Eavesdropping and Jamming via Pilot Attacks in 5G Massive MIMO

Marc Bernice Angoue Avele, Darian Pérez-Adán, and Dariel Pereira-Ruisánchez

Aerospace Technology research group, University of Vigo, 36310 Vigo, Spain.
Department of Computer Engineering & CITIC Research Center, University of A Coruña, Spain.
Correspondence: marcbernice.angoue@uvigo.gal

DOI: *https://doi.org/10.17979/spudc.000024.02*

Abstract: In this work, we investigate pilot attacks for 5G single-cell multi-user massive multiple-input multiple-output (MaMIMO) systems with a single-antenna active eavesdropper and a single-antenna jammer operating in time-division duplex (TDD) schemes. Firstly, we describe the attacks when the base station (BS) estimates the channel state information (CSI) based on the uplink pilot transmissions. Finally, we propose a reinforcement learning (RL)-based framework for maximizing the system sum rate that proved robust to the eavesdropping and jamming attacks.

1 Introduction

5G is the name given to the next generation of wireless connectivity, which cellular phone companies are deploying worldwide due to the large demand for high data rates and low latency in mobile service. It is slated to succeed the existing 4G networks, which currently serve as the backbone for most contemporary mobile devices Zhang et al. (2020). All 5G wireless devices are connected to the Internet network by radio waves via an antenna in the cell. Some of the key technologies to be deployed in 5G technology are MaMIMO, device-to-device (D2D) communications, intelligent reflecting surfaces (IRS), and millimeter-wave (mmWave) Perez-Adan et al. (2021). massive multiple-input multiple-output (MaMIMO) is a key 5G technology, which refers to deploying a vast number of antennas at the base stations (BSs) to support multiple users at the same time-frequency resources. MaMIMO has the potential to concentrate the radiation energy in the expected direction by using precoding algorithms, and thus the inter-cell interference can be reduced Wang et al. (2021). Due to the large number of antennas at the BSs and the relatively short channel coherence time, the channel state information (CSI) between the BS and individual users must be frequently estimated by using uplink pilot transmissions Wang et al. (2021). However, the security aspects of MaMIMO systems remain relatively unexplored. Among the critical concerns within MaMIMO systems is the pilot contamination (PC) attack, often referred to simply as a pilot attack Akgun et al. (2018). As a preliminary attempt, the work in Akgun et al. (2018) approaches an important attack scenario, in which a malicious user may send false CSI feedback to a target BS to jam or eavesdrop on messages received by other benign users. Thus leading to corruption in the signal transmitted between the communication ends. In this work, we briefly overview the eavesdropping and jamming attacks in 5G MaMIMO systems and approach reinforcement learning (RL)-based solutions to detect/mitigate communication intrusions.

1.1 Organization

The remainder of this work is structured as follows. We describe the system model and the attacks in Section 2 and Section 3, respectively. In Section 4, we briefly overview RL solutions to detect intrusions and propose an RL-based solution for the precoding design. Simulation results and comparisons are presented in Section 5. Finally, Section 6 is devoted to the conclusions of the paper.

2 System model

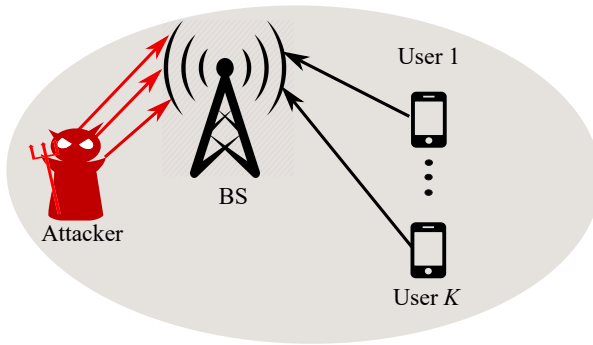


Figure 1: Pilot attack model in a multi-user (K users) uplink MaMIMO system.

Let us consider a MaMIMO system as shown in Figure 1, where a BS is equipped with M antennas to communicate with K single-antenna users, such that $M \gg K$. On the other hand, an attacker (the red devil) is trying to eavesdrop or jam the transmissions between the users and BS. We assume a time division duplex time-division duplex (TDD) system and channel reciprocity holds for coherence time. In MaMIMO systems, the BS needs the channel response of the user terminal to get the estimate of the channel. The TDD protocol establishes that the user sends an uplink pilot sequence which is used by the BS to estimate the CSI for that user in that cell. The BS employs this CSI to estimate the uplink data and for the beamforming design in downlink transmissions.

3 Attack description

The MaMIMO CSI estimation phase is vulnerable to malicious attacks, which can be classified into two forms: Pilot active eavesdropping attack and pilot jamming attack. In the following, we describe both forms of attack and state the corresponding signal model.

3.1 Pilot active eavesdropping attack

Pilot active eavesdropping attacks occur during the uplink. A user transmits a pilot symbol to the BS for channel estimation, and the BS transmits a precoded signal toward the users. At the same time as the uplink pilot transmission, the eavesdropper starts an attack by sending another pilot symbol with the basic assumption that it has the perfect knowledge of the user's pilot symbol and the exact time to transmit. It means that the attacker is synchronized with the legitimate transmission, and this is possible by overhearing the signaling exchange between the BS and the users.

Let $\mathbf{h}_k \in \mathbb{C}^{M\times 1}$ and $\mathbf{h}_{\mathrm{E}} \in \mathbb{C}^{M\times 1}$ be the column vectors representing the uplink channels from the legitimate user (k-th) and eavesdropper to BS, respectively. The elements in $\mathbf{h}_k$ and

$\mathbf{h}_{\mathrm{E}}$ follow a Rayleigh fading model. To estimate the channel response, each user sends a pilot symbol $x_{\mathrm{k},i}$ which is exactly known by the BS. The received pilot at the i-th time instant with $i = 1, \ldots, L$ and without eavesdropping can be expressed as

$$\mathbf{y}_i = \sum_{k=1}^{K} \sqrt{P_k}\mathbf{h}_k x_{k,i} + \mathbf{n}_i, \tag{2.1}$$

where $\mathbf{y}_i$ and $\mathbf{n}_i$ are the $M \times 1$ vectors of received signal and noise, respectively, P_k is the power transmission available in the K users. The vector $\mathbf{n}_i$ contains the additive white Gaussian noise (AWGN) modeled as $\mathbf{n} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{\mathrm{n}}^2 \mathbf{I}_M)$. The received signal after L pilot transmissions can be stated as

$$\mathbf{Y} = \sum_{k=1}^{K} \sqrt{P_k}\mathbf{h}_k \mathbf{x}_k + \mathbf{N}, \tag{2.2}$$

where $\mathbf{x}_k \in \mathbb{C}^{1\times L}$ is the block of L symbols corresponding to pilot transmission from the k-th user and $\mathbf{N}$ is the $M \times L$ AWGN matrix. Under a prior knowledge of $\mathbf{x}_k$, the estimated channel (without eavesdropping) would be

$$\hat{\mathbf{h}}_k = \frac{\mathbf{Y}\mathbf{x}_k^*}{\sqrt{P_k}L} = \sum_{i=1}^{K} \frac{\sqrt{P_i}\mathbf{h}_i \mathbf{x}_i \mathbf{x}_k^*}{\sqrt{P_k}L} + \frac{\mathbf{N}\mathbf{x}_k^*}{\sqrt{P_k}L} = \mathbf{h}_k + \tilde{\mathbf{n}}_k, \tag{2.3}$$

with $\tilde{\mathbf{n}}_k \triangleq \frac{\mathbf{N}\mathbf{x}_k^*}{\sqrt{P_k}L} \sim \mathcal{CN}\left(0, \frac{1}{P_k L}\mathbf{I}_M\right)$

If the eavesdropper is active (i.e., it synchronously sends the same pilot sequence as the target users), the pilot-based channel estimation will also contain the component of the eavesdropper to the BS, hence the received signal at the BS is written as

$$\mathbf{Y} = \sum_{k=1}^{K} \sqrt{P_k}\mathbf{h}_k \mathbf{x}_k + \sqrt{P_{\mathrm{E}}}\mathbf{h}_{\mathrm{E}} \mathbf{x}_j + \mathbf{N}, \tag{2.4}$$

where $\mathbf{x}_j$ is the signal sent from the attacker and P_{E} is the attacker power. $\mathbf{Y}$ is the $M \times L$ matrix containing the pilots received by M antennas at BS. We use the model of $\mathbf{x}_j$ by considering that $\mathbf{x}_j = \sqrt{P_{\mathrm{E}}} \sum_{k=1}^{K} \mathbf{x}_k$, as in the reference Akgun et al. (2017). In this case, the estimated channel for the k-th user will be given by Akgun et al. (2017)

$$\hat{\mathbf{h}}_k = \mathbf{h}_k + \tilde{\mathbf{n}}_k + \sqrt{\alpha_k}\mathbf{h}_{\mathrm{E}}, \tag{2.5}$$

where $\alpha_k = P_{\mathrm{E}}/P_{\mathrm{k}}$ is the ratio between the average power at the attacker and the power allocated by the k-th user to the pilot.

The active eavesdroppers aim to disturb the functioning of the network. Specifically, the eavesdropper's aims are the following

- Exploit the weaknesses in the user capacity-optimized pilot sequence design to increase the pilot attacks within the uplink channel estimation.
- Degrade the user signal-to-interference-plus-noise ratio (SINR) to a point where it cannot meet its requirements, even with a large number of antennas at the BS.

3.2 Pilot jamming attack

By considering the uplink of a single-cell MaMIMO system, depicted in Figure 1, let us consider now a single-antenna jammer (the red devil). During the uplink, the users send to the BS a pilot sequence, and an attacker, in this case, sends a jamming signal to interfere with the channel estimation, and it can adopt a strategy according to its knowledge of the system:

- If the jammer does not have prior knowledge of the pilot sequences used by the user, then it will send a random sequence to attack the system Do et al. (2016). It means that during the uplink, the user sends a pilot sequence, while the jammer sends a random jamming sequence. where $\mathbf{n}_j$ is a pseudorandom noise pilot transmitted by the jamming.
- The jammer has prior knowledge of the pilot sequences used by the users, and it can know the transmission protocol and the pilot set. The jammer can obtain this information by listening to the channel for some consecutive blocks.

In any case, this attacker transmits a random jamming sequence. Therefore, the signal received by the BS in (2.4) would be written as

$$\mathbf{Y} = \sum_{k=1}^{K} \sqrt{P_k}\mathbf{h}_k\mathbf{x}_k + \sqrt{P_{\mathrm{E}}}\mathbf{h}_{\mathrm{E}}\mathbf{n}_j + \mathbf{N}, \tag{2.6}$$

and the estimated channel in (2.5) for the k-th user will be a highly distorted version of $\mathbf{h}_k$ due to the noise transmitted by the attacker.

Since one of the main advantages of MaMIMO is achieving high spectral efficiency, the jammer, by launching a pilot attack, will degrade the asymptotic spectral efficiency of the legitimate system Do et al. (2016). In Vinogradova et al. (2016) is shown that if the jammer smartly adjusts its transmission power to match the desired signals, the spectral efficiency is significantly affected.

4 Technical solution

In this section, we discuss a possible technical solution for mitigating pilot attacks in 5G MaMIMO systems. We proposed a method to deal with pilot attacks using RL-based solutions. In particular, we aim to maximize the system sum rate in the downlink system by considering an active eavesdropper or a jamming signal. RL is one of the three primary machine learning (ML) paradigms, alongside supervised and unsupervised learning. In this area of ML, the agent is given a reward for taking actions that lead to desired outcomes. Over time, the agent learns to take actions that maximize the notion of cumulative reward. Some works are approached in the literature to detect communication intrusions. The work in Tu et al. (2021) proposes an RL-based technique to detect impersonation attacks in device-to-device (D2D) communications. They formulate this task as a Markov decision process and learn the optimal policy for detecting impersonation attacks. The authors in Sedjelmaci (2020) propose an RL-based approach to detect attacks in 5G wireless networks. The approach uses a hierarchical RL algorithm to learn the optimal policy to detect attacks.

4.1 RL-based solution

In this subsection, we develop a solution for active eavesdropping and jamming mitigation based on RL. We model a sum-rate maximization problem and design the downlink precoders by considering RL-based optimization.

4.2 Downlink transmission under active eavesdropping

Let s_k be the information signal sent to the k-th user from the BS, which is previously precoded with $\mathbf{v}_k \in \mathbb{C}^{M\times 1}$.

$$y_k = \sum_{i=1}^{K} \sqrt{P_i{}^{(d)}}\mathbf{h}_k^{*}\mathbf{v}_i s_i + n_k^{(d)}, \tag{2.7}$$

where $P_k^{(d)} = \mathbf{v}_k^* \mathbf{v}_k$ and $n_k^{(d)}$ are the allocated power to s_k at BS and the downlink AWGN signal. The achievable rate for the k-th user can be defined as follows by assuming $\sigma_{\mathrm{n}}^2 = 1$

$$R_k = \log\left(1 + \frac{P_k{}^{(d)} \mid \hat{\mathbf{h}}_k^* \mathbf{v}_k \mid^2}{\sum_{l \in \mathcal{K}/k} P_l{}^{(d)} \mid \hat{\mathbf{h}}_l^* \mathbf{v}_l \mid^2 + 1}\right). \tag{2.8}$$

Note that the following sum-rate maximization problem can be addressed to determine the downlink precoders and the power allocation

$$\begin{aligned} \left[\mathbf{v}_1^* \cdots \mathbf{v}_K^*\right] &= \underset{\mathbf{v}_k, \forall k \in \mathcal{K}}{\arg\max} \sum_{k=1}^{K} R_k \\ \text{s.t.} \sum_{k=1}^{K} \mathbf{v}_k^* \mathbf{v}_k &\leqslant P_{\mathrm{A}}, \end{aligned} \tag{2.9}$$

being $P_{\mathrm{A}} \geqslant \sum_{k=1}^{k} P_k^{(d)}$ the total power available at the BS with SNR (dB) $= 10 \log_{10}(P_{\mathrm{A}})$. However, note that the channel estimation is corrupted by the active eavesdropper or the jamming attacker (cf. (2.5)).

Due to the cost function and the design constraints for the precoders, the formulation in (2.9) becomes a non-trivial optimization problem. Besides, handling the eavesdropping/jamming scenario without knowing the statistics of the CSI errors is a cumbersome task. We propose an RL-based solution to solve (2.9) by leveraging the learning capabilities of neural networks.

State, action, and reward function

The state, action, and reward elements that we consider to solve 2.9 are the following. The **state** vector $\mathbf{t}_\ell$ is constructed as $\mathbf{t}_\ell = [\hat{\mathbf{h}}_1^*, ..., \hat{\mathbf{h}}_K^*]$. Notice that the states stack the information related to the channel realizations (BS-users). The action vector is composed of the vectors that we are optimizing (i.e., the precoders), such that $\mathbf{a}_\ell = [\mathbf{v}_1^*, ..., \mathbf{v}_K^*]$. Finally, the reward function will be defined by

$$r_\ell = \sum_{i=1}^{K} R_k \Big| (\mathbf{t}_\ell, \mathbf{a}_\ell). \tag{2.10}$$

Algorithm 1 DCB-DDPG algorithm

Initialize:
set $\pi(\mathbf{s}, \boldsymbol{\vartheta}_\pi)$ with random $\boldsymbol{\vartheta}_\pi$
set $r(\mathbf{s}, \mathbf{a}, \boldsymbol{\vartheta}_r)$, $r(\mathbf{s}, \mathbf{a}, \tilde{\boldsymbol{\vartheta}}_r)$ with $\boldsymbol{\vartheta}_r = \tilde{\boldsymbol{\vartheta}}_r$ and set the buffer $\mathcal{R}$
for $\ell = 0, \ldots, T-1$ **do:**
  set $\mathbf{t}_\ell$ given $\hat{\mathbf{h}}_{\mathrm{k}}, \forall k$
  agent takes $\mathbf{a}_\ell = \pi(\mathbf{s}_\ell, \boldsymbol{\vartheta}_\pi) + \mathbf{n}_{\mathrm{e}}$
  environment returns r_ℓ
  $\mathcal{R}$ stores $\mathcal{E}_\ell = (\mathbf{s}_\ell, \mathbf{a}_\ell, r_\ell)$
  if $|\mathcal{R}| > |\mathcal{B}|$:
    Sample $|\mathcal{B}|$ random experiences $\mathcal{E}_i = (\mathbf{s}_i, \mathbf{a}_i, r_i)$, $i = 0, \ldots, |\mathcal{B}| - 1$
    Compute L_{c} and backpropagate to update $\boldsymbol{\vartheta}_r$
    Compute L_{a} and backpropagate to update $\boldsymbol{\vartheta}_\pi$
    $\tilde{\boldsymbol{\vartheta}}_r \leftarrow \tau \boldsymbol{\vartheta}_r + (1-\tau)\tilde{\boldsymbol{\vartheta}}_r$
  end if
Obtain $\mathbf{v}_k, \forall k$ by evaluating $\pi(\mathbf{s}, \boldsymbol{\vartheta}_\pi)$

Output: $[\mathbf{v}_1^* \cdots \mathbf{v}_K^*]$

In the algorithmic solution, we use a deep contextual bandit-oriented deep deterministic policy gradient (DCB-DDPG) agent similar to the one approached in Pereira-Ruisánchez et al. (2023). Similar structures are employed for the neural networks in the actor and critic networks but proper adaptations have been performed for the dimensions of the state vectors.

The proposed agent is composed of the actor-network $\pi(\mathbf{t}, \boldsymbol{\vartheta}_\pi)$, the critic network $r(\mathbf{t}, \mathbf{a}, \boldsymbol{\vartheta}_r)$, the target critic network $r(\mathbf{t}, \mathbf{a}, \tilde{\boldsymbol{\vartheta}}_r)$, and the replay buffer $\mathcal{R}$. Note that $\boldsymbol{\vartheta}_\pi$ and $\boldsymbol{\vartheta}_r$ are vectors of weights of the actor and critic network, respectively. The actor and critic networks are trained from stored experiences. We compute the critic and the actor losses as

$$L_{\mathrm{c}} = \frac{1}{|\mathcal{B}|} \sum_i (r_i - r(\mathbf{s}_i, \mathbf{a}_i, \boldsymbol{\vartheta}_r))^2 \tag{2.11}$$

and

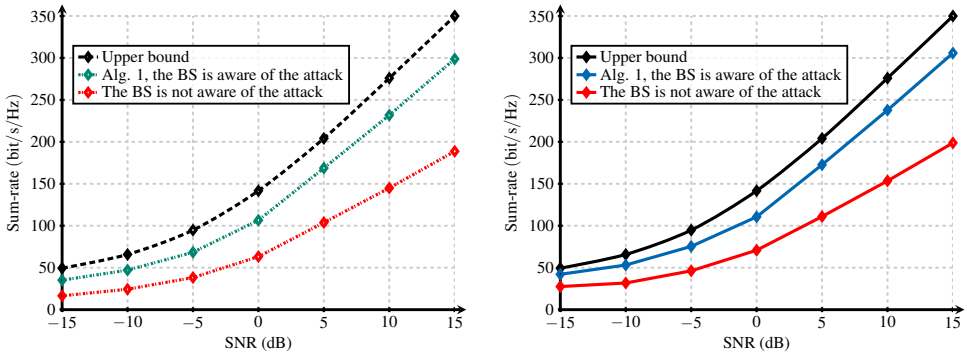
$$L_{\mathrm{a}} = -\frac{1}{|\mathcal{B}|} \sum_i r(\mathbf{s}_i, \pi(\mathbf{s}_i, \boldsymbol{\vartheta}_\pi), \tilde{\boldsymbol{\vartheta}}_r), \tag{2.12}$$

respectively. The exploration noise is defined as $\mathbf{n}_{\mathrm{e}} \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{\mathrm{n_e}}^2 \mathbf{I}_{D_{\mathrm{action}}})$. Algorithm 1 summarizes the interactions between these elements during the training stage.

5 Simulation results

In this section, we present computer experiments to analyze the capability of the proposed DCB-DDPG to solve the optimization problem in (2.9) while considering active eavesdropping and jamming. We have previously approached the active eavesdropping scheme, however, note that the jamming scenario can be easily modeled by considering (2.6) instead of (2.4). We have considered a multi-user MaMIMO setup with $K = 10$ single-antenna users and $M = 400$ antennas at the BS, where a single-antenna eavesdropper or jammer has attacked during the pilot transmission. The number of pilot symbols in the CSI estimation is set to $L = 20$.

The values of the training steps ($T = 100000$) and the size of the replay buffer, $|\mathcal{R}|_{\max}$, were selected to fit the intended training time. The mini-batch is defined as $|\mathcal{B}| = 16$ whereas the exploration noise variance is set to $\sigma_{\mathrm{n_e}}^2 = 0.05$. The remaining parameters were obtained experimentally to provide the highest system performance.



(a) Active eavesdropping attack.

(b) Jamming attack.

Figure 2: Sum rate by considering $K = 10$ users, $M = 400$ antennas at the BS, $L = 20$ pilot symbols, and different strategies to configure the precoders and power allocation.

Figure 2 shows the achievable sum rates obtained with the proposed algorithm and two baseline strategies: 1-) an upper bound strategy without eavesdropping or jamming; 2-) a lower bound (non-robust) strategy where the BS disregards the effects of active eavesdropping or jamming attack. As shown, the performance of the proposed algorithm comes close to the upper bound scheme while offering large gains over the non-robust strategy for both scenarios active eavesdropping (Figure 2(a)) and jamming (Figure 2(b)) attacks. It is also observed that slightly higher system performance is achieved with our proposed RL-based solution under the jamming attacker scenario over that assessed under the active eavesdropping attack.

6 Conclusions

In this paper, we have briefly discussed the eavesdropping and jamming pilot attacks in 5G massive MIMO. We have also proposed an RL-based system design to deal with active eavesdropping and jamming in the downlink of a multi-user massive MIMO system. The results show large gains (in terms of sum rate) provided by the proposed solution over a baseline strategy that neglects the effects of the attacker in the channel estimation process in the communication system.

Acknowledgments

CITIC is funded by the Xunta de Galicia through the collaboration agreement between the Consellería de Cultura, Educación, Formación Profesional e Universidades and the Galician universities for the reinforcement of the research centres of the Galician University System (CIGUS).

Bibliography

B. Akgun, M. Krunz, and O. O. Koyluoglu. Pilot contamination attacks in massive MIMO systems. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2017.

B. Akgun, M. Krunz, and O. O. Koyluoglu. Vulnerabilities of massive MIMO systems to pilot contamination attacks. *IEEE Trans. Inf. Forensics Secur.*, 14(5):1251–1263, 2018.

T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund. Massive MIMO pilot retransmission strategies for robustification against jamming. *IEEE Wireless Commun. Lett.*, 6 (1):58–61, 2016.

D. Pereira-Ruisánchez, O. Fresnedo, D. Pérez-Adán, and L. Castedo. Deep contextual bandit and reinforcement learning for IRS-assisted MU-MIMO systems. *IEEE Transactions on Vehicular Technology*, 72(7):9099–9114, 2023. doi: 10.1109/TVT.2023.3249353.

D. Perez-Adan, O. Fresnedo, J. P. Gonzalez-Coma, and L. Castedo. Intelligent reflective surfaces for wireless networks: An overview of applications, approached issues, and open problems. *Electronics*, 10(19):2345, 2021.

H. Sedjelmaci. Attacks detection approach based on a reinforcement learning process to secure 5g wireless network. In *IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2020.

S. Tu, M. Waqas, S. U. Rehman, T. Mir, G. Abbas, Z. H. Abbas, Z. Halim, and I. Ahmad. Reinforcement learning assisted impersonation attack detection in device-to-device communications. *IEEE Transactions on Vehicular Technology*, 70(2):1474–1479, 2021.

J. Vinogradova, E. Björnson, and E. G. Larsson. Detection and mitigation of jamming attacks in massive mimo systems using random matrix theory. In *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2016.

Z. Wang, D. Shi, and H. Wu. The role of massive MIMO and intelligent reflecting surface in 5g/6g networks. In *2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, pages 309–312. IEEE, 2021.

X. Zhang, X. Liu, G. Wei, Y. Zhao, and Y. Guo. The study of 5G massive MIMO end-to-end MPAC test solution. In *14th European Conference on Antennas and Propagation (EuCAP)*, pages 1–5. IEEE, 2020.