Timely and Covert Communications under Deep Learning-Based Eavesdropping and Jamming Effects

Maice Costa and Yalin E. Sagduyu

***Abstract*—This paper explores the concept of timeliness in covert communications when faced with eavesdropping and jamming. Time-sensitive information is to be transmitted through a wireless channel between a transmitter and a receiver, while an adversary seeks to detect the communication attempts with a deep learning-based classifier (using feedforward or convolutional neural networks). The adversary jams any detected transmission, subject to an average power budget. When the transmit power is set at a high level, the outage probability decreases, resulting in more reliable communication. However, this also increases the accuracy of the adversary's detection, making it more likely for the jammer to successfully identify and jam the communication. On the other hand, using a low transmit power leads to a higher outage probability for communication but decreases the accuracy of the adversary in detecting and disrupting a transmission. The trade-off between reliability, timeliness, and stealthiness in wireless communications is analyzed in this paper by characterizing the Age of Information and its behavior under the influence of eavesdropping and jamming effects. Results indicate novel operation modes for timely and covert communications under eavesdropping and jamming effects.**

***Index Terms*—Age of information, covert communications, deep learning, eavesdropping, jamming, status updates, timeliness.**

I. Introduction

THE next generation wireless communications systems will serve a variety of applications, from vehicle networks to the automation of the electric grid, everything is to be connected. The requirements and constraints vary according to the objectives of communication, and traditional metrics as delay and throughput no longer suffice to describe the performance of a communication system. In many cases, the communication should deliver time-sensitive and private information on time, possibly in a hostile environment. This work analyzes important trade-offs in wireless communications involving reliability, timeliness, and stealthiness, under the presence of channel fading, noise, and interference.

When a message carries information to guide any decision happening immediately upon receipt, it is crucial to analyze the system with respect to metrics related to information timeliness. Age of Information (AoI) defined as the time elapsed since the last received update was generated [1] provides the framework to quantify timeliness of messages transmitted through a communication network. Applications where timeliness is of utmost importance include networked control systems, industrial automation, vehicular networks, online gaming, and healthcare.

Many applications concerned with timeliness are also concerned with privacy or resilience to adversary activity. This is certainly the case in military applications, but it may also hold in civilian applications, for example when data transmission includes personal identifiable information. Due to the open and shared nature of wireless communications, information privacy is a fundamental challenge. In a hostile environment, wireless communication involves a transmitter and a receiver, as well as an eavesdropper who attempts to gather information about the communication between the two parties. The eavesdropper can have different objectives, such as decoding the transmissions or simply detecting whether communication is taking place. Ideally, communication in a hostile environment requires a coding scheme that is resilient to every jamming strategy. Classical security mechanisms seek to protect the content so that an adversary is unable to decode it. Unauthorized decoding has been the subject of extensive study, with research exploring encryption-based security and information-theoretical approaches [2].

In this work, we consider the problem of transmitting time-sensitive information in a hostile environment under the presence of noise and adversarial interference. We focus on the signal detection task performed by the adversary and investigate the performance trade-offs between AoI and transmission power under different channel conditions. While increasing the transmission power increases the signal-to-noise ratio (SNR) in the channel between source and destination, it also increases SNR in the channel to the adversary, increasing the probability of detection and interference. To the best of our knowledge, no previous work has discussed in detail the coupling of transmission power and the detection task performed by the adversary under time-sensitivity requirements. We elicit the trade-offs involved in the selection of transmission power to attempt stealthy communication with low probability of detection and low probability of interception (LPD/LPI). Since a low power transmission can be jammed with low power interference, the stealthy transmission may save power for the adversary. On the other hand, the detection errors may cause the adversary to waste power when a false alarm occurs. In this paper, we seek to better understand such trade-offs.

The remainder of this paper is organized as follows. Section II presents related work in the literature related to AoI, covert communication, and jamming in wireless communications. In Section III we present the models and assumptions for

Manuscript received May 22, 2023; revised July 31, 2023; approved for publication by Yin Sun, Guest Editor, August 8, 2023.

The authors are with the Virginia Tech National Security Institute, Blacksburg, Virginia, USA. email: {mcosta, ysagduyu}@vt.edu.

M. Costa is the corresponding author.

Digital Object Identifier: 10.23919/JCN.2023.000034

1229-2370/23/$10.00 © 2023 KICS

the communication system and adversary. Section IV presents the tools and metrics used in our analysis, including the outage and AoI formulations, as well as the deep learning models used for signal detection by the adversary. Section V presents numerical results. Section VI provides concluding remarks.

II. Related Work

The pioneer work in [1] introduced the concept of AoI. The initial work on AoI [1], [3], [4] focused on queuing models to establish the need for new performance metrics for timeliness. Work by Ephremides et al. contributed to those initial steps, helping to sparkle interest from the wireless network research community [5]–[7]. The topic received a great deal of attention in the last decade. The literature is vast, and the applications that require such timeliness metrics are numerous; refer to [8] for an introduction and survey. This shift to consider information timeliness also led to a new paradigm of communications accounting for quality of information, as opposed to quantity in the traditional approach, such as envisioned for semantic- and goal-oriented communications [9], [10]. To that end, AoI was analyzed for task-oriented communications with the goal of completing (potentially machine learning) tasks at the receiver rather than reconstructing messages [11],

The impact of hostile interference on AoI was addressed in [12], where the interaction is formulated as a non-zero-sum two player game to determine the transmission and interference power levels. A dynamic game was proposed in [13] to study the selection of transmission times, focusing on medium access for the definition of utilities. The work in [14] extended [12] for the case with background noise, presenting the Nash equilibrium strategies as function of updating rate, and a Stackelberg equilibrium with the transmitter as a leader. Channel access and scheduling for AoI-focused transmissions in adversarial environments have also been considered in [15] and [16].

Covert communication attempts to hide the fact that any content is being transmitted. Stealthy communication is a similar concept, where the symbols may be drawn from an innocent distribution when no communication happens, as opposed to the zero symbols required in covert communication. Previous research has investigated covert (stealth) communications, where the aim is to hide information in noise by reducing the SNR at the eavesdropper [17]–[20]. The combination of covertness and timeliness requirements has also been considered. In [21], time uncertainty was introduced to confuse the adversary and enable covert communication. A covertness maximization problem under the AoI constraint to optimize the transmit probability was considered in [22]. Covertness and timeliness trade-offs were also investigated in [23], seeking the optimal block-length and prior transmission probability.

when the transmission is not covert, it can be interfered with brute-force jamming using a fixed signal (such as Gaussian noise). Alternatively, an adversarial machine learning (AML) approach can be applied to generate signals for covert communications. Previous research in [24] has explored the privacy of wireless communications when an eavesdropper uses a deep learning classifier to detect transmissions of interest. In this setting, a single transmitter communicates with its receiver while an eavesdropper is present. To counter the eavesdropper, a cooperative jammer (CJ) (potentially with multiple antennas [25]) transmits carefully crafted adversarial perturbations to deceive the eavesdropper into classifying the received signal as noise. This constitutes an evasion or adversarial attack within the realm of AML. Another approach is for the transmitter itself to add perturbations to its own signals and deceive the eavesdropper [26] into misclassifying the perturbed signals as noise.

There are different levels of uncertainty for a jammer to overcome in a wireless network in order to launch a successful jamming attack. For example, the jammer may not know the role of a transmitter, e.g., a legitimate transmitter to jam or another jammer. To that end, concealing the role of a transmitter can create uncertainty for the jammer [27], [28] so that the jammer is potentially fooled into missing jamming opportunities. Also, the dynamic packet traffic makes the time instants of transmission uncertain for the jammer so that the jammer may waste jamming power as it is fooled into jamming idle slots when there is no transmission [29], [30]. In this paper, we consider traffic uncertainty as well as potential errors in identifying jamming opportunities (such as classifying received signals as idle channel by the eavesdropper). Subject to these uncertainty effects, we analyze AoI in the presence of an adversary with eavesdropping and jamming objectives.

III. System Model

A. Communication Model

We consider a transmitter (Tx) sending time-sensitive information to a receiver (Rx) in a hostile environment where an active adversary (J) can potentially eavesdrop and interfere with the attempted communication. We assume that transmissions are subject to Rayleigh fading plus Gaussian noise. The signal transmitted by Tx will reach Rx through a fading channel with average power coefficient h_1, and it will reach the eavesdropper through another channel with average power coefficient h_2. When the adversary chooses to jam the signal, it will send an interference signal to Rx through another independent channel with average power coefficient h_3. We assume that a packet transmission takes place within the channel coherence time, so fading coefficients remain the same throughout the packet duration. The transmission power is denoted with P_T, the jamming power (if any) is denoted with P_J. All transmissions through channel h_i are subjected to noise n_i and noise power is denoted with σ_i^2, for $i \in \{1, 2, 3\}$. We illustrate the network model in Fig. 1.

We assume that communication takes place using fixed and independent resource blocks. The signal is modulated using phase shift keying (PSK), and we show results for binary (BPSK) and quadrature (QPSK) modulation. Unless otherwise stated, we assume a packet consists of 32 I/Q symbols. We also discuss the effect of the number of symbols in Section IV, where we show results for 16, 32, 64, and 128 I/Q symbols.

An outage occurs when the selected transmission rate is not supported by the channel. At the receiver, the interference

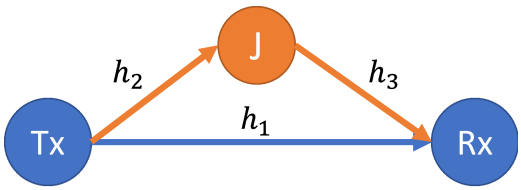


Fig. 1. Network model.

caused by jamming activity may result in an outage, which we regard as a packet loss for the purposes of calculating the age of the information available at Rx. For each of the channels, we denote the SNR (SINR) with γ_i, for $i \in \{1, 2, 3\}$ with the understanding that γ_2 and γ_3 represent the SNR in channels connecting Tx and eavesdropper, and eavesdropper and Rx, where we do not assume any interference. In the direct channel between Tx and Rx, we have

$$\gamma_1 = \frac{h_1 P_T}{\sigma^2 + \mathbb{I}_J h_3 P_J}, \tag{1}$$

where $\mathbb{I}_J$ represents an indicator function which takes the value $\mathbb{I}_J = 1$ if the adversary decides to cause interference. We assume that an outage event occurs if the SINR falls below a certain threshold $\gamma_{\min}$,

$$p_{out} = \mathbb{P}\left[\frac{h_1 P_T}{\sigma^2 + \mathbb{I}_J h_3 P_J} \leq \gamma_{\min}\right]. \tag{2}$$

By conditioning on the jamming activity, we write the probability of a packet loss as

$$\begin{aligned} p_{out} = &\ \mathbb{P}\left[\frac{h_1 P_T}{\sigma^2 + \mathbb{I}_J h_3 P_J} \leq \gamma_{\min} | \mathbb{I}_J = 0\right] \mathbb{P}[\mathbb{I}_J = 0] \\ &+ \mathbb{P}\left[\frac{h_1 P_T}{\sigma^2 + \mathbb{I}_J h_3 P_J} \leq \gamma_{\min} | \mathbb{I}_J = 1\right] \mathbb{P}[\mathbb{I}_J = 1] \\ = &\ \mathbb{P}\left[\frac{h_1 P_T}{\sigma^2} \leq \gamma_{\min}\right] \mathbb{P}[\mathbb{I}_J = 0] \\ &+ \mathbb{P}\left[\frac{h_1 P_T}{\sigma^2 + h_3 P_J} \leq \gamma_{\min}\right] \mathbb{P}[\mathbb{I}_J = 1]. \end{aligned} \tag{3}$$

B. Adversary Model

We assume a machine learning based adversary eavesdropper (J) listening to the communication channel and using a deep learning classifier to decide about the presence of a signal to interfere with. The output of the classifier is imperfect, so the adversary makes Type 1 (false positive) and Type 2 (false negative) errors. The accuracy of the classification task depends on the transmission power used by Tx and the channel quality between Tx and J.

When a signal is detected, the adversary may not only passively eavesdrop, but actively jam the signal, increasing the interference level to disrupt the communication between Tx and Rx. Let hypothesis $\mathcal{H}_0$ represent the absence of signal and $\mathcal{H}_1$ represent the presence of signal. That is, the signal at J, $y_J(t)$, under each hypothesis is

$$\mathcal{H}_0 : y_J(t) = n_2(t), \tag{4}$$

$$\mathcal{H}_1 : y_J(t) = X(t) + n_2(t), \tag{5}$$

where $X(t)$ is the received signal and $n_2(t)$ is the additive white Gaussian noise of power σ_2^2. The decision about the presence of a signal is a binary hypothesis test. According to Neyman-Pearson criterion, the optimal decision rule for a given transmission power is the likelihood ratio test (LRT). With a threshold Y_{th} and average power received at the eavesdropper given by $\bar{y}_J$, we write the decisions, D_0 for $\mathcal{H}_0$ or D_1 for $\mathcal{H}_1$ as

$$\bar{y}_J \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} Y_{th}. \tag{6}$$

We assume that the adversary never transmits an interfering signal when it believes $\mathcal{H}_0$ is the true hypothesis. Let $p_f = \mathbb{P}[\mathcal{D}_1|\mathcal{H}_0]$ denote the probability of a false alarm (false positive), and $p_m = \mathbb{P}[\mathcal{D}_0|\mathcal{H}_1]$ denote the probability of misdetection (false negative). Under the LRT, the detection error probability is defined as

$$\epsilon = \mathbb{P}[\mathcal{H}_0] p_f + \mathbb{P}[\mathcal{H}_1] p_m. \tag{7}$$

The well-known square root law established the information theoretic limits for covert communication for AWGN channels [31], if the minimum detection error satisfies

$$\epsilon^* \geq \min\{\mathbb{P}[\mathcal{H}_1], \mathbb{P}[\mathcal{H}_0]\} - \delta, \tag{8}$$

where δ is a tolerance level for the covert communication. A positive rate for covert communication can be obtained with the introduction of uncertainty in the channel to the adversary, including cooperative jamming and uncertainty in time of transmissions. For a machine learning based adversary, detection errors may also be introduced by the classifier or by an evasion attack.

The decision to jam the detected signal is subject to an average jamming power constraint $\bar{P}_{\max}$ that represents the concerns of an adversary with limited power budget. The average power $\bar{P}_J$ satisfies $\bar{P}_J \leq \bar{P}_{\max}$, with

$$\begin{aligned} \bar{P}_J = &\ \mathbb{P}[\mathcal{H}_0]\left(0 \times (1 - p_f) + P_J \times p_f\right) \\ &+ \mathbb{P}[\mathcal{H}_1]\left(0 \times p_m + P_J \times (1 - p_m)\right). \end{aligned} \tag{9}$$

C. Status Updating Model

We consider two options for the status updates: a buffer model (M1) and a bufferless just-in-time model (M2). We assume that Tx will not hold packets if they are ready to be transmitted, meaning that the only times Tx is silent is when it has no packets to transmit. A packet transmission has fixed duration as determined by the system's resource block size.

(M1): A random arrival model where the packets are generated according to a Poisson process, placed in a buffer with unlimited capacity, and transmitted in a first-come-first-served fashion. In this case, the system is modeled as a M/G/1 queue. With a service time S, where $\mathbb{E}[S] = 1/\mu$ and utilization factor $\rho = \min\{1, \lambda/\mu\}$, the expected sojourn time is calculated as the sum of service and waiting times as [32]

$$\mathbb{E}[T] = \mathbb{E}[S] + \mathbb{E}[W] = \mathbb{E}[S] + \frac{\lambda \mathbb{E}[S^2]}{2(1 - \rho)}. \tag{10}$$

For a network with fixed resource blocks, we assume a deterministic service time of duration $S = D$ and use the M/D/1 queue model, so $\mu = 1/D$ and $\rho = \lambda D$.

(M2): A bufferless just-in-time updating model where the packet is generated and transmitted within one time slot. In this case, there is no queuing of packets waiting for transmission. We assume that Tx decides to send an update or not at a given slot according to a Bernoulli process, so updates are generated with rate λ as in M1. We assume that the time to generate the update is negligible, so service time is also assumed to have deterministic duration D, and system utilization is also $\rho = \lambda D$.

IV. Performance Analysis

A. Outage Probabilities

To evaluate the probability of losing a packet, we need to determine the probability distributions of the SNR, $F_{\gamma(\cdot)}$ and that of the SINR, $F_{\gamma_I}(\cdot)$. Under the assumption of Rayleigh fading with fixed transmission power and constant noise power during one resource block, the SNR is exponentially distributed,

$$F_{\gamma_i}(y) = 1 - \exp\left(-\frac{\sigma_i^2 y}{h_i P_j}\right), \quad i \in \{1,2,3\},\ j \in \{T,J\},\ y \geq 0, \tag{11}$$

where h_i represents the average signal gain in the channel.

For the case of transmission between Tx and Rx under interference, we have the denominator of SINR $I = \sigma^2 + h_3 P_J$ representing the total amount of interfering power. This random variable depends on the noise and the channel gain between the jammer and Rx. Assuming a constant noise power, the distribution function is

$$F_I(y) = F_{H_3}\left(\frac{y-\sigma^2}{P_J}\right) = 1 - \exp\left(-\frac{y-\sigma^2}{h_3 P_J}\right),\ y \geq \sigma^2, \tag{12}$$

where h_3 represents the average signal gain in the channel between the jammer and Rx. Using standard tools to calculate the distributions of transformations of random variables, we obtain the distribution of the SINR as [33]

$$F_{\gamma_I}(y) = 1 - \frac{P_T}{P_T + y P_J}\exp\left(-\frac{\sigma^2}{P_T} y\right). \tag{13}$$

B. Signal Detection at Adversary

For both status updating models, (M1) with Poisson arrivals, or (M2) with just-in-time updates, we assume that the system is idle for a fraction of time given by $1-\rho$, where ρ is the system utilization. With a fixed service time of duration D, so $\rho = \lambda D$. As we assume that Tx always transmits if there is packet waiting, $\mathbb{P}[\mathcal{H}_0] = 1 - \rho = 1 - \mathbb{P}[\mathcal{H}_1]$.

Since the transmissions occur at random resource blocks, the adversary does not know when a signal is present, and needs to sense the channel every time slot. The scenario where the adversary has knowledge of transmission power, resource block length, and prior probability ρ represents the worst case.

The signal detection activity is implemented using a deep learning classifier. It is well-known that deep neural networks can effectively capture the spectrum data characteristics and provide higher accuracy in wireless signal classification compared to simpler machine learning models or other statistical methods such as energy detection [34]–[36]. We experimented with two types of networks, a feedforward neural network (FNN), and a convolutional neural network (CNN), with Glorot uniform initializer, Adam optimizer, and categorical cross entropy loss function, to implement a binary classifier with labels 'Signal' vs. 'No signal'.

TABLE I
Deep neural network architectures for the adversary classifier.

FNN	CNN
Dense (64, ReLU)	Conv2D ((1,3), ReLU)
Dropout (0.1)	Flatten
Dense (16, ReLU)	Dense (32, ReLU)
Dropout (0.1)	Dropout (0.1)
Dense (4, ReLU)	Dense(8, ReLU)
Dropout (0.1)	Dropout (0.1)
Dense (2, SoftMax)	Dense (2, SoftMax)

TABLE II
Number of trainable parameters versus number of I/Q symbols per packet.

I/Q symbols	FNN	CNN
16	3,230	37,306
32	5,278	70,074
64	9,374	135,610
128	17,566	266,682

The FNN classifier used by the adversary to decide about the presence of a signal consists of three dense layers of sizes $64, 16$, and 4, respectively, all with ReLU activation, and a dense layer of size 2 with SoftMax activation as the final layer for the two classes.

The CNN classifier consists of a Convolution2D layer with kernel size $(1,3)$ and ReLU activation function, followed by a Flatten layer, a Dense layer with size 32 and and ReLU activation function, a Dropout layer with dropout rate 0.1, a Dense layer with size 8 and and ReLU activation function, a Dropout layer with dropout rate 0.1, and finally an output Dense layer with size 2 and SoftMax activation function. FNN has a smaller memory footprint, making it more amenable for embedded implementation on edge devices with limited memory. On the other hand, CNN achieves higher classification accuracy at the expense of higher memory requirement (due to the dense connections introduced by the flatten later and the subsequent dense layers). We summarize the two architectures in Table I.

The classification accuracy depends on the SNR in the channel between the transmitter and the adversary, as well as the number of symbols to be detected. The detection accuracy is better with CNN in comparison to FNN and, for both models, the accuracy increases when we increase the packet size. We illustrate this effect with packet sizes of $16, 32, 64, and 128$ I/Q samples, as shown in Fig. 2.

The increased accuracy for larger number of symbols comes at the expense of large number of parameters for the classifier. In Table II, we summarize the number of trainable parameters for each classifier versus packet size.

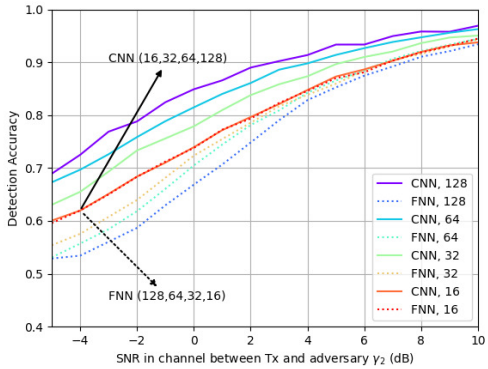


Fig. 2. Classifier accuracy versus SNR between transmitter and adversary and effect of number of I/Q symbols per packet.

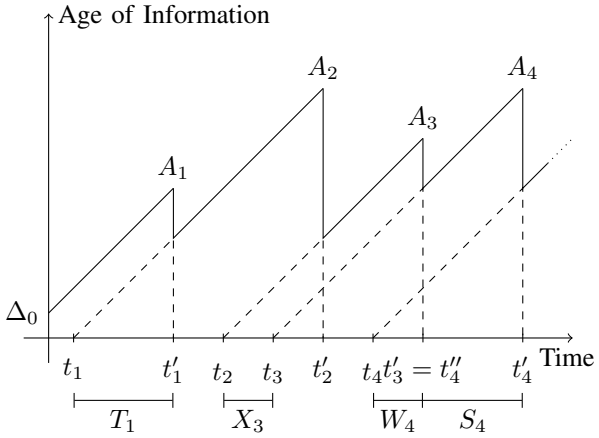


Fig. 3. Sawtooth curve - A sample path for AoI.

C. Communication Timeliness

For the status update model (M1), we consider a M/D/1 queue with packet errors and follow steps analogous to those taken in [37] to obtain the expected peak AoI (PAoI) [38]. We assume Poisson arrivals of rate λ and deterministic service time D. The service rate is $\mu = 1/D$ and the utilization factor is $\rho = \lambda/\mu$. Packets are dropped with probability p (which depends on SNR, or SINR under potential jamming).

Let $\mathcal{I}$ denote the set of informative packets at the receiver. That is, the set of packets that are received successfully and contribute to reducing the AoI. Denote with t_k the generation time of packet k, while t_k' denotes its departure time. Let t_k'' denote the time packet k begins to be served. We define the interarrival time, waiting time, service time, and sojourn time, respectively, as

$$X_k \coloneqq t_{k+1} - t_k, \tag{14}$$
$$W_k \coloneqq t_k'' - t_k, \tag{15}$$
$$S_k \coloneqq t_k' - t_k'', \tag{16}$$
$$T_k \coloneqq t_k' - t_k. \tag{17}$$

We illustrate (14)–(17) and the evolution of AoI with a sample path in Fig. 3, where we denote with Δ_0 the initial value of AoI and with A_k the peak values reached immediately before receiving the packet update k.

The PAoI is given by the interarrival time between two informative packets plus the time a packet spends in the system (sojourn time). Let $m(k)$ be the first informative packet that arrives no earlier than packet k, defined as [37]

$$m(k) \coloneqq \min\{k_i | k_i \in \mathcal{I}, t_{k_i} \geq t_k\}. \tag{18}$$

The interarrival is

$$\hat{X}_k = t_{m(k)} - t_k, \tag{19}$$

and the service time is

$$\hat{S}_k = t'_{m(k)} - t''_k. \tag{20}$$

If $k \in \mathcal{I}$, then $m(k) = k$, $\hat{X}_k = 0$, and $\hat{S}_k = S_k$. Now consider an informative packet k_i. The next packet to arrive is $k_i + 1$, and the next informative packet is k_{i+1}. The expected PAoI in this case is

$$A_p = \mathbb{E}\left\{X_{k_i} + \hat{X}_{k_i+1} + T_{k_{i+1}} | k_i, k_{i+1} \in \mathcal{I}\right\}, \tag{21}$$

where

$$\begin{aligned}\mathbb{E}[\hat{X}_{k_i+1}] = {} & (1-p)\mathbb{E}[\hat{X}_{k_i+1} | k_i + 1 \in \mathcal{I}] \\ & + p\mathbb{E}[X_{k_i+1} + \hat{X}_{k_i+2} | k_i + 1 \notin \mathcal{I}].\end{aligned} \tag{22}$$

Using $\mathbb{E}[\hat{X}_{k_i+1}] = \mathbb{E}[\hat{X}_{k_i+2}]$, we write

$$\begin{aligned}\mathbb{E}[\hat{X}_{k_i+1}] &= 0 + p\left[\frac{1}{\lambda} + \mathbb{E}[\hat{X}_{k_i+1}]\right] \\ \mathbb{E}[\hat{X}_{k_i+1}] &= \frac{p}{(1-p)\lambda}.\end{aligned} \tag{23}$$

Substitute (23) in (21), together with $\mathbb{E}[X_{k_i}] = 1/\lambda$, and using the expected sojourn time for M/D/1 queue [32], we obtain for updating model (M1) the average PAoI as

$$A_p^{\text{M/D/1}} = \frac{1}{\lambda(1-p)} + D + \frac{D\rho}{2(1-\rho)}, \tag{24}$$

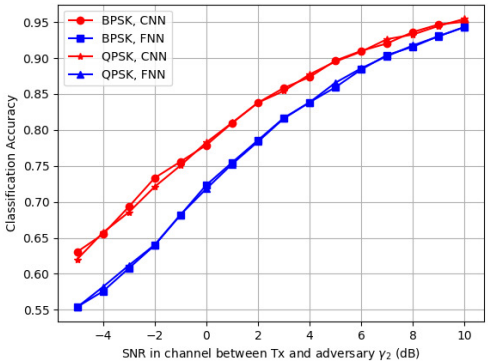
while for just-in-time (JIT) updates we eliminate the waiting time and

$$A_p^{\text{JIT}} = \frac{1}{\lambda(1-p)} + D. \tag{25}$$

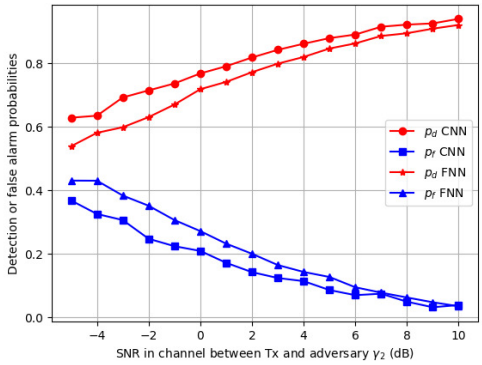
We could say that from a timeliness perspective, the cost of queuing is $C = \mathbb{E}[W] = d\rho/2(1-\rho)$. Clearly, the probability that a packet is dropped has a negative impact on PAoI. We highlight that under our model this probability p carries the intricate relationships between several parameters involved in the communication between Tx and Rx, and the decisions of an active adversary, subject to classification results and an average jamming power budget. In this paper, we investigate those relationships and trade-offs.

For updating model (M1), under a fixed probability of loss p, we calculate the arrival rate that minimizes the PAoI in (24), noting that $\rho = \lambda D$ and D is a deterministic service time. We calculate the derivative

$$\frac{\partial A_p^{\text{M/D/1}}}{\partial \lambda} = \frac{2 - 4D\lambda + \lambda^2 D^2(p+1)}{2(p-1)\lambda^2(1-\lambda D)^2}, \tag{26}$$



(a) Classification accuracy versus SNR γ_2.



(b) Detection and false alarm versus SNR γ_2.

Fig. 4. Classifier performance for FNN and CNN architectures with BPSK and QPSK signals.

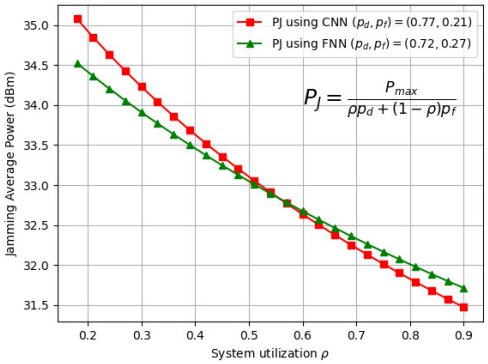


Fig. 5. Jamming power versus channel utilization with fixed SNR between Tx and jammer $\gamma_2 = 0$ dB.

and we select the root that satisfied the stability condition $\lambda D \leq 1$, hence

$$\lambda^* = \frac{2 - \sqrt{2(1-p)}}{D(1+p)}. \tag{27}$$

For updating model (M2), since packets are not 'aging' in a queue, the PAoI is minimized with $\lambda^* = 1/D$, so Tx would generate and transmit a packet in every resource block.

In the adversarial environment, some uncertainty with respect to the time of transmission works to the advantage of Tx. Also, the loss probability p depends on the system utilization (hence on λ) through the expected jamming power given by the constraint (9). We discuss this effect in Section V.

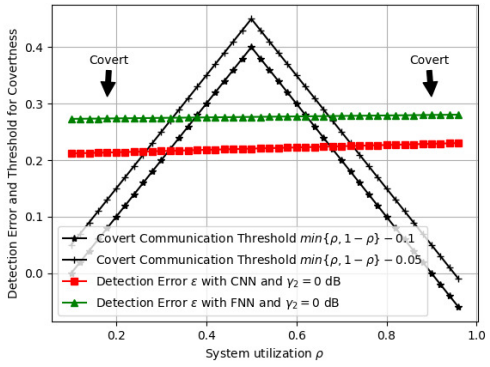
V. Numerical Results

We implemented a deep learning binary classifier to decide between 'Signal' or 'No signal.' Data is sent as packets, each one representing a data sample of size (2,32) corresponding to 32 I/Q (wireless signal) samples. We consider both BPSK and QPSK modulations, but our experiments indicate that the classifier performance is very similar for the two modulation schemes. We used 5000 samples – 80% for training and 20% for testing, and averaged our results over 20 simulations. Accuracy results are presented in Fig. 4, where we show in Fig. 4(a) the average accuracy as the average SNR in the channel between Tx and the adversary increases, and we show the detection and false alarm probabilities for BPSK in Fig. 4(b). As expected, accuracy and detection probability increase with SNR, while false alarm probability decreases with SNR.

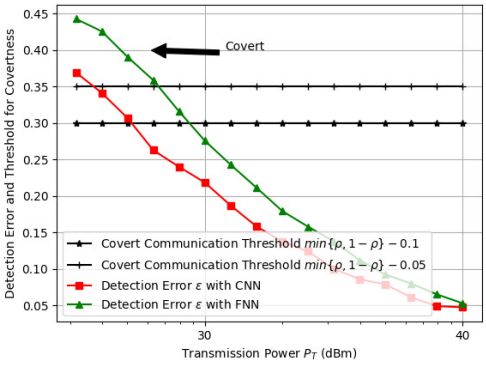
An interesting behavior is observed for the selection of jamming power. We assume the adversary satisfies the constraint in (9) with equality. If the channel under observation is very busy (Tx transmits often and $\rho > 0.6$), then the adversary with more accurate classifier (namely, CNN) would interfere more often but with less power than its counterpart with a weaker classifier (namely, FNN), which has higher probability of missing the signal but when it causes interference it does so with higher power. In the case of smaller channel utilization, with $\rho < 0.4$, the jamming power is smaller for the FNN adversary, because it wastes more power in the false alarm events. We illustrate the jamming power selection in Fig. 5, where we consider a fixed SNR in the channel between Tx and the adversary, $\gamma_2 = 0$ dB, and use the performance of each classifier corresponding to this SNR value. This result points to the need of adaptive power control for the adversary. From the perspective of the transmitter, those errors are beneficial and necessary for covert communication.

We illustrate the total detection error in comparison to the threshold for covert communication as in (8). We include two curves for the threshold to indicate the behavior with the variable δ, which indicates the covertness tolerance. We plot the total error for the CNN and FNN classifiers and compare to the threshold depending on system utilization. In Fig. 6(a) we assume $\gamma_2 = 0$ dB and use the corresponding performance for the FNN and CNN classifiers. We show that the total error can be above the threshold for very small or very large system utilization. In Fig. 6(b) we fix the system utilization to $\rho = 0.4$ and vary the transmission power (hence the SNR in the channel to the jammer). The total detection error decreases with increasing P_T, and the comparison to the threshold lines indicate the need to keep transmit power very low if the objective is covert communication. As we discuss next, this objective of covertness may be conflicting with one for timeliness.

If the signal is successfully detected at the eavesdropper,

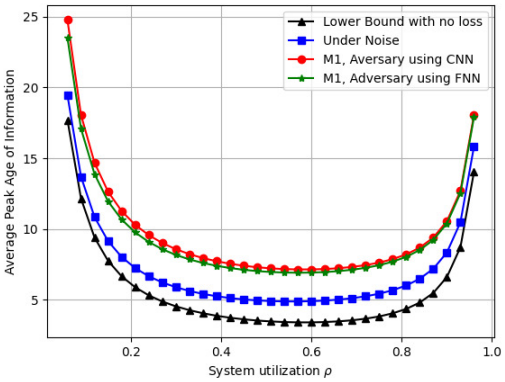


(a) Versus system utilization ρ with $\gamma_2 = 0$ dB.

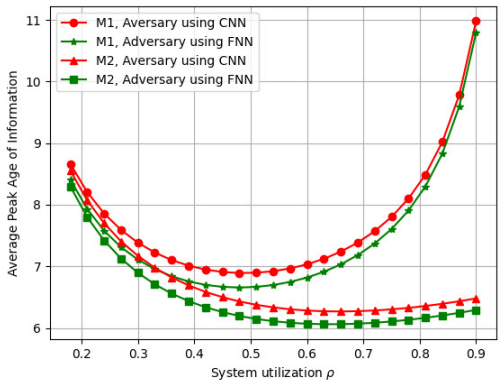


(b) Versus Transmission Power P_T (dBm) with $h_2 = 1$.

Fig. 6. Detection error ϵ and threshold for covertness.



(a) Average PAoI for M1 and baseline cases.



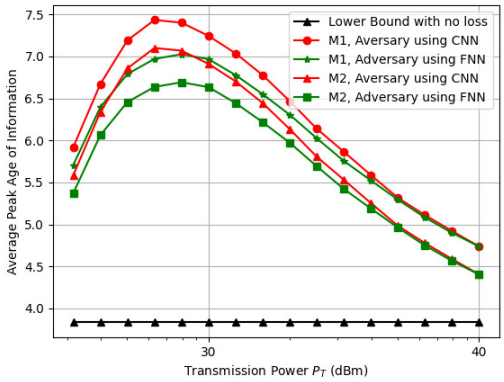
(b) Average PAoI with and without queues.

Fig. 7. Average PAoI A_p versus system utilization ρ with $h_2 = h_3 = 1$ and $h_1 = h_2/\alpha$.

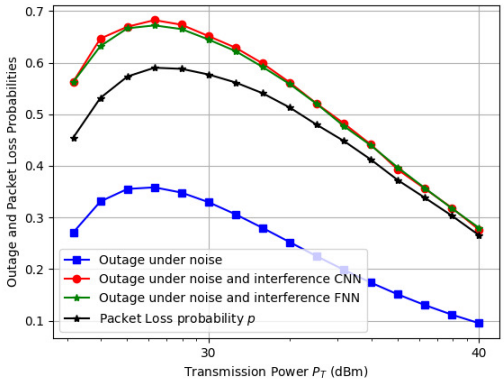
then the transmitter may have to endure some level of adversary interference. Moving forward, we present results related to the communication between Tx and Rx in the presence of the adversary. Unless otherwise stated, we assume the noise power $\sigma_i^2 = 1$, $\forall i \in \{1, 2, 3\}$, the required SNR threshold $\gamma_{\min} = 1$, and the average jamming power constraint $\bar{P}_{\max} = 1$. When varying transmit power, we assume $\gamma_2 \in [-5, 10]$ dB, and investigate different conditions among channel coefficients. When varying system utilization, we fix $\gamma_2 = 0$ dB. We assume that the adversary will interfere if the signal is correctly detected by the classifier, and the jamming power is the average power satisfying the power constraint (9).

We calculate the average PAoI as in (24) and plot versus system utilization with and without packet loss. Packets are lost with probability p depending on the SNR or SINR under jamming activity. The SNR to adversary is kept constant $\gamma_2 = 0$, and transmission power is fixed to $P_T = 30$ dBm. We assume that average channel gains satisfy $h_2 = 1$ and $h_1 = h_2/\alpha$ where $\alpha \in (0, 1]$, hence channel to adversary is assumed to be weaker than channel to intended receiver. We increase the system utilization by increasing the arrival rate, while $D = 1$. The Average PAoI is shown in Fig. 7(a) in four cases: A lower bound with loss probability equal to zero, a scenario with noise only, a scenario with (M1) updating model and adversary using FNN, and one scenario with (M1) model and adversary using CNN classifier to decide about the presence of a signal. The PAoI takes the traditionally seen U-shape form, but we highlight that in a highly congested system the effect of jamming becomes less significant. While the increase in average PAoI due to adversarial activity may surpass 47% for system utilization around $\rho = 0.5$, for a very congested system the difference falls below 20%, reaching 14% when $\rho = 0.96$ (comparing the CNN adversary with the noise-only case). Comparing the FNN and CNN adversaries, the CNN (a more efficient adversary) resulted in average PAoI increasing more than 5% for small system utilization, but for a more congested system the difference is below 0.1% reaching as low as 0.086% for $\rho = 0.96$.

From the adversary point of view, investing in a more accurate classifier is justified if the transmissions to be detected are sparser. Fig. 7(b) shows the average PAoI comparing the two status update models, (M1) representing the scenario where messages arrive according to a Poisson process and may wait in queue, and (M2) representing the scenario where updates can be generated just in time for transmission. We already expected that a system without queuing results in smaller AoI, but we also understand that it is not always feasible to generate the updates on demand with such a short latency, so the JIT assumption provides a lower bound. For small system utilization, the cost of waiting is small. For $\rho = 0.3$, we observe an improvement of 3% when using

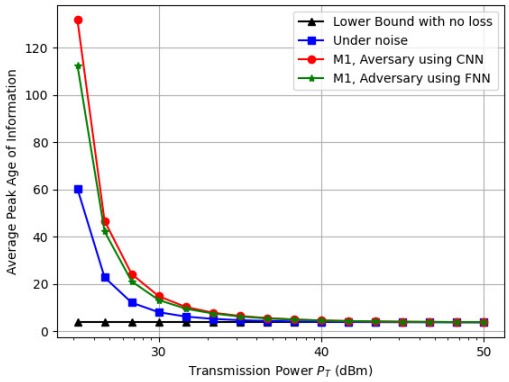


(a) Average PAoI versus transmission power P_T.

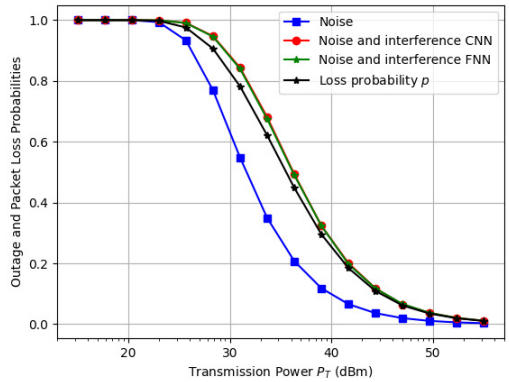


(b) Loss Probabilities versus transmission power P_T.

Fig. 8. Average PAoI and loss probabilities with $h_2 = \alpha h_1$.



(a) Average PAoI versus transmission power P_T.



(b) Loss probabilities versus transmission power P_T.

Fig. 9. Average PAoI and loss probabilities versus transmission passivelyower with $h_1 = 1$.

JIT updates as opposed to letting the updates in a buffer. If the updating rates are high, then JIT offers significant advantages, with a reduction of 20% at $\rho = 0.75$ and 41% at $\rho = 0.9$. Similar gains are observed for both the CNN and FNN adversaries.

With the same scenario of average channel gains $h_2 = 1$ and $h_1 = h_2/\alpha$, we now vary the transmission power P_T between $25-40$ dBm. The SNR in the channel to the adversary increases accordingly and the results present a clear trade-off between the potential improvement of communication between Tx and Rx as a result of higher power, and the improvement in classification performance that benefits an efficient operation of the adversary. We present the Average PAoI versus the transmission power in Fig. 8(a), and complement this example with the loss probabilities in this scenario, as shown in Fig. 8(b), where the packet loss considers the system utilization, the classification performance and jamming activity, and the outage probabilities with or without interference. The outage probability under noise calculated as (12), $F_\gamma(\gamma_{\min})$, is maximized with the tuple $(\alpha, P_T)^* = \arg\max_{(\alpha,P_T)} \frac{\alpha}{P_T}$ and that is also the point that results in maximum packet loss and maximum average PAoI.

Next, we remove the condition that the average channel gains are related by the fraction α so that channel quality is worse in the channel between Tx and the adversary in comparison to the channel between Tx and Rx. Instead, we assume $h_1 = 1$ and $\gamma_2 \in [-5, 10]$ dB. In this case, we observe that outage and loss probabilities are strictly decreasing with transmission power as shown in Fig. 9(b), and the same is observed for the average PAoI, as depicted in Fig. 9(a). It is interesting to note that the outage probability remains very high for transmission power below 22 dBm. The decay in outage probability under adversarial interference is slower, as the increased power also results in higher detection probability more interference from the jammer.

VI. Conclusions and Future Work

This paper discussed the trade-offs involving communication reliability, timeliness, and stealthiness, characterizing the AoI in a hostile RF environment with an active adversary that can eavesdrop and jam the communication between a transmitter and a receiver. This adversary uses a deep learning classifier to identify the transmissions. We analyzed the effect of classification performance on the selection of jamming power for an adversary with limited resources, comparing the use of different deep neural network models. We show that the conditions for covert communication, with very low or very high system utilization, as well as low transmit power,

may conflict with the timeliness objective. We analyze the AoI when the active adversary may cause packet loss in the system, and show that a proper trade-off between AoI and transmit power may exist, depending on the channel conditions between the nodes. Given the importance of analyzing new performance metrics that quantify quality and relevance of information, and the increasing concerns with secure communication in hostile environments, we envision that this analysis shall be extended in future work. Regarding the transmission of status updates, we have considered first-come-first-served policies, with arrivals modeled as a Poisson distribution. The analysis of other queuing models, including last-come-first-served policy and more general distributions for arrival and service times are important extensions to consider. Modeling bursty arrivals, e.g., using compound Poisson processes is also of interest. Physical layer techniques may also be included in the analysis, including the use of coding. Regarding the adversarial environment, potential directions for future work include considering countermeasures to confuse the adversary, as friendly jamming and evasion attacks, and their effect in AoI and other metrics for information relevance.

REFERENCES

[1] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?," in *Proc. IEEE INFOCOM*, 2012.

[2] M. Bloch *et al.*, "An overview of information-theoretic security and privacy: Metrics, limits, and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[3] R. D. Yates and S. Kaul, "Real-time status updating: Multiple sources," in *Proc. IEEE ISIT*, 2012.

[4] S. K. Kaul, R. D. Yates, and M. Gruteser, "Status updates through queues," in *Proc. CISS*, 2012.

[5] C. Kam, S. Kompella, and A. Ephremides, "Age of information under random updates," in *Proc. IEEE ISIT*, 2013.

[6] C. Kam, S. Kompella, and A. Ephremides, "Effect of message transmission diversity on status age," in *Proc. IEEE ISIT*, 2014.

[7] M. Costa, M. Codreanu, and A. Ephremides, "Age of information with packet management," in *Proc. IEEE ISIT*, 2014.

[8] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, and S. Ulukus, "Age of information: An introduction and survey," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1183–1210, 2021.

[9] N. Rajaraman, R. Vaze, and G. Reddy, "Not just age but age and quality of information," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1325–1338, 2021.

[10] T. M. Getu, G. Kaddoum, and M. Bennis, "Making sense of meaning: A survey on metrics for semantic and goal-oriented communication," *IEEE Access*, vol. 11, pp. 45456–45492, 2023.

[11] Y. E. Sagduyu, S. Ulukus, and A. Yener, "Age of information in deep learning-driven task-oriented communications," in *Proc. IEEE INFOCOM Workshop*, 2023.

[12] G. D. Nguyen, S. Kompella, C. Kam, J. E. Wieselthier, and A. Ephremides, "Impact of hostile interference on information freshness: A game approach," in *Proc. WIOPT*, 2017.

[13] Y. Xiao and Y. Sun, "A dynamic jamming game for real-time status updates," in *Proc. IEEE INFOCOM Workshop*, 2018.

[14] A. Garnaev, W. Zhang, J. Zhong, and R. D. Yates, "Maintaining information freshness under jamming," in *Proc. IEEE INFOCOM Workshop*, 2019.

[15] Y. Yang, X. Wei, R. Xu, L. Peng, and L. Liu, "Game-based channel access for aoi-oriented data transmission under dynamic attack," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8820–8837, 2022.

[16] A. Sinha and R. Bhattacharjee, "Optimizing age-of-information in adversarial and stochastic environments," *IEEE Trans. Inf. Theory*, vol. 68, no. 10, pp. 6860–6880, 2022.

[17] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.

[18] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.

[19] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 12, pp. 26–31, Dec. 2015.

[20] P. Mukherjee and S. Ulukus, "Covert bits through queues," in *IEEE CNS*, pp. 626–630, Oct 2016.

[21] X. Lu, S. Yan, W. Yang, M. Li, and D. W. K. Ng, "Covert communication with time uncertainty in time-critical wireless networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1116–1129, 2023.

[22] Y. Wang, S. Yan, W. Yang, and Y. Cai, "Covert communications with constrained age of information," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 368–372, 2021.

[23] W. Yang, X. Lu, S. Yan, F. Shu, and Z. Li, "Age of information for short-packet covert communication," *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1890–1894, 2021.

[24] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "How to make 5G communications "invisible": Adversarial machine learning for wireless privacy," in *Proc. IEEE ACSSC*, 2020.

[25] B. Kim, Y. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Adversarial machine learning for nextg covert communications using multiple antennas," *Entropy*, vol. 24, no. 8, p. 1047, 2022.

[26] B. Kim, T. Erpek, Y. E. Sagduyu, and S. Ulukus, "Covert communications via adversarial machine learning and reconfigurable intelligent surfaces," in *Proc. IEEE WCNC*, 2022.

[27] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 112–118, 2011.

[28] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming in wireless networks under uncertainty," *Mobile Netw. Appl.*, vol. 16, pp. 246–254, 2011.

[29] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games for power controlled medium access with dynamic traffic," in *Proc. IEEE ISIT*, 2010.

[30] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Wireless jamming attacks under dynamic traffic uncertainty," in *Proc. IEEE WIOPT*, 2010.

[31] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.

[32] R. Nelson, *The M/G/1 Queue*, pp. 283–327. New York, NY: Springer New York, 1995.

[33] F. Naghibi and J. Gross, "How bad is interference in IEEE 802.16e systems?," in *Proc, EW*, pp. 865–872, 2010.

[34] N. E. West and T. O'shea, "Deep architectures for modulation recognition," in *Proc. IEEE DySPAN*, 2017.

[35] Y. Shi *et al.*, "Deep learning for RF signal classification in unknown and dynamic spectrum environments," in *Proc. IEEE DySPAN*, 2019.

[36] T. Erpek *et al.*, "Deep learning for wireless communications," *Development and Analysis of Deep Learning Architectures*, pp. 223–266, 2020.

[37] K. Chen and L. Huang, "Age-of-information in the presence of error," in *Proc. IEEE ISIT*, 2016.

[38] M. Costa, M. Codreanu, and A. Ephremides, "On the age of information in status update systems with packet management," *Trans. Inf. Theory*, vol. 62, no. 4, 2016.

Maice Costa is a Research Assistant Professor at Virginia Tech National Security Institute. Her research interests lie at the intersection of data sciences, operations research, and communications, applying Machine Learning, and Artificial Intelligence to support decision-making. She received her Ph.D. in Electrical Engineering from the University of Maryland College Park in 2015. Her dissertation focused on the characterization of information timeliness through new metrics that describe the age of information, a concept that has since received a lot of attention for its relevance to communication and control systems. Dr. Costa is the recipient of a Distinguished Graduate Fellowship from the James Clark School of Engineering, as well as the DAAD RISE Professional Scholarship for training in Germany. She was a visiting researcher at the University of Oulu, Finland, an intern at Bell Labs Stuttgart, Germany, and a postdoctoral research fellow at Trinity College Dublin, Ireland. Prior to joining VTNSI, she was a senior research scientist at Intelligent Automation, Inc./BlueHalo, where she led several efforts at the Networks and Security Division. She is a member of IEEE and an associate editor of IEEE Open Journal of the Communications Society.

Yalin E. Sagduyu received the B.S. degree in electrical and electronics engineering from Bogazici University, Istanbul, Turkey, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, MD, USA. He is currently a Research Professor with Virginia Tech National Security Institute, Arlington, VA, USA. Prior to that, he was the Director of networks and security with Intelligent Automation, Inc./BlueHalo, Rockville, MD, USA. He is also a Visiting Research Professor with the Department of Electrical and Computer Engineering, University of Maryland. His research interests include wireless communications, networks, security, and machine learning. He is an Editor of IEEE Transactions on Communications and an Editor of IEEE Transactions on Cognitive Communications and Networking. He chaired workshops at ACM MobiCom, ACM WiSec, IEEE CNS, and IEEE ICNP. He was a Track Chair at IEEE PIMRC, IEEE GlobalSIP, and IEEE MILCOM, and served in the Organizing Committee of IEEE GLOBECOM and IEEE MILCOM. He was the recipient of IEEE HST 2018 Best Paper Award. He is a Senior Member of IEEE.