] M. Chen et al. "Wireless Communications for Collaborative Federated Learning". In: *IEEE Commun. Mag.* 58.2 (Dec. 2020), pages 48–54.

[She+22] D. Shenaj et al. "Learning Across Domains and Devices: Style-Driven Source-Free Domain Adaptation in Clustered Federated Learning". In: *arXiv:2210.02326* (Oct. 2022).

[Hu+21] Y. Hu et al. "Distributed Multi-agent Meta Learning for Trajectory Design in Wireless Drone Networks". In: *IEEE J. Select. Areas Commun.* (Oct. 2021).

[Abd+22] M. Abdel-Aziz et al. "Vehicular Cooperative Perception Through Action Branching and Federated Reinforcement Learning". In: *IEEE Trans. Commun.* 70.2 (Feb. 2022), pages 891–903.

[Kim+22] M. Kim et al. "On the Tradeoff between Energy, Precision, and Accuracy in Federated Quantized Neural Networks". In: *Proc. Int. Conf. on Communications*. Seoul, South Korea, June 2022.

The Authors

Walid Saad (Fellow, IEEE) (S'07, M'10, SM'15, F'19) received the Ph.D. degree from the University of Oslo in 2010. He is currently a Professor with the Department of Electrical and Computer Engineering, Virginia Tech, where he leads the Network sciEnce, Wireless, and Security (NEWS) Laboratory. He is also the Wireless Next-G Faculty Lead for Virginia Tech's new Innovation Campus. His research interests include wireless networks (5G/6G/beyond), machine learning, game theory, security, unmanned aerial vehicles, semantic communications, cyber-physical systems, and network science. He was the author/coauthor of 11 conference best paper awards at WiOpt in 2009, ICIMP in 2010, IEEE WCNC in 2012, IEEE PIMRC in 2015, IEEE SmartGridComm in 2015, EuCNC in 2017, IEEE GLOBECOM in 2018, IFIP NTMS in 2019, IEEE ICC in 2020 and 2022, and IEEE GLOBECOM in 2020. He was a recipient of the NSF CAREER Award in 2013 and the Young Investigator Award from the Office of Naval Research (ONR) in 2015. He was also a recipient of the 2015 and 2022 Fred W. Ellersick Prize from the IEEE Communications Society, the 2017 IEEE ComSoc Best Young Professional in Academia Award, the 2018 IEEE ComSoc Radio Communications Committee Early Achievement Award, and the 2019 IEEE ComSoc Communication Theory Technical Committee. He was also the coauthor of the 2019 IEEE Communications Society Young Author Best Paper and the 2021 IEEE Communications Society Young Author Best Paper. From 2015 to 2017, he was named the Stephen O. Lane Junior Faculty Fellow at Virginia Tech and, in 2017, he was named the College of Engineering Faculty Fellow. He received the Dean's Award for Research Excellence from Virginia Tech in 2019. He was also an IEEE Distinguished Lecturer in 2019 and 2020. He currently serves as an Editor for the IEEE Transactions on Mobile Computing and the IEEE Transactions on Cognitive Communications and Networking. He is an Area Editor of the IEEE Transactions on Network Science and Engineering, and an Editor for several major IEEE Transactions. He is the Editor-in-Chief of the IEEE Transactions on Machine Learning in Communications and Networking.

The Authors

Christina Chaccour (Graduate Student Member, IEEE) (S'17) received the B.E. degree (Summa Cum Laude) in Electrical Engineering from Notre Dame University-Louaize, Lebanon, in 2018 and the M.S. degree in Electrical Engineering from Virginia Tech, Blacksburg, VA, USA, in 2020. She is currently pursuing the Ph.D. degree with the Bradley Department of Electrical and Computer Engineering, Virginia Tech, where her research interests include wireless communications, 5G and 6G networks, extended reality, terahertz frequency bands, machine learning, and semantic communications. She has derived some of the first performance analysis results on the potential of networking at THz frequencies. Christina is the co-founder of the startup Internet of Trees (IOTree); IOTree has won many local and international awards. She has held summer internship positions at Ericsson Inc., Plano, TX, USA, and Cadence Design Systems, Munich GmBh. She was the recipient of the Best Paper Award for her peer-reviewed conference paper at the 10th IFIP Conference on New Technologies, Mobility, and Security (NTMS), Canary Islands, in 2019. Her paper in IEEE Communication Surveys and Tutorials was featured on the Top Access article listing from June 2022, till October 2022. Additionally, Christina was the recipient of the exemplary reviewer (fewer than 2%) award from IEEE Transactions on Communications in 2021. She has also served as a reviewer and a technical program committee member for various IEEE transactions and flagship conferences.

6. Thoughts of Prof. Yalin Sagduyu

NextG Communications Security through the Lens of Adversarial Machine Learning

Author: Prof. Yalin E. Sagduyu,
Virginia Tech National Security Institute
Arlington, VA 22203, USA,
ysagduyu@vt.edu

Machine learning (ML) has been instrumental in advancing the design and optimization of wireless communication systems. However, ML is vulnerable to attacks. Smart adversaries can manipulate the ML engines in training and test times, and disrupt the performance of wireless systems. Therefore, adversarial machine learning (AML) has emerged as a major security concern for NextG communications systems. This paper reviews the AML attacks and defense mechanisms, discusses the unique properties, challenges and opportunities of the AML attacks in the wireless domain, and points at security vulnerabilities of ML-driven NextG communications systems to the AML attacks.

6.1 Introduction

Machine learning (ML) has been considered a key enabler for *next-generation (NextG) communications systems* to push the performance limits [**Erpek2019**; **Letaief2019**]. Supported by advances in algorithmic capabilities, computational resources, open source software libraries, and data generation and sharing efforts, deep learning (DL) has emerged as a powerful solution to solve complex problems in wireless communications that have not been feasible before by analytical and conventional ML approaches. To that end, deep neural networks (DNNs) can effectively learn from the high-dimensional and dynamic spectrum data and optimize the communication functionalities to keep up with the ever-growing performance demands such as high rate, low latency, and energy-efficiency.

One key question is whether we can trust ML. This question can be decomposed to further questions: Can we explain and account for how ML makes decisions? How robust is ML as data characteristics may change from training time to test time? Can we repeat or reproduce ML results? How do the ML decisions depend on uncertainties in wireless systems regarding channel, traffic, interference, and hardware impairment effects? Can we trust edge devices to perform ML? What are the security vulnerabilities of ML when adopted in wireless communications? This paper will take a deep dive into the final question regarding the new attack surface due to the growing use of ML in wireless systems.

Learning in the presence of adversaries is studied *under adversarial machine learning* (AML) [**Goodfellow2015**; **Vorobeychik2018**; **Szegedy2013**]. As a canonical example of an AML attack borrowed from the computer vision domain, consider an API that classifies images to labels such as panda or gibbon. High classification accuracy can be achieved by proper training of a DNN with suitable data. As a stealthy attack, the adversary can add a small perturbation (that cannot be detected by visual detection) to the pixels of a panda image before sending it to the classifier. Then, the classifier is fooled into classifying this perturbed image as gibbon.

While the DNNs can capture the intrinsic properties of wireless communications (such as waveform, channel, interference, traffic, and hardware effects), the complex decision space of the DNNs is highly sensitive to even small variations in inputs. Therefore, the DNNs used in wireless system are vulnerable to attacks, where smart adversaries tamper with the training and/or test (inference) time operations of the DNNs and fool them into making errors in their decisions [**Sagduyu2020**; **Adesina2022**; **Liu2022**]. In training time, the adversaries can manipulate the training data and prevent the DNN models from being trained properly such that they cannot perform well later in test time. In test time, the adversaries can manipulate the input samples such that the DNN models make wrong decisions.

This paper discusses the applications of the AML attacks to the wireless domain in terms of their unique properties, opportunities, and challenges including over-the-air attacks, channel effects, broadcast transmissions, synchronization effects, multiple antennas, and vulnerabilities due to open-source development of radio access network (RAN) architectures. Various vulnerabilities of the NextG communications systems are presented by discussing the AML attacks on wireless signal classification, spectrum sharing, initial access,

power control, MIMO, end-to-end autoencoder communications, and network slicing.

The remainder of the paper is organized as follows. Section 6.2 presents a general overview of the AML attacks. Section 6.3 discusses defense mechanisms against AML the attacks. Section 6.4 describes the properties, opportunities and challenges of the AML attacks in the wireless domain. Section 6.5 discusses the AML attacks on different components of NextG communications. Section 6.6 concludes the paper.

6.2 Adversarial Machine Learning Attacks

This section reviews various ways to launch attacks built upon AML.

- *Inference (exploratory)* attacks seek to learn how the victim ML algorithm functions. By observing the input-output relationships (or their noisy variants), the adversary builds a surrogate model to mimic the victim model behavior, as depicted in Fig. 6.2. This surrogate model can be used to launch subsequent attacks (such as brute-force jamming or other AML attacks) on the victim model. One challenge is that the adversary may need a large number of samples to train a high-fidelity surrogate model. This may not be possible or it may take long to collect these samples delaying the start of the attack. Therefore, the adversary can augment the training data, e.g., by generating synthetic samples with *generative adversarial networks (GANs)*. The adversary can also pursue *active learning* to reduce the number of training samples needed. For that purpose, the adversary repeatedly collects training samples based on the trained surrogate model and then updates the surrogate model with new samples to improve it over time.

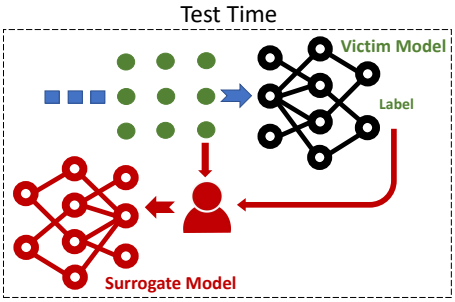


Figure 6.1: Inference (exploratory) attack.

- In test time, *adversarial (evasion) attacks* seek to manipulate the input samples of the victim model (e.g., by adding a small perturbation) such that it cannot make a reliable decision for these samples, as illustrated in Fig. 6.2. The effect of this attack is measured by the model accuracy for the manipulated input samples (the lower accuracy indicates a more effective attack). The perturbation is selected by minimizing the perturbation strength subject to the condition that an error occurs in the decision of the victim model. Since solving this optimization problem is difficult, Fast Gradient Method (FGM) can be applied by linearizing the loss function and using the gradient of the loss function when crafting the perturbation. Other attack methods include Fast Gradient Sign Method (FGSM), Basic Iterative Method (BIM), Projected Gradient

Descent (PGD), Momentum Iterative Method, DeepFool, and Carlini Wagner (C&W).

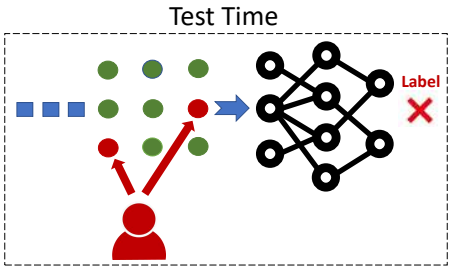


Figure 6.2: Adversarial (evasion) attack.

- In training time, *poisoning (causative) attacks* seek to manipulate the training data of the adversary, namely, modify some of the features and labels, as illustrated in Fig. 6.3. When trained with the poisoned samples, the fidelity of the DNN model would drop for all input samples in test time. When selecting which samples to poison, the goal is to maximize the impact on the decision space of the trained DNN. The larger decrease in the accuracy of the trained model indicates a more effective attack.

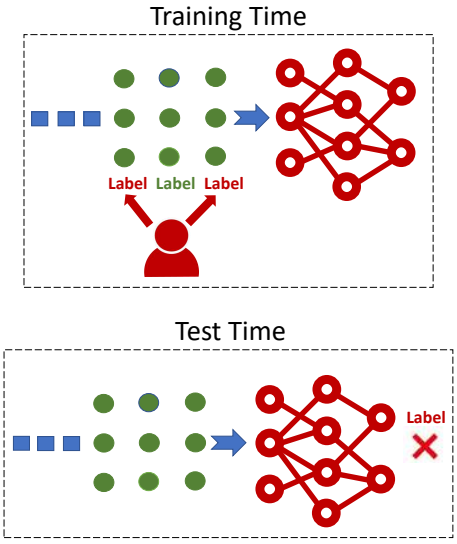


Figure 6.3: Poisoning (causative) attack.

- *Backdoor (Trojan) attacks* take place in both training and test times, as shown in Fig. 6.1. The adversary inserts insert triggers to some training samples in training time and then activate them in test time such that the poisoned model makes errors in test time only for selected input samples that are poisoned with the same triggers. The effect of this attack is measured by (i) the model accuracy for poisoned test input samples (the lower accuracy indicates that the attack is more effective) and (ii) the model accuracy for unpoisoned test input samples (the higher accuracy indicates that the attack is stealthier).

For stealthy attacks, it is necessary to impose *realistic constraints on the attack vectors*. For

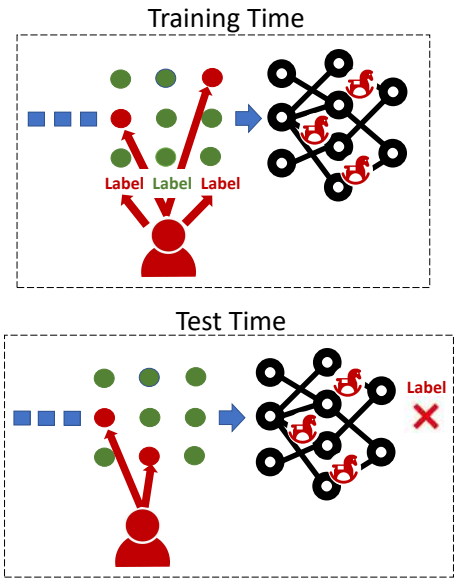


Figure 6.4: Backdoor (Trojan) attack.

example, an upper bound on the perturbation strength can be imposed for adversarial attacks. In the wireless domain, the perturbation strength is expressed as the perturbation-to-noise ratio (PNR) that measures the perturbation strength relative to the noise power [**Sadeghi2018**]. The smaller the PNR is, the stealthier and more energy-efficient the attack is. For poisoning and backdoor attacks, an upper bound is imposed on the number of poisoned samples such that the smaller number indicates that the attack is stealthier [**Sagduyu2019**; **Davaslioglu2019**].

With AML, it is possible to launch *targeted and non-targeted attacks*. The targeted adversarial attacks aim to cause errors only for input samples from a specific set of classes by minimizing the loss function of the victim DNN with respect to the target class. The non-targeted adversarial attacks aim to cause errors for all input samples by maximizing the loss function of the victim DNN for all classes.

The AML attacks can be launched in *black-box* or *white-box* settings. In white-box attacks, the adversary knows the model and/or the training data. To relax this assumption for a black-box attack, the adversary can build a surrogate model and use it (instead of the unknown victim model) for subsequent attacks. In a *membership inference attack*, the adversary can also infer whether a sample has been used in the training data of the victim model [**Shi2020**; **Shi2022**].

If the adversary does not know the test samples for the adversarial attack, it needs to build a *universal adversarial perturbation (UAP)* that is agnostic to test samples [**Moosavi-Dezfooli**]. The UAP can be built by first generating attack vectors for different (potential) input samples and then reduce their dimension (e.g., by autoencoder and principal component analysis (PCA)) to a common attack vector that can be used against different (unknown) input samples [**Sadeghi2018**].

The goal of the AML attack depends on the victim model. The AML attack on a DNN (such

as feedforward, convolutional and recurrent neural networks) seeks to reduce its accuracy, The AML attack on reinforcement learning (RL) also seeks to increase the convergence time for RL [**Shi2021**; **Wang2022**; **Shi2022-2**; **Shi2021-2**].

6.3 Defense against Adversarial Machine Learning Attacks

The AML attacks can be counteracted by *proactive* and *reactive defenses*. The victim model can be made more robust against adversarial perturbations by different proactive defenses:

- *Gradient masking* (gradient obfuscation) prevents the victim model from having useful gradients (that may be exploited by the adversaries) by using a simple classifier instead of a DNN [**Papernot2017**].
- *Distillation* trains the DNN by using the knowledge extracted from a DNN to improve its own resilience to adversarial samples [**Papernot2016**].
- *Adversarial training* creates adversarial examples and incorporates them into the training process by anticipating perturbations added to the input samples in test time [**Madry2017**].
- *Randomized smoothing* augments the training data by adding noise samples to data and makes the DNN robust to adversarial perturbations in test time [**Cohen2019**].
- *Certified defense* guarantees the model robustness against adversarial attacks by augmenting the received signals with Gaussian noise samples in test time and checking statistical significance of model decisions [**Raghunathan2018**].

Beyond the proactive defenses, a *reactive defense* seeks to detect attacks [**Metzen2017**; **Lee2018**]. For that purpose, the DNN can be augmented with a small detector subnetwork that is trained to detect data samples with adversarial perturbations.

Since many AML attacks start with an inference attack that builds a surrogate model, a defense mechanism is to increase the adversary's *uncertainty* by introducing controlled errors in victim model decisions. These errors poison the training data of the adversary and prevents it from building a reliable surrogate model. However, this defense also reduces the model performance in the absence of an attack. Therefore, the defender may prefer to apply the defense not all the time. There is also an incentive for the adversary not to launch an attack all the time because the attack is more effective in the absence of a defense and there is a cost of launching an attack (for training data collection and surrogate model training). These interactions can be formulated as a *non-cooperative game*, where the attack and defense mechanisms select their randomized strategies. The, the *Nash equilibrium* strategies correspond to operation modes such that the attacker or the defender cannot unilaterally improve its utility given the other's strategy is fixed [**Sagduyu2022**].

6.4 Properties, Opportunities, and Challenges of Adversarial Machine Learning in the Wireless Domain

There are unique properties, opportunities and challenges in the wireless domain that the adversary needs to consider when launching the AML attacks. Fig. 6.5 illustrates how adversarial attacks depend on channel effects, broadcast transmissions, and potential use

of multi-antenna configurations in wireless systems.

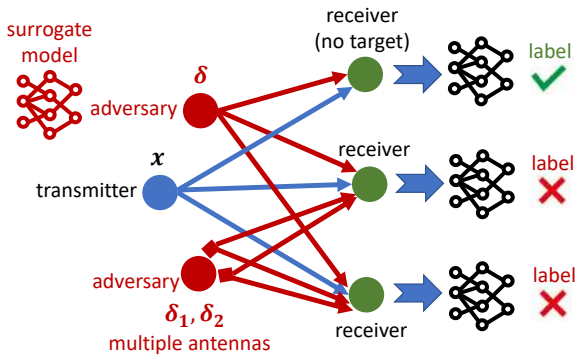


Figure 6.5: Wireless properties in the context of adversarial attacks.

- *Over-the-air attacks and channel effects*: As a wireless transmitter, the adversary cannot directly manipulate the sample inputs to the victim model that resides at another receiver. The adversary needs to consider channel effects when launching an AML attack. For an adversarial attack, the adversary needs to determine the perturbation to be transmitted by accounting for the channel effects that the perturbation and victim signals will individually experience when reaching the receiver [**Kim2022**; **Kim2020**]. This attack is selective in the sense that the perturbation designed for a particular channel is only effective against the receiver that experiences this particular channel and not effective against other receivers with different channels.
  This channel-aware attack paradigm is different from attacks in different data domains (e.g., computer vision or NLP) where the adversary can directly query the victim models and directly manipulate their inputs. Adversarial attacks are known to be transferrable, i.e., attacks trained against one model may be effective against other (potentially unknown) models [**Papernot2016-2**]. However, the discrepancy between the surrogate model and the victim model may render the transferred attacks ineffective. In an inference attack for a wireless system, the adversary can overhear the transmissions that follow from the victim model's decisions and builds the surrogate model without directly querying the victim model. However, this surrogate model may differ from the victim model significantly because the adversary and the receiver (where the victim model resides experience) different channels and their models are trained with different distributions of inputs [**Kim2021**].
- *Broadcast transmissions*: Wireless signals can be broadcast with omnidirectional transmissions. Therefore, the adversary can reach and manipulate multiple models at different receivers with a single transmission of a common perturbation. This paradigm is different from other data domains where the adversary needs to attack each victim model (e.g., at different APIs) separately. This broadcast property can be exploited by the adversary to reduce the time and energy spent for the attack on multiple models. The broadcast attack can generate perturbations for DNN models at different receivers and then combine them to a common attack vector [**Kim2022**]. Alternatively, the adversary can extend the underlying optimization problem to select a common perturbation for all receivers.

- *Synchronization effects:* The perturbation transmitted by the adversary s not necessarily aligned in time with the transmission of the victim transmitter. Since the adversary is not typically synchronized with the victim transmitter, there is a shift between the transmitter and perturbation signals. To that end, a shift-invariant perturbation should be generated by accounting for potential synchronization effects [**Sadeghi2018**].
- *MIMO communications:* Both the adversary and the receiver with the victim model may use multiple antennas. By using multiple transmit antennas, the adversary has more degrees of freedom to determine different perturbations for different antennas. The superpositions of these perturbations are received at potentially multiple antennas of the receiver. Therefore, the adversary needs to consider both the power allocation among antennas and the utilization of channel diversity when crafting adversarial perturbations [**Kim2022-2**; **Kim2020-2**]. For a similar effect, multiple adversaries at different locations, each with a single antenna, can transmit perturbations that are induced by channel effects and superimposed at the receiver. This way, they can jointly build a perturbation that is more effective than what a single adversary can achieve. The input size of the victim model increases with the number of receive antennas. As this property increases the complexity of the victim model, the adversary needs to adapt its attack to a more difficult setting while exploiting multiple entries of the attack surface.
- *Open Nature of NextG Software Development:* Open source software development has been a catalyst for fast and collaborative progress of 5G and beyond RAN technologies. O-RAN provides an open RAN architecture with virtualized network elements and interfaces. Various RF applications of ML can be implemented as xApps in the *near real-time RAN intelligence controller* (Near-RT RIC) of O-RAN. These xApps can be offered in a market place and adopted as part of RAN development efforts. An adversary can exploit the openness of the software development in various forms. First, it can get access to the training data or the trained model through the xAPP for a NextG application. Then, it can train a reliable surrogate model to construct adversarial attacks on NextG communications systems that utilize this particular xApps. Second, the adversary itself may be the one offering the xApp that is built upon the training data samples or trained models poisoned with backdoors. Then, it is possible to fool the ML engine of a NextG communication task by activating the triggers for selected input samples in test time.
- *Defense Mechanisms against the AML Attacks in the Wireless Domain:* The DNNs used for wireless applications can be made more robust against the AML attacks by proactive defense methods such as randomized smoothing [**Kim2022**], certified defense [**Kim2022**], and adversarial training [**McClintick2022**]. In addition, frequency domain features [**Sahay2021**] and forward error correction codes [**DelVecchio2020**] can be used to mitigate the effects of adversarial attacks. On the other hand, reactive methods based on statistical outlier detection can be applied to detect the adversarial perturbations and triggers in test time [**Davaslioglu2019**; **Filipovic2019**].

6.5 Vulnerabilities of NextG Communications to Adversarial Machine Learning

6.5.1 Attacks on Wireless Signal Classification

One prominent application of DL in the wireless domain is the classification of wireless signals that needs to capture waveform, channel and radio hardware effects jointly. Over-the-air received signals need to be classified for various purposes including spectrum sensing, waveform recognition (e.g., modulation classification), device identification, user equipment (UE) authentication, RF fingerprinting, and mobile crowdsensing. Various *adversarial attacks* have been considered against wireless signal classifiers [**Sadeghi2018**; **Kim2022**; **Kim2020**; **McClintick2022**; **Sahay2021**; **DelVecchio2020**; **Filipovic2019**; **Lin2020**; **Bahramali2021**]. These attacks can be launched by transmitting perturbations over the air and interfering with the transmitted signals to fool the wireless signal classifier into returning wrong labels based on the received signals. On the other hand, *backdoor attacks* can be launched by adding specific phase shifts as triggers in the training data of the wireless signal classifier. In test time, the adversaries can transmit signals with these specific phase shifts and deceive the wireless signal classifier only for the selected input samples (e.g., for infiltration of an authentication system) [**Davaslioglu2019**].

As an example, consider a targeted adversarial attack on a wireless signal classifier. A transmitter transmits signals modulated with BPSK or QPSK over an additive white Gaussian noise channel with 5dB signal-to-noise ratio. A DNN at the receiver classifies the received signals to BPSK and QPSK. The input consists of 16 I/Q samples and the DNN consists of dense layers of size 128, 32, 8, and 2 (with ReLU activation) separated by dropout layers (with dropout rate 0.2) and followed by the output layer (with SoftMax activation). An adversary seeks to change the DNN's output labels to QPSK for the BPSK-modulated signals by transmitting perturbations generated by FGSM. Fig. 6.6 shows that the adversarial attack reduces the classifier accuracy significantly and the FGSM-generated perturbation is much more effective than Gaussian noise.

6.5.2 Attacks on Spectrum Sharing

For efficient utilization of the spectrum, NextG communications systems are envisioned to share the spectrum with the incumbent (high-priority) users. One example is the 3.5GHz Citizens Broadband Radio Service (CBRS) band that has been reserved for the incumbent user such as radar and recently opened to the use of commercial systems. To prevent harmful interference to the incumbent user, the Environmental Sensing Capability (ESC) sensors need to detect the incumbent signals. Then, the Spectrum Access System (SAS) reconfigures the NextG network to prevent harmful interference to the incumbent users. By monitoring the spectrum, the adversary can launch an *inference attack* to build a surrogate model based on its sensing results to predict when a successful NextG transmissions will occur. Then, the adversary can effectively *jam* these NextG transmissions [**Shi2018**; **Erpek2019-2**; **Sagduyu2021**]. In case of *cooperative spectrum sensing*, spectrum sensors can falsify their spectrum sensing results when reporting them to the fusion center in form of a *poisoning attack* [**Luo2022**]. Spectrum sensing can be also performed by *federated learning* (FL) [**Shi2022-3**]. In a wireless setting, FL is subject to selfish (free-riding) clients that may refrain from participating in model updates due to transmission costs [**Sagduyu2022-2**]. In

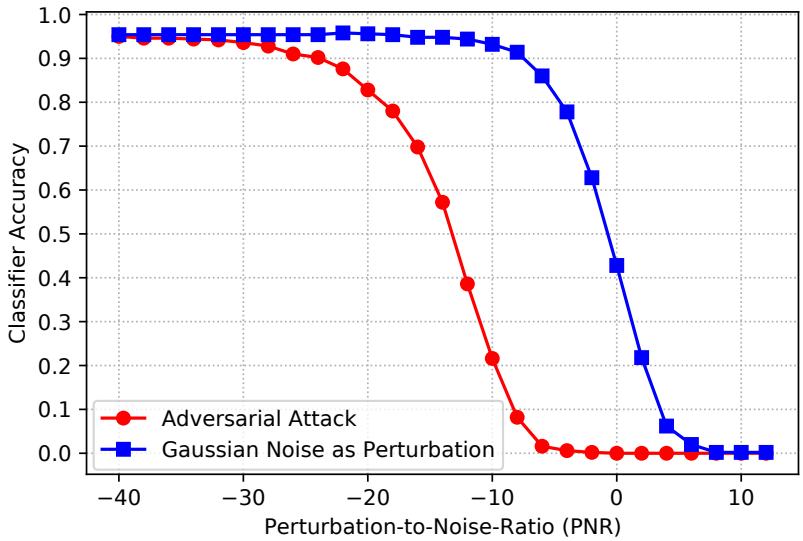


Figure 6.6: Adversarial attack on wireless signal classification.

addition, the adversary can attack FL by jamming model updates exchanged between the server and the clients. For that purpose, the adversary selects which clients to attack in order to reduce the global server accuracy [**Shi2022-4**; **Shi2022-5**].

Beyond brute-force jamming of data transmissions, the adversary can also falsify the spectrum sensing data over the air by transmitting during the spectrum sensing period [**Sagduyu2019**]. If the sensing results are used as test data to make NextG transmit decisions, the adversary fools the NextG system into making incorrect decisions in detecting the incumbent signal (*adversarial attack*). If the sensing results are used as training data to retrain the DNN for spectrum sensing over time, the DNN for spectrum sensing is retrained incorrectly for future decisions (*poisoning attack*). As an outcome of these attacks, either a false alarm occurs, namely the performance of NextG communications drops due to the transmission opportunities, or a misdetection occurs, namely harmful interference is created for the incumbent user. These attacks with low spectrum footprint are hard to detect and energy-efficient as they do not directly jam data transmissions but make low-power transmissions during sensing time.

6.5.3 Attacks to Facilitate Covert Communications

Adversarial attacks can be utilized to hide wireless communications from an eavesdropper that can employ a DNN classifier to detect transmissions of interest. For *covert communications*, a transmitter can add a perturbation to its own signal before transmitting it over the air to its receiver [**Hameed2021**]. This perturbation is carefully selected to be effective with respect to the channel from the transmitter to the adversary but does not significantly impact the communications performance, e.g., the bit error rate, experienced over the channel from the transmitter to the receiver. Instead of adding the perturbation directly to

the transmitted signal, a *cooperative jammer* that is physically distant from the transmitter can transmit adversarial perturbations over the air to fool the eavesdropper into classifying the received superposition of (transmitter and perturbation) signals as noise. [**Kim2022-3**; **Kim2022-4**; **Kim2022-5**]. Multiple cooperative jammers can also coordinate with each other and transmit perturbations that are superimposed at the receiver to boost the adversarial attack against eavesdropping.

6.5.4 Attacks on Initial Access

Operation at high frequencies such as mmWave and THz is ultimately needed for NextG communication systems to achieve high data rates over wider frequency bands. However, this paradigm rises the need for communications with narrow directional beams. When a UE connects to the network for the first time, it needs to establish the *initial access* with the base station. For that purpose, the base station transmits pilot signals with different narrow beams and the UE computes the received signal strengths for all beams and finds the most suitable beam. Since sweeping all beams takes long, a DNN can be trained to predict the beam that is best slanted to each UE by using the received signal strengths from a smaller set of possible narrow beams. As an attack on the DNN for initial access, an adversary can generate adversarial perturbations and transmit them over the air during the initial access. This way, the adversary manipulates the received signal strengths and consequently the inputs to the DNN used for beam prediction. This over-the-air attack can reduce the initial access performance significantly by fooling the DNN into choosing the beams with small RSSs [**Kim2021-2**].

6.5.5 Attacks on Power Control

Transmit resources need to be allocated by the NextG base stations to optimize the communication performance of the UEs. For example, to optimize the achievable rates, the base station allocates transmit power to multiple subcarriers to serve multiple UEs. DL provides a low-complexity solution to solve the underlying non-convex optimization problem by training a regression model that takes channel gains as the input and returns the allocated transmit powers as the output. This model for *power control* is vulnerable to adversarial attacks that aim to minimize the total rate achieved across all UEs. The adversary may be an external transmitter that transmits an adversarial perturbation and interferes with the pilot signals transmitted to measure the channel. Or, the adversary may be a rogue user equipment that sends falsified channel gains (with perturbations added) to the base station. In both cases, the adversary manipulates the inputs to the DNN used for power allocation. These attacks can effectively reduce the rate of communications while remaining robust to the uncertainty at the adversary regarding channel gains [**Kim2021-3**].

6.5.6 Attacks on MIMO Communications

Another way of using DL for power control is for *multi-cell massive MIMO communications*. A regression model can be trained to maximize the aggregate performance, such as the product of signal-to-interference-and-noise ratios, across all users [**Sanguinetti2018**]. The input to the DNN consists of the geographical positions of the UEs. The output is the

set of transmit powers allocated to the UEs. The training data is obtained by solving the optimization problem with conventional high-complexity methods. To attack this DNN, the rogue UEs manipulate the inputs to the trained model by falsifying their reported location. This attack is effective in making the power control solution infeasible such that the power constraints are violated [**Manoj2021**].

6.5.7 Attacks on End-to-End Autoencoder Communications

In addition to optimizing various transmitter and receiver operations, DL can be used for the clean-slate design of the transmitter-receiver chain, e.g., communication blocks can be modeled as an *autoencoder* system. The modulation and coding operations at the transmitter are modeled as an encoder, whereas the demodulation and decoding operations at the receiver are modeled as a decoder. The encoder maps to the input symbols to modulated signals. These signals are transmitter over a wireless channel and then mapped by the decoder to reconstructed the symbols. This encoder-decoder pair is jointly trained to minimize the error rate by accounting for the channel effects. This approach improves the end-to-end performance compared to conventional communication schemes [**Erpek2019**]. An adversary can jam the transmission to increase the error rate at the expense of using high power budget. On the other hand, the adversary can launch an adversarial attack on the autoencoder communications system by transmitting carefully-crafted small perturbations to interfere with the signals received by the decoder. This way, the adversary can manipulate the input of the decoder and prevent the reliable reconstruction of the symbols [**Sadeghi2019**].

6.5.8 Attacks on Radio Access Network Slicing

5G has introduced the *RAN slicing* capability that multiplexes and serves multiple virtualized and independent logical networks on the same physical network to secure and prioritize different services. The static allocation of communication and computation resources is replaced by reserving them on the fly to match the dynamic user demand in terms of quality of experience (QoE) requirements such as high rate and low delay. The admission control and resource allocation for network slices can be practically implemented in Near-RT RIC of O-RAN. The underlying optimization problem is complex since available resources and demands change over time and coupled. Instead of training a static model to make admission control and resource allocation decisions, RL can be used as a model-less approach, where the reward is the weighted number of accepted requests (weights correspond to priorities of network slices), the states are the available resources, and the actions are to admit or reject slicing requests and to allocate the necessary resources [**Shi2020-2**].

While RL is effective in maximizing the reward compared to myopic or random decision schemes, it is also susceptible to attacks. For that purpose, an adversary can jam the resource blocks. However, this jamming does not need to be brute-force and does not have the sole objective of making transmissions fail. Instead, the objective is to fool the learning process over time by manipulating the reward so that RL deviates from its ideal operation and cannot recover for a while even after a short episode of jamming ends [**Shi2021**; **Wang2022**; **Shi2022-2**]. Again, the first step is to build a surrogate model. To that end, it is also possible

to utilize inverse RL to identify the reward and other structural components of the RL mechanism by probing the execution traces. Another attack on RAN slicing is the *flooding attack*, where an adversary generates fake network slicing requests to consume the RAN resources that would be otherwise available to real requests of network slices. By using its surrogate model, the adversary decides on how to craft fake requests to minimize the reward of real requests over time. This attack can significantly reduce the portion of the reward achieved by real requests [**Shi2021-2**].

6.6 Conclusions

As ML finds more applications in NextG communications systems, the attack surface expands due to the AML attacks that target the ML engines. First, the AML attacks in test and training times, and the corresponding defenses were described. Then, the unique properties, opportunities and challenges were presented for the AML attacks when applied to the wireless domain. Finally, the vulnerabilities of NextG communications systems to the AML attacks were discussed. As wireless communications systems rely more on ML to perform difficult tasks, this strong reliance opens the door to novel attacks by the adversaries that exploit the vulnerabilities of ML engines in NextG communication systems. Therefore, it is imperative to pay more attention to the characterization of this emerging attack surface and design mechanisms to protect NextG communications against the AML attacks.

Bibliography

[Erpek2019] T. Erpek, T. O'Shea, Y. E. Sagduyu, Y. Shi, and T. C. Clancy, "Deep Learning for Wireless Communications," *Development and Analysis of Deep Learning Architectures, Springer*, 2019.

[Letaief2019] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, Y.A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks." *IEEE Communications Magazine*, Aug. 2019.

[Goodfellow2015] I. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples." *International Conference on Learning Representations (ICLR)*, 2015.

[Vorobeychik2018] Y. Vorobeychik and M. Kantarcioglu, "Adversarial Machine Learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, Aug. 2018.

[Szegedy2013] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, and I. Goodfellow, and R. Fergus, "Intriguing Properties of Neural Networks," *arXiv preprint arXiv:1312.6199*, 2013.

[Sagduyu2020] Y. E. Sagduyu, Y. Shi, T. Erpek, W. Headley, B. Flowers, G. Stantchev, and Z. Lu, "When Wireless Security Meets Machine Learning: Motivation, Challenges, and Research Directions," *arXiv preprint* arXiv:2001.08883, 2020.

[Adesina2022] D. Adesina, C-C Hsieh, Y. E. Sagduyu, and L. Qian, "Adversarial Machine Learning in Wireless Communications using RF Data: A Review," *IEEE Communications Surveys & Tutorials*, 2022.

[Liu2022] J. Liu, M. Nogueira, J. Fernandes and B. Kantarci, "Adversarial Machine Learning: A Multilayer Review of the State-of-the-Art and Challenges for Wireless and Mobile Systems," *IEEE Communications Surveys & Tutorials*, 2022.

[Sadeghi2018] M. Sadeghi and E. G. Larsson, "Adversarial Attacks on Deep-learning Based Radio Signal Classification," *IEEE Wireless Communications Letters*, Feb. 2019.

[Sagduyu2019] Y. E. Sagduyu, Y. Shi, and T. Erpek, "Adversarial Deep Learning for Over-the-Air Spectrum Poisoning Attacks," *IEEE Transactions on Mobile Computing*, 2019.

[Davaslioglu2019] K. Davaslioglu and Y. E. Sagduyu, "Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning," *IEEE Workshop on Data-Driven Dynamic Spectrum Sharing of IEEE DySPAN*, 2019.

[Shi2020] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Over-the-Air Membership Inference Attacks as Privacy Threats for Deep Learning-based Wireless Signal Classifiers," *ACM Workshop on Wireless Security and Machine Learning (WiseML)*, 2020.

[Shi2022] Y. Shi and Y. E. Sagduyu, "Membership Inference Attack and Defense for Wireless Signal Classifiers with Deep Learning," *IEEE Transactions on Mobile Computing*, 2022.

[Moosavi-Dezfooli] S-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, "Universal Adversarial Perturbations," *IEEE Conference on Computer Vision and Pattern Recognition*, 2017.

[Shi2021] Y. Shi, Y. E. Sagduyu, T. Erpek, M. C. Gursoy, "How to Attack and Defend NextG Radio Access Network Slicing with Reinforcement Learning," *arXiv preprint* arXiv:2101.05768, 2021.

[Wang2022] F. Wang, M. C. Gursoy, S. Velipasalar, and Y. E. Sagduyu, "'"Robust Deep Reinforcement Learning Based Network Slicing Under Adversarial Jamming Attacks," *IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2022.

[Shi2022-2] Y. Shi and Y. E. Sagduyu, T. Erpek, and M. C. Gursoy, "Jamming Attacks on NextG Radio Access Network Slicing with Reinforcement Learning," *IEEE Future Networks World Forum (FNWF)*, 2022.

[Shi2021-2] Y. Shi and Y. E. Sagduyu, "Adversarial Machine Learning for Flooding Attacks on 5G Radio Access Network Slicing," *IEEE International Conference on Communications (ICC) Workshops*, 2021.

[Papernot2017] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical Black-Box Attacks against Machine Learning," *ACM on Asia Conference on Computer and Communications Security (ASIA CCS)*, 2017.

[Papernot2016] N. Papernot, P. McDaniel, X. Wu, S. Jha and A. Swami, "Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks," *IEEE Symposium on Security and Privacy (SP)*, 2016.

[Madry2017] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," *arXiv preprint* arXiv:1706.06083, 2017.

[Cohen2019] J. M. Cohen, E. Rosenfeld, and Z. Kolter, "Certified Adversarial Robustness via Randomized Smoothing," *International Conference on Machine Learning*, 2019.

[Raghunathan2018] A. Raghunathan, J. Steinhardt, and P. Liang, "Certified Defenses against Adversarial Examples," *arXiv preprint* arXiv:1801.09344, 2018.

[Metzen2017] J. H. Metzen, T. Genewein, V. Fischer, and B. Bischoff, "On Detecting Adversarial Perturbations," *arXiv preprint* arXiv:1702.04267, 2017.

[Lee2018] K. Lee, K. Lee, H. Lee, and J. Shin, "A Simple Unified Framework for Detecting Out-of-distribution Samples and Adversarial Attack," *Advances in Neural Information Processing Systems*, 2018.

[Sagduyu2022] Y. E. Sagduyu, "Adversarial Machine Learning and Defense Game for NextG Signal Classification with Deep Learning," *IEEE Military Communications Conference (MILCOM) Workshops*, 2022.

[Kim2022] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers," *IEEE Transactions on Wireless Communications*, 2022.

[Kim2020] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Over-the-Air Adversarial Attacks on Deep Learning Based Modulation Classifier over Wireless Channels," *Conference on Information Sciences and Systems (CISS)*, 2020.

[Papernot2016-2] N. Papernot, P. McDaniel, and I. Goodfellow, "Transferability in Machine Learning: From Phenomena to Blackbox Attacks using Adversarial Samples," *arXiv preprint* arXiv:1605.07277, 2016.

[Kim2021] B. Kim, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, and S. Ulukus, "Channel Effects on Surrogate Models of Adversarial Attacks against Wireless Signal Classifiers," *IEEE International Conference on Communications (ICC)*, 2021.

[Kim2022-2] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Adversarial Machine Learning for NextG Covert Communications using Multiple Antennas," Entropy 24, no. 8: 1047, 2022.

[Kim2020-2] B. Kim, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, S. Ulukus, "Adversarial Attacks with Multiple Antennas Against Deep Learning-Based Modulation Classifiers," IEEE GLOBECOM Open Workshop on Machine Learning in Communications, 2020.

[McClintick2022] K. W. McClintick, J. Harer, B. Flowers, W. C. Headley and A. M. Wyglinski, "Countering Physical Eavesdropper Evasion with Adversarial Training," *IEEE Open Journal of the Communications Society*, 2022.

[Sahay2021] R. Sahay, C. G. Brinton and D. J. Love, "Frequency-based Automated Modulation Classification in the Presence of Adversaries," *IEEE International Conference on Communications (ICC)*, 2021.

[DelVecchio2020] M. DelVecchio, B. Flowers and W. C. Headley, "“Effects of Forward Error Correction on Communications Aware Evasion Attacks," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2020.

[Filipovic2019] S. Kokalj-Filipovic and R. Miller, "Adversarial Examples in RF Deep Learning: Detection of the Attack and its Physical Robustness," *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2019.

[Lin2020] Y. Lin, H. Zhao, Y. Tu, S. Mao, and Z. Dou, "Threats of Adversarial Attacks in DNN-based Modulation Recognition," *IEEE Conference on Computer Communications (INFOCOM)*, 2020.

[Bahramali2021] A. Bahramali, M. Nasr, A. Houmansadr, D. Goeckel, and D. Towsley, "Robust Adversarial Attacks against DNN-based Wireless Communication Systems," *ACM SIGSAC Conference on Computer and Communications Security (CC)*, 2021.

[Shi2018] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, Z. Lu and J. H. Li, "Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies," *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018.

[Erpek2019-2] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep Learning for Launching and Mitigating Wireless Jamming Attacks," *IEEE Transactions on Cognitive Communications and Networking*, 2019.

[Sagduyu2021] Y. E. Sagduyu, T. Erpek, and Y. Shi, "Adversarial Machine Learning for 5G Communications Security," *Game Theory and Machine Learning for Cyber Security*, 2021.

[Luo2022] Z. Luo, S. Zhao, Z. Lu, J. Xu and Y. E. Sagduyu, "When Attackers Meet AI: Learning-Empowered Attacks in Cooperative Spectrum Sensing," *IEEE Transactions on Mobile Computing*, 2022.

[Shi2022-3] Y. Shi, Y. E. Sagduyu, and T. Erpek, "Federated Learning for Distributed Spectrum Sensing in NextG Communication Networks," *SPIE Defense + Commercial Sensing (DCS) Conference on Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications*, 2022.

[Sagduyu2022-2] Y. E. Sagduyu, "Free-Rider Games for Federated Learning with Selfish Clients in NextG Wireless Networks," *IEEE Conference on Communications and Network Security (CNS): Cyber Resilience Workshop*, 2022.

[Shi2022-4] Y. Shi and Y. E. Sagduyu, "Jamming Attacks on Federated Learning in Wireless Networks," *arXiv preprint* arXiv:2201.05172, 2022.

[Shi2022-5] Y. Shi and Y. E. Sagduyu, "How to Launch Jamming Attacks on Federated Learning in NextG Wireless Networks," *IEEE Globecom Workshops (GC Wkshps): The Seventh IEEE Workshop on 5G and Beyond Wireless Security (7th IEEE Wireless-Sec)*, 2022.

[Hameed2021] M. Z. Hameed, A. Gyorgy, and D. Gunduz, "The Best Defense is a Good Offense: Adversarial Attacks to Avoid Modulation Detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, 2021.

[Kim2022-3] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "How to make 5G communications 'invisible': Adversarial machine learning for wireless privacy," *Asilomar Conference on Signals, Systems, and Computers*, 2020.

[Kim2022-4] B. Kim, T. Erpek, Y. E. Sagduyu, and S. Ulukus, "Covert Communications via Adversarial Machine Learning and Reconfigurable Intelligent Surfaces," IEEE Wireless Communications and Networking Conference (WCNC), 2022.

[Kim2022-5] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Adversarial Machine Learning for NextG Covert Communications using Multiple Antennas," *Entropy*, 2022.

[Kim2021-2] B. Kim, Y. E. Sagduyu, T. Erpek, and S. Ulukus, "Adversarial Attacks on Deep Learning Based mmWave Beam Prediction in 5G and Beyond," *IEEE Statistical Signal Processing (SSP) Workshop*, 2021.

[Kim2021-3] B. Kim, Y. Shi, Y. E. Sagduyu, T. Erpek, and S. Ulukus, "Adversarial Attacks against Deep Learning Based Power Control in Wireless Communications," *IEEE Global Communications Conference (GLOBECOM) Workshops*, 2021.

[Sanguinetti2018] L. Sanguinetti, A. Zappone and M. Debbah, "Deep Learning Power Allocation in Massive MIMO," *Asilomar Conference on Signals, Systems, and Computers*, 2018.

[Manoj2021] B. R. Manoj, M. Sadeghi and E. G. Larsson, "Adversarial Attacks on Deep Learning Based Power Allocation in a Massive MIMO Network," *IEEE International Conference on Communications*, 2021.

[Sadeghi2019] M. Sadeghi and E. G. Larsson, "Physical Adversarial Attacks Against End-to-end Autoencoder Communication Systems," *IEEE Communications Letters*, 2019.

[Shi2020-2] Y. Shi, T. Erpek, and Y. E. Sagduyu, "Reinforcement Learning for Dynamic Resource Optimization in 5G Radio Access Network Slicing," *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2020*.

The Author

Bio: Yalin E. Sagduyu received his B.S. degree in Electrical and Electronics Engineering from Bogazici University, Turkey and his M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Maryland at College Park. He is a Research Professor at Virginia Tech National Security Institute. Prior to that, he was the Director of Networks and Security at Intelligent Automation, Inc./BlueHalo. He is also a Visiting Research Professor at the Department of Electrical and Computer Engineering at the University of Maryland, College Park. His research interests are in wireless communications, networks, security, and machine learning. He is an Editor of IEEE Transactions on Communications. He chaired workshops at ACM MobiCom, ACM WiSec, IEEE CNS and IEEE ICNP, served as a Track Chair at IEEE PIMRC, IEEE GlobalSIP and IEEE MILCOM, and served in the organizing committee of IEEE GLOBECOM and IEEE MILCOM. He received the IEEE HST 2018 Best Paper Award.