IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 April 2022, accepted 29 June 2022, date of publication 6 July 2022, date of current version 15 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3188876

RESEARCH ARTICLE

Performance Analysis of Signature-Based Grant-Free Random Access Under Impersonation Attacks

NAM YUL YU, (Senior Member, IEEE)
School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology (GIST), Gwangju 61005, South Korea
e-mail: nyyu@gist.ac.kr

This work was supported in part by the National Research Foundation of Korea (NRF) Grant through the Korea Government (MSIT) under Grant NRF-2021R1F1A1046282, and in part by the GIST Research Project grant funded by the GIST in 2022.

ABSTRACT In massive machine-type communications (mMTC), user-specific and non-orthogonal signatures can be assigned to wireless devices for uplink grant-free access. In this paper, we analyze the performance of signature-based grant-free random access in the presence of an adversary. To enhance the access security, we assume that an mMTC system renews the signatures of legitimate devices at each access secretly between the devices and a base station (BS). To gain unauthorized access to this mMTC system, we assume that the adversary attempts to impersonate legitimate devices by sending malicious signatures to the BS. By this impersonation attack, the adversary takes a chance to modify the data transmitted from legitimate devices and/or inject false data to the system. Moreover, this attack may deteriorate the performance of activity detection of legitimate devices through jamming. Under this scenario, we investigate the impacts of this impersonation attack on the performance of signature-based grant-free access theoretically and numerically, with respect to data modification, false authentication, and jamming.

INDEX TERMS Grant-free access, impersonation attacks, massive machine-type communications (mMTC), signatures.

I. INTRODUCTION

Massive machine-type communications (mMTC) aims to connect a massive number of wireless devices with low latency, low control overhead, and low power consumption for delay-sensitive, energy efficient, and secure communications [1], [2]. Through massive connectivity, mMTC provides a concrete platform for the Internet of Things (IoT). In an mMTC cell, non-orthogonal signature sequences can be uniquely assigned to all devices for massive connectivity [3], [4]. Also, grant-free access is considered for reducing signaling overhead and achieving low latency in uplink access. Allowing multiple devices to share common resources non-orthogonally with low signaling overhead, uplink grant-free access is of paramount interest for enabling low latency and high energy efficiency in mMTC [5].

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

Unfortunately, grant-free access is inherently vulnerable to potential attacks from an adversary, due to openness of wireless channels and non-discriminating access of devices. For instance, an adversary may intercept messages from legitimate devices by eavesdropping, which breaks the data confidentiality [6]. Also, an adversary pretends to be legitimate to gain unauthorized access to a system, breaking the device integrity. Moreover, an adversary can disrupt wireless access of legitimate devices by transmitting jamming signals. Several techniques have been proposed to prevent eavesdropping [7], [8], verify the legitimacy of devices [9]–[11], and mitigate jamming attacks [12]–[14], in an effort to enhance the security of wireless access. Readers are referred to [15]–[17] for surveys on challenges and threats to wireless access at physical layer.

In signature-based grant-free random access, a connection of wireless devices can be tampered by an adversary's attempt to impersonate legitimate devices. In specific, an adversary may attempt to gain unauthorized access to an mMTC system

by sending some legitimate signatures to a base station (BS). If it succeeds in the impersonation attack, the adversary takes a chance to modify the data transmitted from legitimate devices and/or inject false data to the system. Also, the adversary may deteriorate the performance of activity detection of legitimate devices by introducing jamming. To the best of our knowledge, no studies have been reported for scrutinizing the impacts of this impersonation attack on signature-based grant-free access.

In [18], a conceptual code-based authentication has been studied with a codebook and its randomly chosen subset, where the knowledge of the subset is a secret shared by a sender and its recipient. Inspired by this idea, we assume a signature-based grant-free access in which unique signatures are assigned and renewed secretly for legitimate devices. In specific, a set of all possible signatures is defined as a codebook, where a subset is randomly chosen at each access. Then, the signatures of the subset are uniquely assigned to all legitimate devices in an mMTC cell. While the codebook is publicly known, the random choice of a subset for signature renewal is a secret shared by a BS and legitimate devices. At each access, a BS and all legitimate devices renew the signatures in a coordinated manner using the secret information, to prevent a potential impersonation attack from an adversary.

In this access model, we assume that an adversary will choose some signatures arbitrarily from the publicly known codebook with no knowledge of the subset of legitimate signatures. Then, it will transmit the malicious signatures to a BS to impersonate legitimate devices. To analyze the impacts of this impersonation attack, this paper first derives an upper bound on the *data modification rate*, which reflects how many malicious signatures successfully detected by a BS coincide with active legitimate ones. Due to the coincidence, the adversary takes a chance to impersonate active legitimate devices. Thus, the analysis of data modification rate gives an insight into the resilience of signature-based grant-free access against the alteration of data transmitted from legitimate devices. In addition, we develop an upper bound on the *false authentication rate*, which reflects how many malicious signatures detected by a BS coincide with legitimate, but inactive ones. This analysis shows the security against false data injection through unauthorized access of the malicious signatures. Finally, we investigate the effect of *jamming* on the performance of activity detection by evaluating the equivalent noise power from the malicious signatures not coinciding with any legitimate ones.

To evaluate the impacts of this impersonation attack, we employ the Zadoff-Chu (ZC) signature sequences [19] for signature-based grant-free random access in a single mMTC cell. Simulation results demonstrate that if the number of malicious signatures is not too large, the data modification and the false authentication rates are tightly bounded by their upper bounds, respectively. As predicted by the theoretical results, we observe that the rates increase over the number of malicious signatures, but they are little affected by the adversary's total power. Also, it turns out that false authentication can be a more serious threat than data modification, against signature-based grant-free random access.

Meanwhile, the goodputs of activity detection for legitimate devices show that the adverse effect of jamming strengthens as the adversary's total power increases, but appears to be irrelevant to the number of malicious signatures, which is also in line with our theoretical result. Numerical results reveal that jamming introduces the additive, non-Gaussian distributed noise with the equivalent noise power. As the adversary moves far away from the BS, we observe that the false authentication rate drops and the goodput of legitimate devices improves, whereas the data modification rate is irrelevant to the adversary's distance from the BS.

In summary, we study the performance of signature-based grant-free random access under impersonation attacks, through theoretical analysis and extensive simulations. By investigating data modification rates, false authentication rates, and goodputs, this paper gives us an insight into the resilience of the access scheme against the impersonation attack, which is the main contribution.

Notations: In this paper, a matrix (or a vector) is represented by a bold-face upper (or a lower) case letter. $\mathbf{X}^T$ denotes the transpose of a matrix $\mathbf{X}$, while $\mathbf{X}^*$ is its conjugate transpose. $diag(\mathbf{x})$ denotes a diagonal matrix whose diagonal entries are from a vector $\mathbf{x}$. The inner product of vectors $\mathbf{x}$ and $\mathbf{y}$ is denoted by $\langle \mathbf{x}, \mathbf{y} \rangle$. The l_p-norm of $\mathbf{x}$ is denoted by $||\mathbf{x}||_p = \left(\sum_{k=1}^{N} |x_k|^p\right)^{\frac{1}{p}}$ for $1 \leq p < \infty$. The Frobenius norm of a matrix $\mathbf{X} = [X_{i,j}]$ is denoted by $\|\mathbf{X}\|_F = \sqrt{\sum_{i,j} |X_{i,j}|^2}$. A circularly symmetric complex Gaussian random vector with mean m and covariance $\mathbf{\Sigma}$ is denoted by $\mathbf{h} \sim \mathcal{CN}(\mathbf{m}, \mathbf{\Sigma})$. Finally, $\mathcal{B}(n, p)$ denotes the binomial distribution of n independent Bernoulli trials each with success probability p.

II. SYSTEM MODEL

A. UPLINK GRANT-FREE RANDOM ACCESS

In this paper, we consider a two-phase grant-free access scheme [20], [21] for single-cell massive connectivity. In an mMTC cell, a base station (BS) receiver equipped with J antennas accommodates total N devices each of which transmits with a single antenna. For a fully grant-free access, we assume that devices are *static* in a cell and thus BS accommodates a fixed set of devices having their own user-specific signatures. In the first phase, each active device transmits its signature sequence as a dedicated pilot. Then, the BS receiver tries to identify active devices and estimate their channel profiles from the superimposed pilots. In the second-phase, data can be directly transmitted from the active devices with no grant from BS. In this two-phase scheme, we assume that the channels and the device activity remain unchanged during L slots for pilot and data transmissions. Figure 1 illustrates this system model.

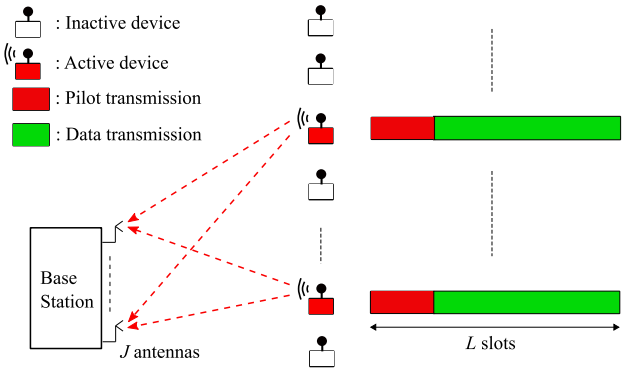

FIGURE 1. Two-phase grant-free access scheme with multiple receiver antennas.

In each access, an activity indicator vector can be defined by $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_N)^T$ with

$$\alpha_n = \begin{cases} 1, & \text{if device } n \text{ is active,} \\ 0, & \text{otherwise,} \end{cases}$$

where $\mathcal{S} = \{n \mid \alpha_n = 1\}$ is a set of active devices and the number of active devices is $|\mathcal{S}| = \sum_{n=1}^{N} \alpha_n = K \ll N$ due to sparse activity. At each access, a device is active with probability p_d in an i.i.d. manner, i.e., $\Pr[\alpha_n = 1] = p_d$. If device n is active, it transmits its unique *signature* $\mathbf{s}_n = (s_{1,n}, \ldots, s_{M,n})^T$ for grant-free random access, where $M < N$. In this paper, we assume that active devices transmit their signatures synchronously with the same transmit power ρ.

Under the flat Rayleigh fading channel, we assume that the channel gain remains unchanged during the coherence time interval of L slots. Let $\mathbf{h}_n = (h_n^{(1)}, \ldots, h_n^{(J)})^T$, $1 \le n \le N$, be a channel vector from device n, where $h_n^{(t)}$ is the channel gain between device n and the BS receiver antenna t. Then, $\mathbf{h}_n \sim \mathcal{CN}(0, \beta_n \mathbf{I})$, where the path-loss component β_n is determined by the device location from the BS. At the BS receiver, the received signal at antenna t is represented by

$$\mathbf{y}^{(t)} = \sqrt{\xi} \sum_{n=1}^{N} \alpha_n h_n^{(t)} \mathbf{s}_n + \mathbf{w}^{(t)} = \sqrt{\xi} \mathbf{S} \mathbf{x}^{(t)} + \mathbf{w}^{(t)}, \quad (1)$$

where $\xi = \rho M$ and $\mathbf{x}^{(t)} = (\alpha_1 h_1^{(t)}, \ldots, \alpha_N h_N^{(t)})^T$ for $1 \le t \le J$. In (1), $\mathbf{S} = [\mathbf{s}_1, \ldots, \mathbf{s}_N] \in \mathbb{C}^{M \times N}$ is a matrix of signature sequences, and $\mathbf{w}^{(t)} \sim \mathcal{CN}(0, \sigma_w^2 \mathbf{I})$ is the complex Gaussian noise vector at antenna t.

Collecting the received signal of (1) from J antennas, we have a multiple measurement vector (MMV) model of

$$\mathbf{Y} = \sqrt{\xi} \mathbf{S} \mathbf{X} + \mathbf{W}, \quad (2)$$

where $\mathbf{Y} = \left[\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(J)}\right]$, $\mathbf{X} = \left[\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(J)}\right]$, and $\mathbf{W} = \left[\mathbf{w}^{(1)}, \ldots, \mathbf{w}^{(J)}\right]$, respectively. Due to the activity indicator $\boldsymbol{\alpha}$, it is clear that $\mathbf{X}$ is *jointly sparse* with K nonzero and $N - K$ zero rows. To solve the MMV problem of (2), a BS can deploy a joint sparse recovery algorithm, which allows to detect the activity indicator $\boldsymbol{\alpha}$ and estimate the channel vector $\mathbf{h}_n$ for $n \in \mathcal{S}$. If the nonzero rows of $\mathbf{X}$ are estimated, the row indices mean a detected index set of active devices, denoted by $\widehat{\mathcal{S}}$, while the coefficients of each nonzero row give an estimated channel vector $\widehat{\mathbf{h}}_n$ for $n \in \widehat{\mathcal{S}}$. The compressed sensing (CS) [22] based joint active user detection (AUD) and channel estimation (CE) complete the first phase of uplink grant-free access. In the second phase, the BS receiver detects the data from the active devices, with the knowledge of device identity and channel profiles obtained from the first phase [20], [21].

Remark 1: In an MMV model, the jointly K-sparse signal $\mathbf{X}$ can be uniquely reconstructed from the noiseless measurements $\mathbf{Y} = \mathbf{S}\mathbf{X}$ if and only if [22]

$$K < \frac{\text{spark}\,(\mathbf{S}) - 1 + \text{rank}\,(\mathbf{X})}{2}, \quad (3)$$

where spark($\mathbf{S}$) is the smallest number of columns of $\mathbf{S}$ that are linearly dependent. In particular, if $\mathbf{X}$ is full rank or rank($\mathbf{X}$) $= K$ and spark($\mathbf{S}$) takes on its largest possible value of $M + 1$, the condition of (3) becomes $M \ge K + 1$. This implies that the MMV problem of (2) requires the signature length to be at least $M = K + 1$ for unique reconstruction of $\mathbf{X}$ in noiseless CS-based AUD and CE.

B. SIGNATURE SET STRUCTURE

To prevent adversary's unauthorized access, we assume that a BS and mMTC devices collaborate to renew the legitimate signatures at each access. Let $\mathcal{T}$ be a set of all available signatures, which is a publicly known codebook with $|\mathcal{T}| = T$. At each access, the signatures of a randomly chosen subset $\mathcal{N} = \{\mathbf{s}_1, \ldots, \mathbf{s}_N\} \subset \mathcal{T}$ are uniquely assigned to all legitimate devices in a cell, where we define the *legitimate signature rate* by $r_d = N/T$. In uplink grant-free access, active devices transmit their own signatures, which form a subset $\mathcal{K} \subset \mathcal{N}$. Note that a choice of $\mathcal{N}$ is a secret shared by a BS and legitimate devices, whereas $\mathcal{K}$ is determined by the activity of legitimate devices, driven by sensing or observation of events in a cell. Finally, the BS receiver presents an estimate of $\mathcal{K}$, or $\widehat{\mathcal{K}}$, through activity detection in the first-phase of access.

With the renewal of legitimate signatures, we assume that an adversary's strategy for impersonating legitimate devices is to choose a set of distinct signatures arbitrarily from the publicly known $\mathcal{T}$, denoted by $\mathcal{A} \subset \mathcal{T}$, where $|\mathcal{A}| = n_a$. In an access attempt, the adversary transmits n_a signatures of $\mathcal{A}$ by multiplexing them, where the *malicious signature rate* is defined by $r_a = n_a/T$. If some of the n_a malicious signatures are successfully detected by a BS, the adversary has a chance to gain access to the mMTC system in the first-phase of access. Then in the second-phase, malicious data transmission from the adversary can disrupt the data of legitimate devices or inject false data to the system. If some malicious signatures do not fall into $\mathcal{N}$ in the first-phase of access, their transmission will cause jamming instead, which deteriorates the performance of activity detection for legitimate devices at a BS. Figure 2 illustrates the structure of signature sequence sets for legitimate and malicious devices, as described above.

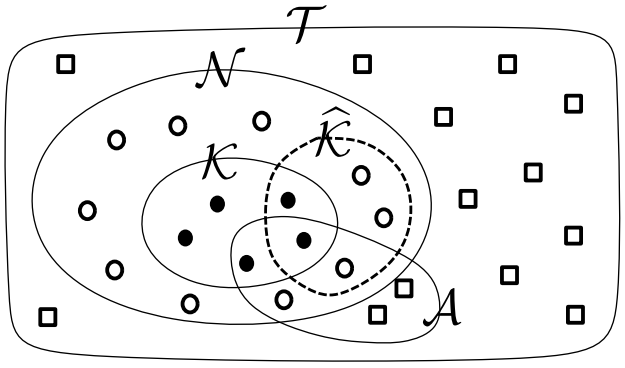

FIGURE 2. Set structure of signature sequences at an access time. Each square denotes a signature sequence not assigned to any devices, while each circle indicates a signature sequence assigned to devices in an mMTC cell. The black-filled circles correspond to signature sequences of active devices.

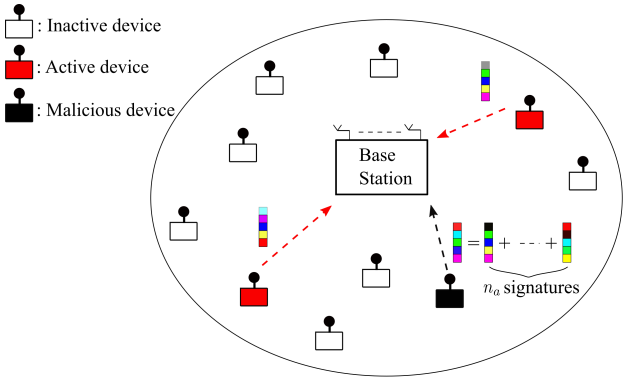

FIGURE 3. Signature-based uplink grant-free access model with impersonation attacks.

As an example of the signature set, we can employ the Zadoff-Chu (ZC) sequences [19]. Each ZC sequence of prime length M is given by $\mathbf{z}^{(u,\theta)} = (z_1^{(u,\theta)}, \ldots, z_M^{(u,\theta)})^T$, where

$$z_m^{(u,\theta)} = \frac{1}{\sqrt{M}} \exp\left(-j\frac{\pi u(m-1+\theta)(m+\theta)}{M}\right), \quad (4)$$

for $m = 1, \ldots, M$. In (4), $\mathbf{z}^{(u,\theta)}$ is a θ-cyclic shift of the uth-root ZC sequence of length M, where $0 \le \theta \le M-1$ and $1 \le u \le M-1$. Therefore, total $T = M(M-1)$ ZC sequences are available for the signature set $\mathcal{T}$ from all pairs of θ and u. For signature renewal, a legitimate device can generate its unique ZC sequence by creating u and θ in a pseudorandom manner. For this purpose, a pseudorandom number generator (PRNG) [23] can be implemented for each device to produce an integer I_n, $0 \le I_n \le T-1$, where $u = \lfloor \frac{I_n}{M} \rfloor + 1$ and $\theta \equiv I_n \pmod{M}$ for $n = 0, \ldots, N-1$. Note that the PRNGs of all devices must operate secretly in a coordinated manner, to ensure that the secrets $I_0, \ldots, I_{N-1}$ are distinct and shared by the BS. The ZC sequences, adopted as preambles for random access in 3GPP-LTE [24], can be suitable for non-orthogonal signatures in uplink grant-free access, since each one has zero autocorrelation [19] and good power spectral characteristics [25], and each pair has theoretically bounded low correlation [26].

Remark 2: In signature renewal, one may consider a codebook $\mathcal{T}$ of randomly generated signatures, which can make the codebook size T extremely large. For example, if the elements of signatures are Gaussian or Bernoulli distributed, we can create a huge number of signatures for a codebook $\mathcal{T}$ by increasing the seed size of the element generator. Then, the adversary's strategy of choosing $\mathcal{A}$ arbitrarily from $\mathcal{T}$ is not likely to succeed for the impersonation attack, since the sample space for the choice is enormous. However, it is difficult for randomly generated signatures to meet some desired properties, e.g., low correlation, low peak power, low implementation cost, etc., for practical applications. Therefore, this paper assumes to use the deterministic ZC signature sequences, which are more suitable for practical mMTC. Also, other deterministic signatures can be considered for our analysis.

C. ATTACK MODEL

For an impersonation attack, we assume that an adversary locates a single malicious mMTC device in a cell. The malicious device transmits a multiplexed sequence of n_a distinct signatures from $\mathcal{A}$ with the transmit power ρ_m at each access. Assuming that the adversary distributes the total transmit power ρ_m equally over the signatures, it is equivalent to transmitting the n_a signatures individually with each transmit power $\rho_a = \frac{\rho_m}{n_a}$. Figure 3 illustrates this attack model.

Under this attack, the MMV model of (2) is changed to

$$\mathbf{Y} = \sqrt{\xi}\mathbf{S}\mathbf{X} + \sqrt{\xi_a}\mathbf{S}_a\mathbf{X}_a + \mathbf{W} \quad (5)$$

where $\xi_a = \rho_a M$. In (5), $\mathbf{S}_a = [\mathbf{S}, \mathbf{S}'] \in \mathbb{C}^{M\times T}$ contains all signatures of a publicly known codebook $\mathcal{T}$ as its columns, where $\mathbf{S} \in \mathbb{C}^{M\times N}$ and $\mathbf{S}' \in \mathbb{C}^{M\times(T-N)}$ have the signatures of $\mathcal{N}$ and $\mathcal{T} \setminus \mathcal{N}$, respectively. Also, $\mathbf{X}_a \in \mathbb{C}^{T\times J}$ is a jointly sparse matrix with n_a nonzero rows, which correspond to the n_a signatures of $\mathcal{A}$. In $\mathbf{X}_a$, the n_a nonzero elements of each column are identical, since each one is the channel gain between the single malicious device and a BS antenna.

From Fig. 2, we define signature subsets $\mathcal{A}_\mathsf{M} = \mathcal{A} \cap \mathcal{K}$, $\mathcal{A}_\mathsf{F} = \mathcal{A} \cap (\mathcal{N} \setminus \mathcal{K})$, and $\mathcal{A}_\mathsf{J} = \mathcal{A} \cap (\mathcal{T} \setminus \mathcal{N})$, respectively. Then, the channel gain matrix $\mathbf{X}_a$ can be rewritten as $\mathbf{X}_a = \left[(\mathbf{X}_\mathsf{M} + \mathbf{X}_\mathsf{F})^T, \mathbf{X}_\mathsf{J}^T\right]^T$, where the nonzero row elements of $\mathbf{X}_\mathsf{M} \in \mathbb{C}^{N\times J}$, $\mathbf{X}_\mathsf{F} \in \mathbb{C}^{N\times J}$, and $\mathbf{X}_\mathsf{J} \in \mathbb{C}^{(T-N)\times J}$ correspond to the channel gains for signatures in $\mathcal{A}_\mathsf{M}$, $\mathcal{A}_\mathsf{F}$, and $\mathcal{A}_\mathsf{J}$, respectively. From the structure of $\mathbf{S}_a$ and $\mathbf{X}_a$, (5) is rewritten as

$$\begin{aligned}\mathbf{Y} &= \sqrt{\xi}\mathbf{S}\mathbf{X} + \sqrt{\xi_a}\mathbf{S}\mathbf{X}_\mathsf{M} + \sqrt{\xi_a}\mathbf{S}\mathbf{X}_\mathsf{F} + \sqrt{\xi_a}\mathbf{S}'\mathbf{X}_\mathsf{J} + \mathbf{W}, \\ &= \sqrt{\xi}\mathbf{S}\widetilde{\mathbf{X}} + \widetilde{\mathbf{W}}, \end{aligned} \quad (6)$$

where $\widetilde{\mathbf{X}} = \mathbf{X} + \sqrt{\frac{\rho_a}{\rho}}\mathbf{X}_\mathsf{M} + \sqrt{\frac{\rho_a}{\rho}}\mathbf{X}_\mathsf{F}$ and $\widetilde{\mathbf{W}} = \sqrt{\xi_a}\mathbf{S}'\mathbf{X}_\mathsf{J} + \mathbf{W}$. In $\widetilde{\mathbf{W}}$, $\mathbf{W}_\mathsf{J} = \sqrt{\xi_a}\mathbf{S}'\mathbf{X}_\mathsf{J}$ is the equivalent noise from the effect of jamming. Note that the nonzero row indices of $\mathbf{X}_\mathsf{F}$ are distinct from those of $\mathbf{X}$ and $\mathbf{X}_\mathsf{M}$, respectively, due to $\mathcal{K} \cap \mathcal{A}_\mathsf{F} = \mathcal{A}_\mathsf{M} \cap \mathcal{A}_\mathsf{F} = \phi$.

Under the impersonation attack, a BS receiver has to tackle the MMV problem of (6). If a signature of $\mathcal{A}_{\mathsf{M}}$ is detected successfully from the corresponding nonzero row index of $\mathbf{X}_{\mathsf{M}}$, the malicious device has a chance to modify the data from a legitimate device of the signature in the second-phase, causing *data modification*. On the other hand, if a signature of $\mathcal{A}_{\mathsf{F}}$ is successfully detected from $\mathbf{X}_{\mathsf{F}}$, the malicious device can be authorized to access the mMTC system to inject false data in the second-phase, which causes *false authentication*. Finally, the signatures of $\mathcal{A}_{\mathsf{J}}$ introduce *jamming* to the system, which will contribute to increasing the noise level of $\widetilde{\mathbf{W}}$ in detection process of legitimate devices.

III. IMPACTS OF IMPERSONATION ATTACKS

In this section, we analyze the impacts of the impersonation attack of Section II on the performance of signature-based grant-free random access, with respect to data modification, false authentication, and jamming, which is the main contribution. In our analysis, we assume that the probability of selecting a sequence from $\mathcal{T}$ remains constant at each selection of n_a malicious signatures, due to sufficiently large T. This assumption allows to use the binomial distribution [27], which facilitates our performance analysis.

A. DATA MODIFICATION

If some signatures transmitted by the malicious device fall into $\mathcal{K}$, their identities override those of legitimate devices in activity detection of the first-phase of access. Then in the second-phase, the data transmitted from the legitimate devices can be modified by the false data from the malicious one, which destroys the *data integrity*.

Theorem 1: Let $\mathcal{A}_{\mathsf{M}} = \mathcal{A} \cap \mathcal{K}$ be a set of signatures falling into $\mathcal{K}$ out of n_a ones chosen from $\mathcal{T}$ by the malicious device. The *data modification rate* λ_m is defined by the average rate of successfully detected signatures of $\mathcal{A}_{\mathsf{M}}$ out of all detected ones in the first-phase of access. Then,

$$\lambda_m = \mathbb{E}\left[\frac{|\mathcal{A}_{\mathsf{M}} \cap \widehat{\mathcal{K}}|}{|\widehat{\mathcal{K}}|}\right] \leq r_a = \frac{n_a}{T}. \tag{7}$$

Proof: See Appendix A. □

In Theorem 1, we assumed that if a legitimate device has the signature of $\mathcal{A}_{\mathsf{M}}$, its data would be modified certainly by the adversary in the second-phase of access. However, the adversary has no idea of which signatures of $\mathcal{A}$ have been detected successfully by a BS, and thus may have to continue to distribute its total power equally over all signatures of $\mathcal{A}$ in the second-phase. Then, if n_a is very large, the data from a legitimate device of the signature in $\mathcal{A}_{\mathsf{M}}$ will be less likely to be modified in the second-phase by the malicious signature with less power $\rho_a = \frac{\rho_m}{n_a}$, which makes the actual λ_m much lower than the upper bound. In this paper, we assume that n_a is small or moderately large to maintain the assumption of Theorem 1.

B. FALSE AUTHENTICATION

In the first-phase of access, if the malicious signatures falling into $\mathcal{N} \setminus \mathcal{K}$ are successfully detected, the adversary is able to deceive the BS by disguising them as legitimate ones, which results in false authentication, destroying the *device integrity*.

Theorem 2: Let λ_f be the *false authentication rate*, defined by the average rate of successfully detected signatures of $\mathcal{A}_{\mathsf{F}} = \mathcal{A} \cap (\mathcal{N} \setminus \mathcal{K})$ out of all detected ones in the first-phase of access. Then,

$$\lambda_f = \mathbb{E}\left[\frac{|\mathcal{A}_{\mathsf{F}} \cap \widehat{\mathcal{K}}|}{|\widehat{\mathcal{K}}|}\right] \leq \frac{r_a(1-p_d)}{p_d + r_a(1-p_d)}, \tag{8}$$

where $r_a = \frac{n_a}{T}$ is the malicious signature rate and p_d is the activity rate of a legitimate device.

Proof: See Appendix B. □

Remark 3: The proof of Theorem 2 shows that the upper bound of (8) is obtained by (18) from $\alpha = p_{\mathsf{sm}}/p_{\mathsf{sg}} = 1$, where p_{sg} and p_{sm} are the probabilities that the signatures of $\mathcal{A}_{\mathsf{M}}$ and $\mathcal{A}_{\mathsf{F}}$ are successfully detected, respectively, in the first-phase of access. However, if n_a increases, a malicious signature of $\mathcal{A}_{\mathsf{F}}$ will be less likely to be detected by a BS, due to its reduced transmit power $\rho_a = \frac{\rho_m}{n_a}$. On the other hand, the signatures of $\mathcal{A}_{\mathsf{M}}$ can still be detected by the aid of signatures of $\mathcal{K}$ with sufficient power, regardless of n_a. In other words, if n_a increases, the power difference of the signatures in $\mathcal{A}_{\mathsf{F}}$ and $\mathcal{A}_{\mathsf{M}}$ may lead to $p_{\mathsf{sm}} < p_{\mathsf{sg}}$, which reduces α. Consequently, the actual λ_f may not increase over n_a indefinitely, due to the reduced α, which will be confirmed by the numerical results of Section IV.

In Theorems 1 and 2, it is noteworthy that the upper bounds are independent of a specific detection scheme at a BS. Also, it is readily checked that for given n_a, the upper bounds decrease monotonically as the codebook size T increases. Therefore, it is essential to construct the codebook $\mathcal{T}$ such that it has as many signatures as possible, to reduce the data modification and the false authentication rates from the impersonation attack.

In (6), the nonzero row indices of $\mathbf{X}$ and $\mathbf{X}_{\mathsf{F}}$ correspond to the active legitimate signatures of $\mathcal{K}$ and the malicious ones of $\mathcal{A}_{\mathsf{F}}$, respectively. As the indices do not coincide with each other due to $\mathcal{K} \cap \mathcal{A}_{\mathsf{F}} = \phi$, the malicious signatures of $\mathcal{A}_{\mathsf{F}}$ increase the number of nonzero rows of $\widetilde{\mathbf{X}}$, which can degrade the performance of CS-based activity detection of legitimate devices at a BS. In what follows, Theorem 3 analyzes the maximum number of malicious signatures of $\mathcal{A}_{\mathsf{F}}$ that increase the number of nonzero row indices of $\widetilde{\mathbf{X}}$.

Theorem 3: Let $q = r_d(1-p_d)$, where $r_d = N/T$, and p_d is the activity rate of a legitimate device. For given n_a, the number of malicious signatures at $\mathcal{A}_{\mathsf{F}}$ is at most

$$K_{\mathsf{F},\max} = \left\lfloor \frac{\log\epsilon - n_a \log e(1-q)}{\log q - \log(1-q)} \right\rfloor. \tag{9}$$

with probability exceeding $1-\epsilon$ for small $\epsilon > 0$.

Proof: See Appendix C. □

As the malicious signatures of $\mathcal{A}_{\mathsf{F}}$ increase the number of nonzero row indices of $\widetilde{\mathbf{X}}$, we also have to increase the

signature length M so that a BS receiver can identify the increased indices of $\widetilde{\mathbf{X}}$ successfully by CS-based detection. For instance, if the elements of signatures are Gaussian distributed and the number of BS antennas is sufficiently large, Remark 1 suggests that the signature length M should be increased by $K_{\mathsf{F},\max}$ even with no noise or jamming, for reliable activity detection of legitimate devices under this impersonation attack.

C. JAMMING

If some malicious signatures fall into $\mathcal{A}_{\mathsf{J}} = \mathcal{A} \cap (\mathcal{T} \setminus \mathcal{N})$, they correspond to the nonzero row indices of $\mathbf{X}_{\mathsf{J}}$. While the signatures are irrelevant to those of legitimate devices, their presence introduces jamming in (6), which degrades the performance of activity detection for legitimate devices. In what follows, we analyze the effect of jamming.

Theorem 4: In the MMV model of (6), assume that each signature is the Zadoff-Chu (ZC) sequence. Then, each column of $\mathbf{W}_{\mathsf{J}} = \sqrt{\xi_a}\mathbf{S}'\mathbf{X}_{\mathsf{J}}$ can be approximated by a noise vector of mean $\mathbf{0}$ and covariance $\mathbf{K}_{\mathsf{J}} = \sigma_{\mathsf{J}}^2\mathbf{I}$ with

$$\sigma_{\mathsf{J}}^2 = \rho_m \beta_m (1 - r_d), \tag{10}$$

where ρ_m is the adversary's total transmit power and β_m is the path-loss component determined by the adversary's distance from a BS.

Proof: See Appendix D. □

While the proof of Theorem 4 assumed a sufficiently large n_a, the numerical results of Section IV demonstrate that the approximation is valid even for a small n_a. Theorem 4 suggests that jamming causes the noise-like interference to signature-based grant-free access, where the equivalent noise power is σ_{J}^2. As a result, jamming degrades the performance of activity detection at a BS by adding the extra noise of power σ_{J}^2 equivalently in the first-phase of access. It is noteworthy that the equivalent additive noise introduced by jamming is not truly Gaussian distributed, which will be observed by the numerical results of Section IV. Theorem 4 also shows that if r_d is sufficiently low, the adversary's power mostly contributes to the noise level increase through jamming, which means that jamming is a major source for performance degradation of signature-based grant-free access by this impersonation attack. A variety of jamming mitigation techniques [12]–[14], exploiting learning, precoding, optimal filters, etc., can be employed for improving the detection performance of legitimate devices.

IV. SIMULATION RESULTS

In simulations, total $N = 500$ legitimate devices are assumed to be randomly located over the range of [0.05km, 0.5km] in an mMTC cell, where each one is active independently with probability $p_d = 0.05$. For signature-based grant-free random access, we assume that each signature is the Zadoff-Chu (ZC) sequence of length $M = 139$ in Section II.B, which forms a codebook $\mathcal{T}$ of $T = M(M-1) = 19182$ signatures. At each access, a signature set $\mathcal{N}$ of N signatures is randomly taken from the codebook $\mathcal{T}$, where each device is assigned its unique signature from $\mathcal{N}$. The path loss of the wireless channel is modeled by $\beta_n = -128.1 - 36.7\log_{10} d_n$ in dB, where d_n is the distance in km from device n to a BS. The transmit power of each active device is $\rho = 23$ dBm and the power spectral density of AWGN at the BS receiver is -169 dBm/Hz over 1 MHz.

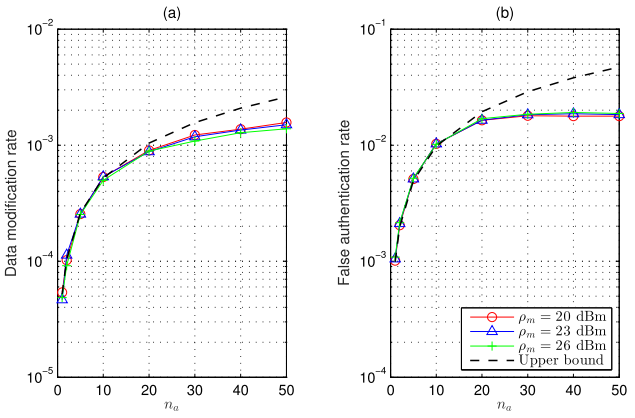

FIGURE 4. Data modification and false authentication rates over the number of malicious signatures n_a, where the malicious device is closest to the BS, located at $R_1 = 0.05$ km from it.

In this mMTC cell, we first assume that an adversary is closest to the BS, locating the malicious device at the inner cell boundary of $R_1 = 0.05$ km. The performance analysis under this assumption can give us an insight into the impacts of attack in the *worst-case* scenario. Later, we investigate the impacts depending on the distance from the BS by moving the position of the malicious device inside the cell.

In the presence of legitimate and malicious devices, a BS receiver with $J = 64$ antennas tries to identify active ones by solving the MMV problem of (6) through the simultaneous orthogonal matching pursuit (SOMP) [28], where we assume that the number of active legitimate devices is known a priori at each access. Although the *sparsity-aware* SOMP with the prior knowledge cannot be realistic in practice, it gives the best achievable performance of activity detection for legitimate devices by this algorithm under the impersonation attack. In simulations, we evaluate a variety of performance measures through 50000 access trials.

Fig. 4 sketches data modification and false authentication rates over the number of malicious signatures n_a, along with their upper bounds of Theorems 1 and 2, respectively. In the figure, we assume that the malicious device located at $R_1 = 0.05$ km transmits the signatures with total power $\rho_m = 20$, 23, and 26 dBm, respectively. The figure shows that if n_a is small, the rates are tightly bounded by the upper bounds, respectively, but deviate from the bounds as n_a increases. It is because less power $\rho_a = \frac{\rho_m}{n_a}$ will be assigned to each malicious signature of $\mathcal{A}_{\mathsf{M}}$ and $\mathcal{A}_{\mathsf{F}}$, respectively, as n_a increases. Thus, if n_a is large, the activity of the malicious signature is not likely to be detected by a BS as successfully as expected. In particular, the deviation is outstanding for the

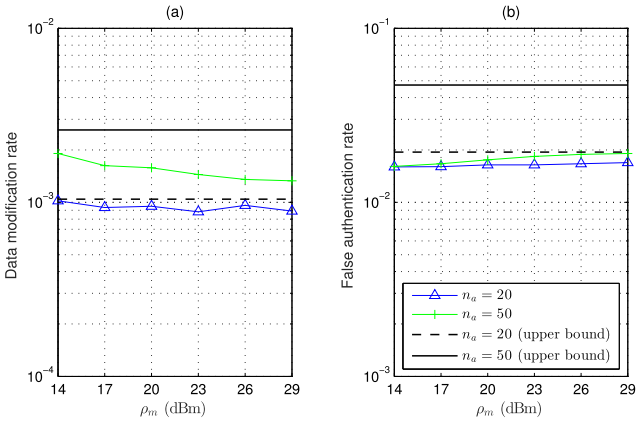

FIGURE 5. Data modification and false authentication rates over the adversary's total transmit power ρ_m, where the malicious device is closest to the BS, located at $R_1 = 0.05$ km from it.

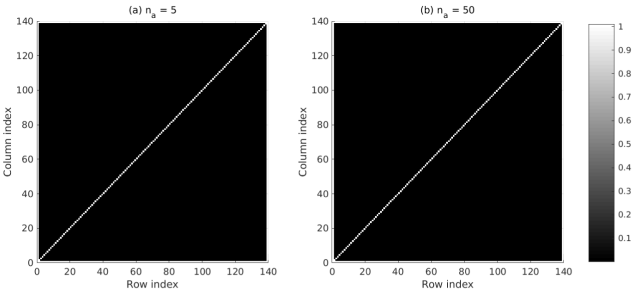

FIGURE 6. Empirical covariance matrices of the jamming samples of $\mathbf{W}_J$ for $n_a = 5$ and 50 at $\rho_m = 23$ dBm, where the malicious device is closest to the BS, located at $R_1 = 0.05$ km from it.

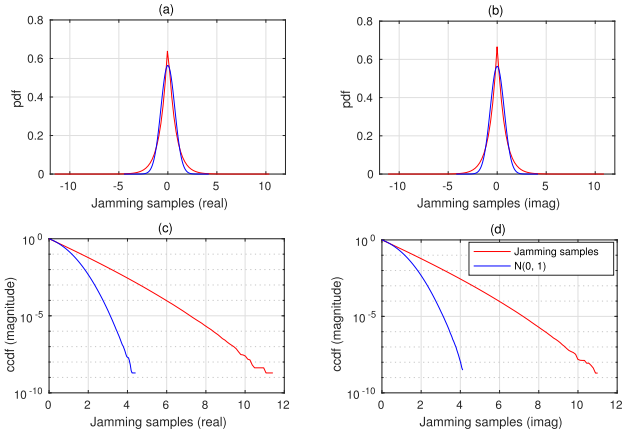

FIGURE 7. Empirical pdfs and ccdfs of the jamming samples of $\mathbf{W}_J$ for $n_a = 5$ and $\rho_m = 23$ dBm, where the malicious device is closest to the BS, located at $R_1 = 0.05$ km from it. Blue lines denote the standard normal distribution with mean 0 and variance 1, while red lines indicate the empirical pdfs and ccdfs of normalized jamming samples.

false authentication rate, flattening it as n_a increases, which conforms to the discussion in Remark 3. Comparing the rates, we observe that false authentication can be a more serious threat to an mMTC system than data modification.

Fig. 5 displays data modification and false authentication rates over the adversary's total transmit power ρ_m, along with their upper bounds of Theorems 1 and 2, respectively. In the figure, we assume that the malicious device located at $R_1 = 0.05$ km transmits $n_a = 20$ and 50 signatures, respectively. In the figure, the upper bounds remain unchanged over the transmit power, since the proofs of Theorems 1 and 2 are based on the worst-case scenarios to maximize the upper bounds, respectively, regardless of the transmit power. Interestingly, the figure shows that the irrelevance to ρ_m can also be seen from the actual rates. It is because jamming strengthens as the transmit power ρ_m increases, as shown by Theorem 4, which degrades the performance of activity detection for both legitimate and malicious signatures. Thus, the poor detection performance for high ρ_m will not increase the data modification or the false authentication rates even with large n_a.

To investigate the statistical properties of jamming, Fig. 6 sketches the magnitudes of covariance matrix elements of a column of $\mathbf{W}_J$ in (6), which have been normalized by σ_J^2 of (10) and averaged over total access trials. In this experiment, the malicious device located at $R_1 = 0.05$ km from BS transmits $n_a = 5$ and 50 signatures with total power $\rho_m = 23$ dBm, respectively. As shown in Fig. 6, the covariance matrix can be approximated by the identity matrix, which gives a numerical evidence that each jamming sample has the variance σ_J^2 and a distinct pair of jamming samples are uncorrelated. Thus, Fig. 6 confirms the result of Theorem 4 numerically for small and moderately large n_a.

Fig. 7 depicts the probability density functions (pdf) and the complementary cumulative distribution functions (ccdf) of real and imaginary jamming samples of $\mathbf{W}_J$, obtained from total access trials for $n_a = 5$, respectively, where each sample has been normalized by $\frac{\sigma_J^2}{2}$. Note that we also observed similar shapes for the functions when $n_a = 50$. For comparison, Fig. 7 sketches the pdfs and ccdfs of the standard normal distribution with mean 0 and variance 1. It appears that the numerical pdfs of jamming samples are similar to the true normal pdfs even for small n_a, but the ccdfs show a clear distinction between them. The ccdfs reveal that the jamming samples tend to take larger magnitudes than the standard normal ones, which implies that jamming may degrade the detection performance of BS more severely than the additive Gaussian noise with zero mean and variance σ_J^2. To sum up, Figs. 6 and 7 suggest that jamming from the impersonation attack introduces the additive noise with power σ_J^2, which will degrade the detection performance more severely than adding the Gaussian noise with the same power.

Fig. 8 depicts the goodputs of activity detection for legitimate devices, defined by the average of $\frac{|\mathcal{K} \cap \widehat{\mathcal{K}}|}{|\widehat{\mathcal{K}}|}$ over total access trials, where $\mathcal{K}$ and $\widehat{\mathcal{K}}$ are true and estimated sets of active legitimate signatures, respectively. Fig. 8(a) shows that while the BS receiver can detect all active legitimate devices successfully with no malicious signature ($n_a = 0$),

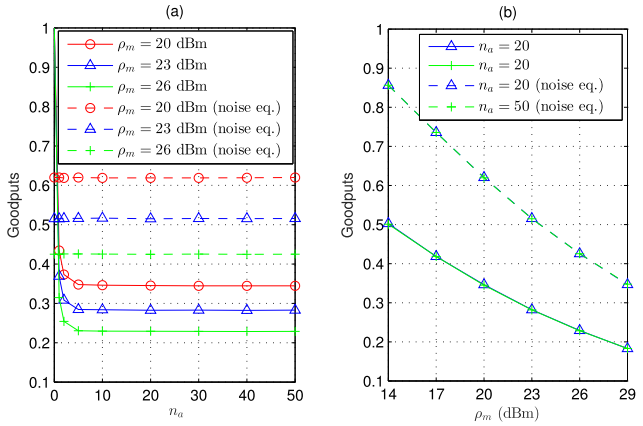

FIGURE 8. Goodputs of activity detection for legitimate devices over the number of malicious signatures n_a and the total transmit power ρ_m, where the malicious device is closest to the BS, located at $R_1 = 0.05$ km from it.

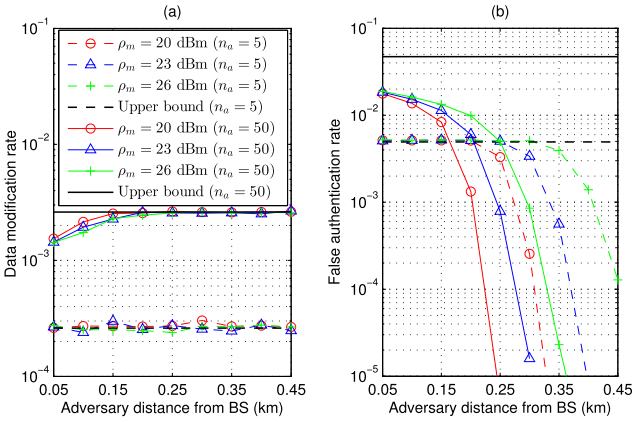

FIGURE 9. Data modification and false authentication rates over the adversary's distance from BS.

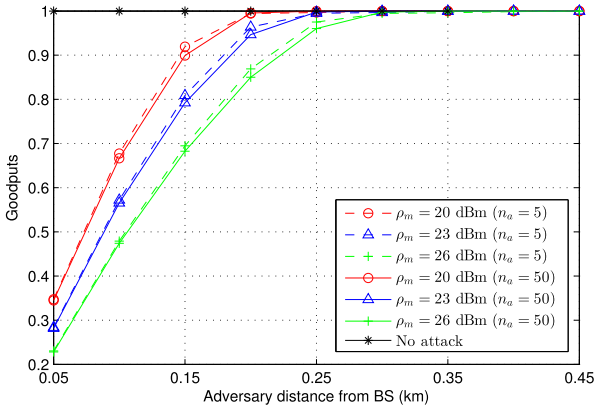

FIGURE 10. Goodputs of activity detection for legitimate devices over the adversary's distance from BS.

the detection performance drops drastically if the malicious device at $R_1 = 0.05$ km transmits the signatures ($n_a > 0$). In Fig. 8(a), the goodputs are rarely affected by various $n_a > 0$, since the the jamming power σ_J^2 does not depend on n_a from (10). Meanwhile, Fig. 8(b) shows that the goodputs are reduced as the transmit power ρ_m of the malicious device increases, which is because the jamming power increases as ρ_m. Fig. 8 also sketches the goodputs for a noise equivalent model that has the received signal of (2) at BS, where the power of AWGN is increased by σ_J^2 with no impersonation attack. As shown in Fig. 8, higher goodputs are achieved in the noise equivalent model than in the true model of impersonation attack, which demonstrates that jamming causes more severe degradation for detection performance than simple addition of the Gaussian noise with the same power.

Up to now, we examined the impacts of impersonation attack in the worst-case scenario that the adversary is closest to BS. In Figs. 9 and 10, we now investigate the impacts by changing the distance of the adversary from BS. Fig. 9 shows that the upper bounds on data modification and false authentication rates remain unchanged over the adversary's distance, since they are derived in the worst-case scenario not considering the received power of signatures determined by the path loss. Fig. 9(a) shows that the data modification rates, tightly bounded by the upper bound of Theorem 1, are little influenced by the adversary's distance. It is because the malicious signatures of $\mathcal{A}_M$ causing data modification can be detected successfully, regardless of the received power, since they are overlapped with legitimate ones of which the received power may be sufficiently high. Meanwhile, Fig. 9(b) indicates that the false authentication rates drop dramatically as the adversary moves far away from the BS, deviating from the upper bound of Theorem 2. It is because the malicious signatures of $\mathcal{A}_F$ causing false authentication are less likely to be detected successfully at BS due to the path loss, if the adversary's distance from BS increases. But if n_a is small, e.g., $n_a = 5$, the false authentication rate drops slowly over the distance, since each malicious signature is transmitted with high power $\rho_a = \frac{\rho_m}{n_a}$. Therefore, the adversary has to choose the number of malicious signatures carefully, depending on its distance from BS, to maximize the false authentication rate.

Fig. 10 demonstrates that the goodputs of activity detection for legitimate devices improve as the adversary moves far away from the BS. The improvement is obvious because jamming from the malicious signatures is reduced considerably due to the path loss, if the adversary's distance from BS increases. In Fig. 10, we also observe that the goodputs are more deteriorated as the malicious signatures strengthen jamming with high transmit power ρ_m. By contrast, they are little influenced by the number of malicious signatures n_a, since the jamming power is not determined by n_a.

V. CONCLUSION

In this paper, we have studied the performance of signature-based grant-free random access when an adversary attempts to impersonate legitimate devices to gain illegal access to an mMTC system. Renewing a legitimate signature set at each

access, we have analyzed the impacts of impersonation attack on the access scheme, with respect to data modification, false authentication, and jamming. The main contributions of this paper are summarized as follows.

- We gained an insight into the resilience of signature-based grant-free random access against the impersonation attack by deriving the upper bounds on data modification and false authentication rates, respectively. The theoretical and numerical results showed that false authentication can be a more serious threat to the access scheme than data modification. We found that both rates are rarely affected by the adversary's total transmit power. To enhance the access security, the codebook should have as many signatures as possible.
- We investigated the effect of jamming on the performance of activity detection for legitimate devices. We found that jamming from this attack can be treated as the additive non-Gaussian noise, where the equivalent noise power is determined by the adversary's total transmit power and the path loss. With a large codebook size, jamming can be a major source of performance degradation of signature-based grant-free access by this attack.
- As the adversary moves far away from the BS, we found that the false authentication rate drops and the goodput of legitimate devices improves, which conforms to our intuition. In contrast, the data modification rate remains unchanged by the adversary's distance from the BS. Thus, signature-based grant-free random access will be vulnerable to data modification by this attack, regardless of the adversary's position in a cell.

In performance evaluation, this paper did not consider any prevention schemes of physical layer security (PLS) to defeat the impersonation attack. The reason is that we have placed the focus of this work on analyzing the impacts of impersonation attack on signature-based grant-free random access with a renewal of signatures, not proposing a new prevention scheme to enhance the access security. A further research considering PLS schemes may be fruitful for improving the resilience of this access scheme against the impersonation attack.

APPENDIX A PROOF OF THEOREM 1

By definition, the data modification rate is approximated by

$$\lambda_m \approx \frac{\mathbb{E}\left[|\mathcal{A}_{\mathsf{M}} \cap \widehat{\mathcal{K}}|\right]}{\mathbb{E}\left[|\widehat{\mathcal{K}}|\right]}. \tag{11}$$

Let $p_m(k)$ be the probability that k signatures of $\mathcal{A}$ fall into $\mathcal{K}$, i.e., $p_m(k) = \Pr[|\mathcal{A}_{\mathsf{M}}| = k]$. A choice of signatures for this event is characterized by the binomial distribution $\mathcal{B}(n_a, r_d p_d)$, where $r_d p_d$ is the average probability that a signature of $\mathcal{K}$ is chosen from the sample space $\mathcal{T}$ by the malicious device. Let p_{sg} be the probability that the activity of a signature in $\mathcal{A}_{\mathsf{M}}$ is detected successfully by a BS in the first-phase of access. Then, the average number of active legitimate devices that are successfully detected in the first-phase, but will suffer from data modification in the second-phase is

$$\begin{aligned}\mathbb{E}\left[|\mathcal{A}_{\mathsf{M}} \cap \widehat{\mathcal{K}}|\right] &= \sum_{k=0}^{n_a} p_m(k) \cdot \mathbb{E}\left[|\mathcal{A}_{\mathsf{M}} \cap \widehat{\mathcal{K}}| \,\middle|\, |\mathcal{A}_{\mathsf{M}}| = k\right] \\ &= \sum_{k=0}^{n_a} p_m(k) \left(\sum_{v=0}^{k} v \binom{k}{v} \cdot p_{\mathsf{sg}}^{v}(1-p_{\mathsf{sg}})^{k-v}\right) \\ &= \sum_{k=0}^{n_a} p_m(k) \cdot k p_{\mathsf{sg}} = n_a r_d p_d \cdot p_{\mathsf{sg}}. \end{aligned} \tag{12}$$

Meanwhile, the average number of devices detected by a BS satisfies

$$\mathbb{E}\left[|\widehat{\mathcal{K}}|\right] \geq \mathbb{E}\left[|\mathcal{K} \cap \widehat{\mathcal{K}}|\right] + \mathbb{E}\left[|\mathcal{A} \cap (\widehat{\mathcal{K}} \setminus \mathcal{K})|\right], \tag{13}$$

where

$$\begin{aligned}\mathbb{E}\left[|\mathcal{K} \cap \widehat{\mathcal{K}}|\right] &\approx \mathbb{E}\left[|\mathcal{K} \setminus \mathcal{A}|\right] \cdot p_{\mathsf{sg}} + \mathbb{E}\left[|\mathcal{A} \cap \mathcal{K}|\right] \cdot p_{\mathsf{sg}} \\ &= \mathbb{E}\left[|\mathcal{K}|\right] \cdot p_{\mathsf{sg}} = N p_d p_{\mathsf{sg}}. \end{aligned} \tag{14}$$

In (14), we assumed that the activity of a legitimate signature in $\mathcal{K}$, whether it falls into $\mathcal{K} \setminus \mathcal{A}$ or $\mathcal{A} \cap \mathcal{K}$, can be detected with the same probability p_{sg}. Let $p_f(k)$ be the probability that k signatures of $\mathcal{A}$ fall into $\mathcal{N} \setminus \mathcal{K}$, i.e., $p_f(k) = \Pr[|\mathcal{A}_{\mathsf{F}}| = k]$, where $\mathcal{A}_{\mathsf{F}} = \mathcal{A} \cap (\mathcal{N} \setminus \mathcal{K})$. A choice of signatures for this event is characterized by $\mathcal{B}(n_a, r_d(1-p_d))$. Let p_{sm} be the probability that the activity of a malicious signature of $\mathcal{A}_{\mathsf{F}}$ is detected successfully in the first-phase of access. Then,

$$\begin{aligned}&\mathbb{E}\left[|\mathcal{A} \cap (\widehat{\mathcal{K}} \setminus \mathcal{K})|\right] \\ &= \sum_{k=0}^{n_a} p_f(k) \cdot \mathbb{E}\left[|\mathcal{A} \cap (\widehat{\mathcal{K}} \setminus \mathcal{K})| \,\middle|\, |\mathcal{A}_{\mathsf{F}}| = k\right] \\ &= \sum_{k=0}^{n_a} p_f(k) \left(\sum_{v=0}^{k} v \binom{k}{v} \cdot p_{\mathsf{sm}}^{v}(1-p_{\mathsf{sm}})^{k-v}\right) \\ &= \sum_{k=0}^{n_a} p_f(k) \cdot k p_{\mathsf{sm}} = n_a r_d (1-p_d) \cdot p_{\mathsf{sm}}. \end{aligned} \tag{15}$$

From (12)–(15), we have

$$\mathbb{E}\left[|\mathcal{A}_{\mathsf{M}} \cap \widehat{\mathcal{K}}|\right] \Big/ \mathbb{E}\left[|\widehat{\mathcal{K}}|\right] \leq \frac{r_a p_d}{p_d + \alpha \cdot r_a(1-p_d)}, \tag{16}$$

where $\alpha = p_{\mathsf{sm}}/p_{\mathsf{sg}} \geq 0$. For given r_a and p_d, the upper bound of (16) decreases over α. Finally, (7) is immediate from (11) and (16) with $\alpha = 0$.

APPENDIX B PROOF OF THEOREM 2

By definition, the false authentication rate is approximated by

$$\lambda_f \approx \frac{\mathbb{E}\left[|\mathcal{A}_{\mathsf{F}} \cap \widehat{\mathcal{K}}|\right]}{\mathbb{E}\left[|\widehat{\mathcal{K}}|\right]} = \frac{\mathbb{E}\left[|\mathcal{A} \cap (\widehat{\mathcal{K}} \setminus \mathcal{K})|\right]}{\mathbb{E}\left[|\widehat{\mathcal{K}}|\right]}. \tag{17}$$

From (14) and (15), we have

$$\mathbb{E}\left[|\mathcal{A} \cap (\widehat{\mathcal{K}} \setminus \mathcal{K})|\right] \Big/ \mathbb{E}\left[|\widehat{\mathcal{K}}|\right] \leq \frac{\alpha \cdot r_a(1-p_d)}{p_d + \alpha \cdot r_a(1-p_d)}, \tag{18}$$

where $\alpha = p_{\mathsf{sm}}/p_{\mathsf{sg}}$ from the definitions of p_{sm} and p_{sg} in the proof of Theorem 1. For given r_a and p_d, it is readily checked that the bound of (18) monotonically increases as α. At a BS, the received power of a signature in $\mathcal{A}_{\mathsf{M}}$ will be higher than that of a signature in $\mathcal{A}_{\mathsf{F}}$, since the former is the addition of powers of legitimate and malicious signatures. Thus, it is reasonable to assume that $p_{\mathsf{sm}} \le p_{\mathsf{sg}}$, or $\alpha \le 1$, which yields the upper bound of (8) from (18) at $\alpha = 1$.

APPENDIX C PROOF OF THEOREM 3

The event that the malicious signatures fall into $\mathcal{A}_{\mathsf{F}}$ is characterized by $\mathcal{B}(n_a, r_d(1-p_d))$. Then, the probability that the number of malicious signatures in $\mathcal{A}_{\mathsf{F}}$ is at most K_{F} is

$$\begin{aligned}\Pr\left[|\mathcal{A}_{\mathsf{F}}| \le K_{\mathsf{F}}\right] &= 1 - \sum_{k=K_{\mathsf{F}}+1}^{n_a} \binom{n_a}{k} q^k (1-q)^{n_a-k} \\ &\approx 1 - \binom{n_a}{K_{\mathsf{F}}+1} q^{K_{\mathsf{F}}+1}(1-q)^{n_a-K_{\mathsf{F}}-1} \\ &\triangleq p_y, \end{aligned} \tag{19}$$

where we used the approximation from $q = r_d(1-p_d) \ll 1$, assuming $r_d \ll 1$ from $N \ll T$. For $p_y > 1-\epsilon$, we obtain from (19)

$$\left(\frac{en_a}{K_{\mathsf{F}}+1}\right)^{K_{\mathsf{F}}+1} q^{K_{\mathsf{F}}+1}(1-q)^{n_a-K_{\mathsf{F}}-1} < \epsilon, \tag{20}$$

where we used $\binom{n}{k} \le \left(\frac{en}{k}\right)^k$. Applying the logarithm to (20), we have

$$\begin{aligned}(K_{\mathsf{F}}+1)\left(1 + \log\frac{n_a}{K_{\mathsf{F}}+1} + \log\frac{q}{1-q}\right) &\le n_a + (K_{\mathsf{F}}+1)\log\frac{q}{1-q} \\ &< \log\epsilon - n_a\log(1-q), \end{aligned} \tag{21}$$

where we used $\log x \le x-1$ for $x = \frac{n_a}{K_{\mathsf{F}}+1} \ge 1$. As $\log\frac{q}{1-q} < 0$ due to $q \ll 1$, (21) becomes

$$K_{\mathsf{F}} > \frac{\log\epsilon - n_a\log e(1-q)}{\log q - \log(1-q)} - 1, \tag{22}$$

which yields (9).

APPENDIX D PROOF OF THEOREM 4

The event of choosing the malicious signatures from $\mathcal{T}\setminus\mathcal{N}$ is characterized by $\mathcal{B}(n_a, 1-r_d)$. From (6), recall that $\mathbf{S}' = [\mathbf{s}'_1, \ldots, \mathbf{s}'_{N_c}]$ contains all the signatures of $\mathcal{T}\setminus\mathcal{N}$ as its columns, where $N_c = T - N$. Define an indicator vector $\boldsymbol{\alpha}' = (\alpha'_1, \ldots, \alpha'_{N_c})$, where $\alpha'_n = 1$ if $\mathbf{s}'_n \in \mathcal{A}_{\mathsf{J}}$, and 0 otherwise. Then, the tth column of $\mathbf{W}_{\mathsf{J}}$ is

$$\mathbf{w}_{\mathsf{J}}^{(t)} = \sqrt{\xi_a}\mathbf{S}'\mathbf{x}_{\mathsf{J}}^{(t)} = \sqrt{\xi_a}\sum_{n=1}^{N_c}\mathbf{s}'_n\alpha'_n x_{\mathsf{J},n}^{(t)}, \tag{23}$$

where $x_{\mathsf{J},n}^{(t)} = x_{\mathsf{J}}^{(t)}$ for all n with $\alpha'_n = 1$, since it is the channel gain between the malicious device and the BS receiver's antenna t. By the definition of α'_n, the average number of nonzero terms in the sum of (23) is $n_a(1-r_d)$. From (4), each element of the ZC sequence $\mathbf{s}'_n$ can be modeled by $\frac{1}{\sqrt{M}}\exp(\frac{j2\pi\phi}{M})$, where ϕ can be assumed as a random phase if the adversary selects the signatures randomly. As (23) shows that $\mathbf{w}_{\mathsf{J}}^{(t)}$ is the sum of $n_a(1-r_d)$ exponential terms of random phases on average, we have $\mathbb{E}[\mathbf{w}_{\mathsf{J}}^{(t)}] \approx \mathbf{0}$ for sufficiently large n_a. Similarly, $\mathbb{E}\left[\mathbf{s}'_n(\mathbf{s}'_l)^*\right] \approx \frac{1}{M}\mathbf{I}$ if $n = l$, and $\mathbf{0}$ otherwise, for sufficiently large n_a.

Given $\boldsymbol{\alpha}'$ and $x_{\mathsf{J}}^{(t)}$, the covariance of $\mathbf{w}_{\mathsf{J}}^{(t)}$ is

$$\begin{aligned}\mathbf{K}_{\mathsf{J}\mid\boldsymbol{\alpha}',x_{\mathsf{J}}^{(t)}}^{(t)} &= \mathbb{E}\left[\mathbf{w}_{\mathsf{J}}^{(t)}\cdot(\mathbf{w}_{\mathsf{J}}^{(t)})^* \,\middle|\, \boldsymbol{\alpha}', x_{\mathsf{J}}^{(t)}\right] \\ &= \xi_a\sum_{n,l=1}^{N_c}\alpha'_n\alpha'_l\mathbb{E}\left[\mathbf{s}'_n(\mathbf{s}'_l)^*\right]\cdot\left|x_{\mathsf{J}}^{(t)}\right|^2 \\ &\approx \rho_a\left|x_{\mathsf{J}}^{(t)}\right|^2\left(\sum_{n=1}^{N_c}\alpha'_n\right)\mathbf{I}, \end{aligned} \tag{24}$$

where the approximation is made for sufficiently large n_a. If $\mathbf{K}_{\mathsf{J}\mid\boldsymbol{\alpha}',x_{\mathsf{J}}^{(t)}}^{(t)}$ is averaged over $\boldsymbol{\alpha}'$ and $x_{\mathsf{J}}^{(t)}$, we have

$$\begin{aligned}\mathbf{K}_{\mathsf{J}} &\approx \rho_a\mathbb{E}\left[\left|x_{\mathsf{J}}^{(t)}\right|^2\right]\cdot\mathbb{E}\left[\sum_{n=1}^{N_c}\alpha'_n\right]\mathbf{I} \\ &= \rho_a\beta_m n_a(1-r_d)\mathbf{I}, \end{aligned} \tag{25}$$

where $\beta_m = \mathbb{E}\left[\left|x_{\mathsf{J}}^{(t)}\right|^2\right]$ is the path-loss component determined by the distance of the malicious device from a BS, and $\mathbb{E}\left[\sum_{n=1}^{N_c}\alpha'_n\right] = n_a(1-r_d)$ indicates the average number of malicious signatures in $\mathcal{A}_{\mathsf{J}}$. Finally, (10) is obtained from (25) with $\rho_m = \rho_a n_a$.

REFERENCES

[1] T. Taleb and A. Kunz, "Machine type communications in 3GPP networks: Potential, challenges, and solutions," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 178–184, Mar. 2012.
[2] *Service Requirements for Machine-Type Communications (MTC)*, document TS 22.368, Version 13.1.0, Release 13, 3GPP, 2015.
[3] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2294–2323, 3rd Quart., 2018.
[4] M. Mohammadkarimi, M. A. Raza, and O. A. Dobre, "Signature-based nonorthogonal massive multiple access for future wireless networks," *IEEE Veh. Technol. Mag.*, vol. 13, no. 4, pp. 40–50. Dec. 2018.
[5] A. C. Cirik, N. M. Balasubramanya, L. Lampe, G. Vos, and S. Bennett, "Toward the standardization of grant-free operation and the associated NOMA strategies in 3GPP," *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 60–66, Dec. 2019.
[6] J. Katz and Y. Lindell, *Introduction To Modern Cryptography*, 2nd ed. New York, NY, USA: Taylor & Francis, 2015.
[7] L. Lv, H. Jiang, Z. Ding, Q. Ye, N. Al-Dhahir, and J. Chen, "Secure non-orthogonal multiple access: An interference engineering perspective," *IEEE Netw.*, vol. 35, no. 4, pp. 278–285, Jul. 2021.
[8] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.
[9] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.
[10] N. K. Pratas, S. Pattathil, C. Stefanovic, and P. Popovski, "Massive machine-type communication (mMTC) access with integrated authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[11] N. Xie, S. Zhang, and A. X. Liu, "Physical-layer authentication in non-orthogonal multiple access systems," *IEEE/ACM Trans. Netw.*, vol. 28, no. 3, pp. 1144–1157, Jun. 2020.

[12] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3377–3389, Apr. 2018.
[13] D. Xu, P. Ren, H. He, and Q. Li, "Jamming-immune receiver design for MIMO-NOMA systems using optimal manifold filtering," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.
[14] H. Wang, Y. Fu, R. Song, Z. Shi, and X. Sun, "Power minimization precoding in uplink multi-antenna NOMA systems with jamming," *IEEE Trans. Green. Commun. Netw.*, vol. 3, no. 3, pp. 591–602, Sep. 2019.
[15] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challeges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.
[16] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city," *IEEE Access*, vol. 7, pp. 54508–54521, 2019.
[17] D. P. M. Osorio, E. E. B. Olivio, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101437–101447, 2020.
[18] E. Martinian, G. W. Wornell, and B. Chen, "Authentication with distortion criteria," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2523–2542, Jul. 2005.
[19] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 4, pp. 531–532, Jul. 1972.
[20] L. Liu and W. Yu, "Massive connectivity with massive MIMO—Part I: Device activity detection and channel estimation," *IEEE Trans. Signal Process.*, vol. 66, no. 11, pp. 2933–2946, Jun. 2018.
[21] L. Liu, E. G. Larsson, W. Yu, P. Popovski, C. Stefanovic, and E. de Carvalho, "Sparse signal processing for grant-free massive connectivity: A future paradigm for random access protocols in the Internet of Things," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 88–99, Sep. 2018.
[22] Y. C. Eldar and G. Kutyniok, *Compressed Sensing—Theory and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[23] L. Chen and G. Gong, *Communication System Security*. New York, NY, USA: Taylor & Francis, 2012.
[24] *Physical Channel and Modulation*, document TS 36.211, Version 13.1.0, 3GPP, Mar. 2016.
[25] E. Dahlman, S. Parkvall, and J. Sköld, *5G NR: The Next Generation Wireless Technology*. New York, NY, USA: Academic, 2018.
[26] D. Sarwate, "Bounds on crosscorrelation and autocorrelation of sequences," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 6, pp. 720–724, Nov. 1979.
[27] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 1991.
[28] J. A. Tropp, A. C. Gilbert, and M. J. Strauss, "Algorithms for simultaneous sparse approximation. Part I: Greedy pursuit," *Signal Process.*, vol. 86, no. 3, pp. 572–588, Mar. 2006.

NAM YUL YU (Senior Member, IEEE) received the B.S. degree in electronics engineering from Seoul National University, Seoul, South Korea, in 1995, the M.S. degree in electronics and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, South Korea, in 2000, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2007.

From 2000 to 2003, he was at the Telecommunication Research and Development Center, Samsung Electronics, South Korea, where he worked on channel coding schemes for wireless communication systems. In 2007, he was a Senior Research Engineer at LG Electronics, South Korea, working on the standardization of the 3GPP-LTE. From 2008 to 2014, he was an Assistant/Associate Professor at the Department of Electrical Engineering, Lakehead University, Thunder Bay, ON, Canada. In 2014, he joined at the Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, where he is currently working as an Associate Professor with the School of Electrical Engineering and Computer Science. His research interest includes communication and signal processing techniques for wireless communications. He was an Associate Editor of sequences in IEEE TRANSACTIONS ON INFORMATION THEORY, from 2009 to 2011.