mathematics

MDPI

Article

Pilot Contamination Attack Detection Methods—An Exhaustive Performance Evaluation Through Probability Metrics and Statistical Classification Parameters

Dimitriya Mihaylova *, Georgi Iliev, Zlatka Valkova-Jarvis and Viktor Stoynov

Faculty of Telecommunications, Technical University of Sofia, 1000 Sofia, Bulgaria; gli@tu-sofia.bg (G.I.); zvv@tu-sofia.bg (Z.V.-J.); vstoynov@tu-sofia.bg (V.S.)

* Correspondence: dam@tu-sofia.bg

Abstract: Among the numerous strategies that an attacker can initiate to enhance its eavesdropping capabilities is the Pilot Contamination Attack (PCA). Two promising methods, based on Phase-Shift Keying (PSK) modulation of Nth order—*2-N-PSK* and *Shifted 2-N-PSK*, can detect an existing PCA by means of analysis of the constellation that the correlation product of received pilot signals belongs to. The overall efficiency of the methods can be studied by the most commonly used probability metrics—detection probability and false alarm probability. However, this information may be insufficient for comparison purposes; therefore, to acquire a more holistic perspective on the methods' performances, statistical evaluation metrics can be obtained. Depending on the particular application of the system in which the PCA detection methods are incorporated and the distribution of attack initiation among all samples, different classification parameters are of varying significance in the efficiency assessment. In this paper, *2-N-PSK* and *Shifted 2-N-PSK* are comprehensively studied through their probability parameters. In addition, the methods are also compared by their most informative statistical parameters, such as *accuracy*, *precision* and *recall*, *F1-score*, *specificity*, and *fall-out*. A large number of simulations are carried out, the analyses of which indisputably prove the superior behavior of the *Shifted 2-N-PSK* compared to the *2-N-PSK* detection method. Since a method's performance is strongly related to the number of antenna elements at the base station, all simulations are conducted for scenarios with different antennae numbers. The most promising realization of *Shifted 2-N-PSK* improves the receiver operating characteristics results of the original *2-N-PSK* by 7.38%, 4.33%, and 5.61%, and outperforms the precision recall analyses of *2-N-PSK* by 10.02%, 4.82% and 3.86%, for the respective number of 10, 100 and 300 antenna elements at the base station.

Keywords: pilot contamination attack; physical layer security; statistical evaluation; binary classification

MSC: 62P30; 68M10

check for updates

Citation: Mihaylova, D.; Iliev, G.; Valkova-Jarvis, Z.; Stoynov, V. Pilot Contamination Attack Detection Methods—An Exhaustive Performance Evaluation Through Probability Metrics and Statistical Classification Parameters. *Mathematics* **2024**, *12*, 3524. https://doi.org/10.3390/math12223524

Academic Editor: Daniel-Ioan Curiac

Received: 9 October 2024
Revised: 6 November 2024
Accepted: 9 November 2024
Published: 12 November 2024

1. Introduction

With the evolution of next generation wireless systems, a large number of autonomous devices are expected to be deployed and connected through heterogeneous technologies. Responsible for a variety of services, including manufacturing and transportation, healthcare and road safety, these intelligent systems will collect a massive amount of sensitive information and exchange the data through communication networks. Hence, the ever-increasing need for reliable and secure operation is one of the key concepts for sixth-generation (6G) wireless networks and beyond.

While cryptography-based solutions have been established as the fundamental approach to secure and private information exchange, lightweight physical layer security (PLS) methods can be used as an alternative to afford information-theoretic protection against unauthorized intervention. The pioneering work of Shannon [1] and Wyner [2] lays the foundations of PLS principles to exploit the random nature of wireless channels and achieve secure transmission using only the properties of the communication medium. Being independent of complex computational algorithms, such as those applied in cryptosystems, PLS approaches are extremely suitable for small resource-constrained devices, the widespread use of which is expected to increase with the evolution of next-generation wireless networks that enable the incorporation of new technologies in a variety of sectors, and the expansion of the concept of the Internet of Things into the Internet of Everything. Furthermore, PLS techniques can be applied as a supplement to upper layers' resources in order to establish trustworthy and resilient security solutions. An exhaustive review of the literature concerning how 6G technology is envisaged, together with an analysis of the available research on PLS applications for 6G is provided in [3].

Being one of the key enablers of fifth-generation (5G) wireless networks, massive multiple-input multiple-output (MIMO) is also envisioned to be an indispensable radio antenna technology in the upcoming 6G. As foreseen, terahertz (THz) communications will be introduced in 6G to achieve very high transmission rates over 100 Gbps and extend the use of available spectrum bands [3,4]. However, the short wavelengths at such high frequencies suffer from molecular absorption loss and severe path loss, and hence require very precise directional beam steering with a narrow main lobe, which could be attained through proper precoding and beamforming [4]. Fortunately, the small size of radio components at this frequency range enables the construction of antenna arrays having tens and even hundreds antenna elements, making it possible to benefit from the advantages of massive MIMO technology. Three different massive MIMO precoding strategies for THz communications are studied in [4], and their sustainability is evaluated through simulation analysis of their energy and spectral efficiencies at different carrier frequency, bandwidth and antenna gain scenarios.

Alongside spatial diversity gain and spatial multiplexing, massive MIMO offers the opportunity for highly directional communication, lessening the probability of a passive eavesdropper launching a successful attack. Nevertheless, in massive MIMO systems with time division duplex (TDD) operation, a resourceful eavesdropper (ED) can initiate an active attack aimed at the process of channel estimation in order to improve its own downlink channel conditions. A main feature of TDD systems, providing the means of one-way channel estimation, is the reciprocity between channels for uplink and downlink transmission. Prior to the information exchange, an uplink training phase is accomplished during which training signals, also called pilot signals, are sent to the base station (BS). The BS processes the received pilot signal and obtains the corresponding channel state information (CSI), which is used to extract the transfer function of the downlink channel and construct the precoding matrix for downlink transmission to send the information signal in the direction of the legitimate user (LU). The malicious intervention known as a PCA, also referred to as a pilot spoofing attack (PSA), consists of the intentional transmission of signals from the same publicly available alphabet as the legitimate pilots by an ED [5]. This way, the signal received at the BS during the uplink training phase is a combination of two correlated components—one from LU and another from the ED. Since no prior knowledge of the channels is available at the BS, no identification of the channel estimation procedure is applicable, and the BS is incapable of distinguishing between both the components of the received signal. As a consequence, the BS obtains a CSI that falls under the influence of the transfer function of the non-legitimate channel between ED and BS, and the computed precoding matrix for the information exchange phase directs the beam of the information signal not only to the intended LU, but also to the ED. The impact of a PCA on system performance is double-edged: on one hand, less signal power is allocated to LU, which deteriorates the quality of legitimate communication; on the other hand, assigning more signal power in the direction of ED overcomes the natural resistance of massive MIMO systems to passive eavesdropping and compromises the security and privacy of information exchange. The PCA can be successfully initiated in every wireless system with TDD operation, however resource-constrained networks, such as Internet of Things, where upper layer authentication of the first training phase is not considered due to hardware and software limitations, are extremely vulnerable to those types of malicious intervention.

1.1. Related Work

Since its first description in [5], PCAs have attracted significant research attention. The resemblance between an intentional PCA and natural contamination, peculiar to multi-cell massive MIMO systems and extensively studied in [6], makes its detection a challenge. Up to now, numerous studies based on PLS approaches have focused on PCA detection. The authors in [7] propose a likelihood ratio test (LRT) detector to discover PCA by the separation of legitimate pilots into two parts and the multiplication of the second part by a diagonal matrix of random numbers. Three other LRT detectors based on different metrics from the channel estimate are proposed in [8]. A main drawback of the detectors in [8] is that all the three schemes are dependent on a certain threshold value determined from false alarm probability prior PCA detection, which is not always available. Instead of using threshold values, another strategy in [9] consists in superimposing a random sequence of scalars onto the original training signal and the detection of PCA by a minimum description length (MDL) source enumeration algorithm.

In [10,11] the authors suggest two-way training channel estimation to detect PCA. In both the papers, the decision for the presence or absence of attack is taken at the LU after downlink training, and different operational principles are followed for the channel estimate. In [10], during the downlink training phase the BS sends the computed CSI together with the acknowledged pilot signal and a decision threshold is extracted from the probability of a false alarm. Instead of re-transmission of the known pilot sequence in the downlink direction, the authors in [11] transmit dedicated signals composed of two separate parts—one containing information for the CSI and another intended for calculating the decision threshold. While in [10], a decision threshold extracted from probability of false alarm and a priori channel knowledge is again used, the authors in [11] criticize methods that rely on test statistics from advanced large-scale fading knowledge and propose a decision metric derived from the second component of the dedicated signal received at the LU.

As discussed in [3], the cell-free massive MIMO, in which a large number of distributed access points are cooperatively serving the users in the cell, benefits from several advantages compared to conventional massive MIMO, such as spectral efficiency improvement, and throughput increase. Apart from the advantages, the authors in [3] draw attention to the intensified vulnerabilities of cell-free massive MIMO to active attacks and comment on appropriate PLS solutions. A promising PLS secure transmission method that successfully removes the PCA component from the channel estimate of cell-free massive MIMO systems is introduced in [12]. The method is composed of two stages: in the first step, the access points collect information about the positions of LU and ED through fingerprint and K-means clustering. The second step involves channel estimation by discrete Fourier transform and the choice of the most appropriate access point. Though the method demonstrates improvement in secure transmission in the presence of PCA, a knowledge of the imperfect CSI is needed in order to localize LU and ED at its first stage, which represents the main drawback of the scheme. The PCA resistance of three other schemes based on different estimation algorithms is studied in [13], all of them operative only in cases where spatial information represented by angles of arrival is already available at the BS.

A random channel training scheme that is able to combat both jamming attacks during the uplink training phase and PCAs is proposed in [14]. This scheme relies on the estimation of legitimate and non-legitimate channels at the BS and the construction of secure beamforming in the downlink direction in order to minimize information leakage to ED. However, the assumption that the BS disposes of statistical information about its channels to LU and ED in advance makes the scheme unattainable in scenarios where prior channel knowledge is unavailable.

Another strategy that also implies random uplink transmission from a set of pilots but abstains from using threshold values to make its decision regarding PCA's existence consists of an analysis of the constellation diagram. This approach is at the basis of two distinct detection methods—an original one, referred to as *2-N-PSK* and firstly proposed in [15], and an improved one called *Shifted-2-N-PSK* detection method, that we proposed in our previous work in [16]. Common to both *2-N-PSK* and *Shifted 2-N-PSK* is the main idea: both the methods involve uplink transmission of a pair of pilot signals during the uplink training phase. The legitimate pilot signals are randomly chosen from an N-PSK constellation diagram, where N = 2^k and k is an integer number. In order to distinguish between the scenarios of presence or absence of attack, the methods require an analysis of two received N-PSK pilot signals, hence their names—*2-N-PSK* and *Shifted 2-N-PSK* detection methods. The correlation between the received pilots from the pair is computed at the BS. According to the argument of the correlation result, which is compared to the angles of a reference constellation, the BS detects intrusion if the correlation phase differs from the phases of the symbols from the reference constellation or reports PCA absence when its phase coincides with one of the referenced ones.

Though *2-N-PSK* and *Shifted 2-N-PSK* share the same detection criteria, the essential distinctions in the operation principles of the methods are shown in the constellation diagrams used for legitimate pilot transmission as well as those for correlation reference. While in the original *2-N-PSK* detection method a single N-PSK alphabet is used for uplink training and decision criterion, the improved method adopts pilots from shifted constellations, subsequently leading to a necessity for altering the reference constellation also. According to the general description of *Shifted 2-N-PSK*, each pilot is adjusted before transmission so that a predefined angle is added to its argument. Different supplementary angles are used for the pilots with odd numbers and those with even running numbers. Hence, two separate reference constellations are obtained—the correlation result computed between the first and the second pilot, forming the first pair of training signals, is compared to a constellation diagram depicting the odd correlations, with another constellation for the even correlations, such as the second one between the second and third received pilot. The aforementioned modifications in the improved method successfully increase the detection capabilities of the original method. However, depending on the choice of supplementary angles to shift the training signals, three different realizations of *Shifted 2-N-PSK* are outlined and, dependent on the choice of implementation scenario, the performance of the *Shifted 2-N-PSK* detection method varies.

1.2. Motivation

Although the detection probability of *2-N-PSK* and *Shifted 2-N-PSK* is studied in several research papers [15–17], there is still a lack of comprehensive investigation of the performance of the methods for different attack types and implementation scenarios. In conformity with their substance, both the methods can be considered as intrusion detection systems (IDSs). Usually, the effective operation of IDSs is examined through two widely used probability metrics, namely detection probability (DP) and false alarm probability (FAP). The DP is a measure of the capability of an IDS to successfully discover existing intrusions, while FAP provides information about the likelihood that the IDS reports an attack, even if there is not one. A study of the DP of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* for a single-antenna BS is given in [16], but the problem of FAP is not discussed there. Another study on both DP and FAP of *2-N-PSK* and *Shifted 2-N-PSK* in [17] includes massive MIMO with different numbers of antennae at the BS, but it is focused only on the best implementation scenario of *Shifted 2-N-PSK*, ignoring its other realizations. Moreover, an analysis of DP and FAP is not sufficient, since it does not give a complete view of the overall methods' performance.

To remedy this gap and give a holistic view of system performance, statistical evaluation metrics can be explored. Being IDSs, *2-N-PSK* and *Shifted 2-N-PSK* can be studied as binary classification models that distinguish between two possible classes—positive, when the IDS detects intrusion, or negative, if the IDS does not register any malicious intervention. In line with the relation of the predicted classes to the actual ones, different statistical parameters can be obtained that give information about the capabilities of the classification models to correctly predict the actual states or the different classification errors that they allow. Among the numerous classification metrics, those that are most commonly chosen for IDS performance evaluation are: *accuracy*, *precision*, *recall*, *Fβ-score*, *specificity*, and *fall-out* [18–20]. Due to existing interdependence between some of the parameters, a geometrical representation of the relation between them is also a powerful tool for IDS analysis, that is to say the receiver operation characteristic (*ROC*) curve and the precision recall (*PR*) curve of an IDS give valuable information about the effectiveness of the system. Since all of these classification metrics show different aspects of system operation, processed jointly they give exhaustive information about the overall system performance, therefore, for comparison purposes and to establish confidence in assessment criteria, *2-N-PSK* and *Shifted 2-N-PSK* can be best evaluated through such a study. The need for an overall assessment of the methods' operation, in order to be adequately analyzed and compared, serves as a motivation for this study.

The rest of the paper is organized as follows: in Section 2 the system model is introduced, the main issues concerning the performance of *2-N-PSK* and *Shifted 2-N-PSK* are outlined, and the statistical evaluation metrics used in the study are presented. In Section 3, simulation results are presented. An algorithm for the secure distribution of legitimate constellation shift values for *Shifted 2-N-PSK* is proposed in Section 4. A brief discussion follows in Section 5, and Section 6 concludes the paper.

2. Methodology: Performance Evaluation Through Probability and Statistics Metrics

2.1. System Model

In this study, the system model considered represents a single-cell massive MIMO system with TDD operation. Three nodes are incorporated in the communication process—a BS with multiple antenna elements, M in number, serves a single-antenna LU, while an ED, again equipped with a single antenna element, aims to disrupt the security of the system. In the interests of simplicity, user mobility is not considered in the system.

The random uplink channels of LU and ED are analytically expressed by their corresponding large-scale fading variables, denoted d_{LU} and d_{ED}, and small-scale fading coefficients—h_{LU} and h_{ED}. Apart from the relevant channel gains, the training signal received at the BS is influenced by the transmit power of LU and ED, assigned by P_{LU} and P_{ED}, and is subject to additive white Gaussian noise (AWGN).

During the uplink training phase, both LU and ED send their pilot signals to the BS, where the CSI is obtained. In order to detect malicious intervention, the BS processes the received pilot signals in pairs and computes their correlation, z_{12}, in accordance with Equation (1) [15]:

$$\begin{aligned} z_{12} = \tfrac{1}{M}\left(\sqrt{P_{LU}}d_{LU}h_{LU}p_1^{LU} + \sqrt{P_{ED}}d_{ED}h_{ED}p_1^{ED}\right)^H \times \\ \left(\sqrt{P_{LU}}d_{LU}h_{LU}p_2^{LU} + \sqrt{P_{ED}}d_{ED}h_{ED}p_2^{ED}\right) + n_{12} \end{aligned}, \quad (1)$$

where the LU training signals from the first and the second pilot intervals are ${p_1}^{LU}$ and ${p_2}^{LU}$, those of ED—${p_1}^{ED}$ and ${p_2}^{ED}$, n_{12} describes the resultant noise and the notation $(\cdot)^H$ represents the Hermitian conjugate of a matrix.

After obtaining the correlation result, the BS analyses its argument, $\varphi(z_{12})$. When it coincides with the angles from the reference constellation, no PCA is reported. Otherwise, an attack is detected. A flow chart of the algorithm involved in *2-N-PSK* and *Shifted 2-N-PSK* is given in Figure 1.

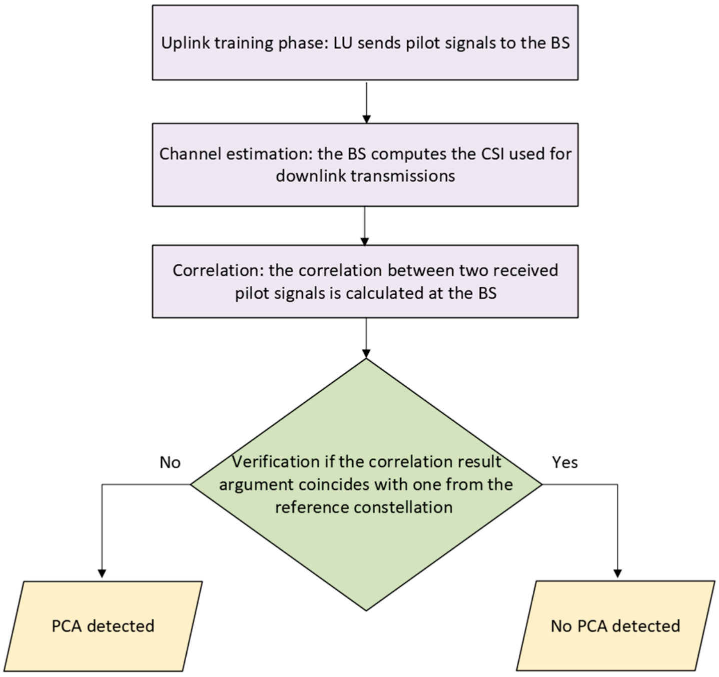

Uplink training phase: LU sends pilot signals to the BS
Channel estimation: the BS computes the CSI used for downlink transmissions
Correlation: the correlation between two received pilot signals is calculated at the BS
Verification if the correlation result argument coincides with one from the reference constellation
No
Yes
PCA detected
No PCA detected

Figure 1. Flow chart of the algorithm involved in *2-N-PSK* and *Shifted 2-N-PSK* [16].

Considering the *2-N-PSK* detection method, the LU sends pilot signals from a publicly known N-PSK constellation. Thus, the reference constellation used to compare the correlation result coincides with the original N-PSK constellation, whose angles are denoted φ_x(N-PSK). When the *Shifted 2-N-PSK* detection method is studied, it should be noted that it operates with pilots from shifted constellations. An offset angle of x_1 degrees is used to alter every pilot with an odd sequential number, and the even pilots are shifted by x_2 degrees. Consequently, the reference constellation diagram also changes in accordance with the offset values. The angle of every correlation that is odd in number—such as the first one, z_{12}—computed between the first and the second received pilots, must be compared with the angles of an odd reference constellation. The odd reference diagram is obtained by the addition of $(x_2 - x_1)$ to the original N-PSK angles. Likewise, the even correlation result angles, for instance the second one, z_{23}, between the second and the third received pilots, should match the phases of an even reference correlation, obtained by the addition of $(x_1 - x_2)$ to the original N-PSK angles.

Since the system is under the influence of noise, even if no PCA exists the correlation result angle may differ from the angles of the reference constellation. Therefore, to acquire authentic results the effect of noise must be taken into account. In an effort to achieve this, the authors of [15] propose a formula that describes the size of the area around each symbol from the reference constellation, where the angle fluctuations are presumed to be caused by noise. This area forms a tunnel around the reference points, whose width in either the positive or negative direction, denoted r, is defined in Equation (2). If the correlation result falls into the tunnel, also referred to as a detection region, it is assumed that its deviation from the reference symbol is a consequence of noise rather than a PCA.

$$r = c\frac{\sqrt{N_0\left(MN_0 + \frac{2P_{LU}d_{LU}^2\|h_{LU}\|^2}{M}\right)}}{M}. \tag{2}$$

In the equation above, N_0 is the noise power; c is a constant, used for scaling purposes; and $\|\cdot\|$ stands for Euclidean norm.

2.2. Main Issues Concerning the Performance of 2-N-PSK and Shifted 2-N-PSK Detection Methods

Up to the present, the DP of *2-N-PSK* and *Shifted 2-N-PSK* has been thoroughly studied in different attack scenarios [15,16]. In these studies, several types of PCAs stand out as being undetectable by the original *2-N-PSK* detection method, as the argument of the correlation result computed at the BS equals an angle from the reference N-PSK constellation. This situation occurs when any of the following conditions is present [16]:

1. The phase of each non-legitimate pilot from the pair coincides with the one of its corresponding legitimate pilot;
2. One of the non-legitimate pilots of the pair has a phase that is reciprocal to the phase of its corresponding legitimate pilot, and at the same time, the phase of the other non-legitimate pilot coincides with the one of its corresponding legitimate pilot or the phase of each non-legitimate pilot from the pair is reciprocal to the one of its corresponding legitimate pilot;
3. ED joins the training procedure during the transmission of the second legitimate pilot from the pair and the phases of the pilots of LU and ED coincide or are reciprocal;
4. The phases of both non-legitimate pilots of the pair differ from those of their corresponding legitimate pilots with the same angle.

Considering the operation principle of *Shifted 2-N-PSK* and the fact that ED does not have any knowledge about the shift values of legitimate constellations, the conditions for undetectable PCAs are modified. In order to initiate a successful attack, which results in a correlation angle that equals an angle from the corresponding reference constellation, for scenarios 1, 2, and 3. the arguments of ED have to be the arguments from the N-PSK constellation that are the closest to the arguments of the shifted pilots of LU or their reciprocals. In scenario 4. ED has to send the N-PSK angles whose arguments are the closest to those of the corresponding shifted pilots of LU plus the identical angle.

The effective performance of *Shifted 2-N-PSK* is strongly related to the offset values selected to change the legitimate N-PSK constellation, i.e., to the values of x_1 and x_2. The different realizations of the method and their detection capabilities are briefly described next [16,17]:

A. Neither the legitimate nor the reference constellations coincide with the original N-PSK constellation, i.e., $|x_1 - x_2| \neq \varphi_x$ (*N-PSK*) and $x_1 \neq x_2 \neq \varphi_x$ (*N-PSK*);

B. The legitimate constellation of one of the pilots from the pair, either the odd or the even, coincides with the original N-PSK constellation, while the other is shifted, i.e., $x_1 = \varphi_x$ (*N-PSK*) or $x_2 = \varphi_x$ (*N-PSK*);

C. The reference constellation used for the odd and the even correlation results coincides with the original N-PSK constellation, i.e., the offset values of both legitimate constellations differ from each other by an N-PSK angle, $|x_1 - x_2| = \varphi_\text{x}$ (N-PSK).

When *Shifted 2-N-PSK* is implemented conforming to *A*, in the absence of noise all PCA scenarios, undetectable for *2-N-PSK* and listed above are successfully revealed by *Shifted 2-N-PSK*. Case *B* is capable of coping with attack types 1, 2, 4, and 3 in most cases, except for the situation where the PCA is initiated during the transmission of the second legitimate pilot from the pair and this pilot is from the N-PSK constellation. When the realization in *C* is implemented, *Shifted 2-N-PSK* manages to discover PCAs of types 2 and 3. However, 1 and 4 are still undetectable. It is worth noting that these observations correspond to scenarios with an absence of noise. In real environments, where the noise power affects communication, its influence must be evaluated according to Equation (2) and taken into consideration.

2.3. Statistical Evaluation Metrics

Statistical evaluation metrics can be used as a means of comprehensively studying and comparing different classification models, as they provide a broad view on different parameters that can be variously weighted according to the particular application. In order to introduce the most widely used metrics, the confusion matrix must first be explained.

2.3.1. Confusion Matrix

The confusion matrix, as illustrated in Table 1, represents a table whose rows, two in number, contain the results of the actual classes—positive and negative—while the two columns stand for the test outcomes. Thus, the element of the matrix with indexes (1, 1) represents the number of test results correctly labeled as positive, i.e., this is the so-called true positive (TP) state. Matrix element (1, 2) holds the number of false negatives (FN), which counts the cases of positive actual states improperly classified as not having the condition. Element (2, 1) of the confusion matrix holds the actual negative samples that are erroneously labeled as positives, namely the false positives (FP). The last element of the matrix, with indexes (2, 2), is known as true negative (TN) state and relates to the number of samples that the classification model accurately evaluates as negatives.

Table 1. The confusion matrix—a basic representation.

		Test Outcome	
		Positive	**Negative**
Actual Class	**Positive**	TP	FN
	Negative	FP	TN

With the particular number of successful and failing predictions, the confusion matrix gives a clear view of the effective performance of classification models and the types of generated errors. Errors of the first kind, also known as Type I errors, are the FP examples, while an error of the second kind or Type II error corresponds to the FN state. According to the particular use of the classification model, one of the error types may have a severe influence on the application results, while the other may not have such a harmful impact. When considering attack detection, usually the cost of Type II error is higher since unrevealed attacks, for the most part, lead to much more detrimental results than the misleading detection of nonexistent intrusion. Thus, in this case, the weight of Type II error is higher.

Apart from giving an overview of correct predictions being made and the error types respectively, the data in the confusion matrix can be very useful when crucial statistical parameters for IDS assessment have to be computed. In the following subsections, the most frequently used classification metrics that provide exhaustive information on different aspects of classification model performance are explained. Then, in Section 3, both PCA detection methods—*2-N-PSK* and *Shifted 2-N-PSK*, will be evaluated through the obtained classification metrics from the conducted simulation study.

2.3.2. Accuracy

Accuracy is the parameter that shows the ability of the classification model to successfully recognize the actual state of a sample [21]. Thus, it accounts for the true test predictions from all classification outcomes. Having the results of the confusion matrix, *accuracy* can be computed according to Equation (3) [22]:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}. \tag{3}$$

High *accuracy* testifies to satisfactory classification model performance. However, relying solely on *accuracy* results could be specious if imbalanced distribution of classes is observed [23].

When the test outcome classes—positive and negative—are not equally present in the training set, the class with fewer examples is referred to as the minority class, while the other is known as the majority class. On the one hand, in the case of a large gap between the majority and minority class, notwithstanding the high *accuracy* value, a classification model may still demonstrate poor capabilities in correct recognition and labeling TP, since they belong to the minority class, which may be characterized with a very few examples in the training set. Hence, for imbalanced classification, *accuracy* could not be a trustworthy metric and others that study the minority class must be observed. Such metrics are *recall* and *precision*.

On the other hand, as *accuracy* does not study the erroneously labeled samples, it gives proportional rates of Type I error and Type II error, making it an impractical metric if one of the error types is with higher cost in the specific scenario of use. Using a metric that focuses on the error type of interest could be more useful.

2.3.3. Precision or Positive Predictive Value (PPV)

One of the metrics that is appropriate for imbalanced distribution of classes, is *precision*, also called *PPV* and calculated according to Equation (4). It is concentrated on the minority class and gives the part of positive test results that are actually positive, i.e., it measures the accuracy of the minority class, showing the reliability of positive predictions and quantifying FP [24].

$$PPV = \frac{TP}{TP + FP}. \tag{4}$$

Though a high *PPV* value testifies to accurate positive predictions and low Type I error, it does not contain any information about the error of Type II, and it permits the possibility of having a large number of actual positive samples that the classification model is incapable of labeling correctly. In case of robust imbalance between classes, a very low number of samples from the minority class exists, so even correct classification of the positive predictions does not ensure a low number of FN [23]. Consequently, when in the specific utilization scenario, the value of FN is with high cost, together with *PPV* it is appropriate to study another classification metric that gives information for Type II error.

2.3.4. Recall or Sensitivity

While precision gives information about the part of positive test results that are indeed positive, *recall*, *sensitivity*, or *True Positive Rate* (*TPR*) shows the accurate predictions from the minority class as a fraction of all real positive samples. With the results from the confusion matrix, recall can be computed by Equation (5) [24]:

$$TPR = \frac{TP}{TP + FN}. \tag{5}$$

In addition to focusing on the minority class, *recall* contains information about the error from the majority class, since the value of FN can easily be subtracted from recall as the sum of its rate and *TPR* equals 1. Analyzing *sensitivity* on its own does not reveal the amount of FP. Hence, the large *sensitivity* can be related to many errors from the minority class, lowering the *precision* value. As both the metrics are in inverse-proportional conjunction, they must be studied together in order to find their most suitable interconnection according to the cost of errors in the particular application.

2.3.5. $F\beta$-Score

The parameter that distinguishes the impact of *precision* and *recall* by assessing the cost of the errors of the first and second kind, is the *Fβ-score* [23]. It is computed from *PPV* and *TPR* as in Equation (6)

$$F_\beta = \left(1 + \beta^2\right) \times \frac{precision \times recall}{(\beta^2 \times precision) + recall} = \frac{(1 + \beta^2) \times TP}{(1 + \beta^2) \times TP + \beta^2 \times FN + FP}, \tag{6}$$

where β denotes a scaling factor for balancing the weight of both metrics in the final result. If β = 1, the equation in (6) takes the form of the harmonic mean of *precision* and *recall* giving equal weight to both parameters, as shown in Equation (7). The larger the value of β is, the more emphasis is put on *recall* by limiting the Type II error at the expense of Type I error, causing loss of *precision*.

$$F_1 = 2 \times \frac{precision \times recall}{precision + recall} = \frac{TP}{TP + \frac{FP+FN}{2}}. \tag{7}$$

The value of *Fβ-score* varies in the interval [0, 1], and the higher it is, the better the performance, such that the ideal operation of the classification model corresponds to no errors of either kind, resulting in *Fβ-score* = 1 [25].

2.3.6. Specificity or True Negative Rate (TNR)

Another statistical metric that can be analyzed to study the performance of a classification model concerning the majority class is the *specificity*, also known as *TNR*. While *sensitivity* measures the portion of all actual positive samples that are accurately labeled, *specificity* relates to the confidence in the classification model to properly define the samples that do not have the condition under study [24]. Calculated according to Equation (8), the *TNR* contains information for the negative class and can be used to subtract the number of Type I errors as well.

$$TNR = \frac{TN}{TN + FP}. \tag{8}$$

2.3.7. Fall-Out or False Positive Rate (FPR)

The parameter known as *fall-out* or *FPR* complements *specificity* as it shows what number of all actual negative samples are mislabeled and are thus Type I errors:

$$FPR = \frac{FP}{FP + TN} \tag{9}$$

Having the same denominator as *specificity*, the *fall-out* is an assessment of the error from the minority class with respect to actual negatives.

2.3.8. ROC Curve and ROC AUC

A separate study of the abovementioned metrics can be beneficial to a narrow analysis focusing on the specific element to consider. However, each of them shows a limited aspect of the system operation, neglecting either the majority or minority class and focusing on either the true test outcomes or the classification errors. An assessment of the overall performance of the classification model requires a more exhaustive investigation of the different statistical parameters, showing the system operation from various points of view. Meanwhile, the parameters that are in certain relation to each other, such that the increase in one of them leads to an increase or a loss in the other, and vice versa, must be evaluated in pairs in an attempt to find an acceptable trade-off that optimizes the overall performance for the specific application. Such pairs of interdependent metrics are *sensitivity–fall-out* and *precision–recall*. An elegant solution for the concurrent analyses of both metrics in the couple is provided by the graphical representation of one of the parameters as a function of the other [26]. Considering the relationship between *sensitivity* and *fall-out*, the illustrative graph is called the *ROC* curve.

According to the nature of *TPR* and *FPR*, though a classification model demonstrates satisfactory performance when low *fall-out* together with high *sensitivity* are observed, both metrics are connected in a direct ratio to one another. Hence, a rise in *TPR* is followed by an increase in the value of *FPR* [23]. For that reason, a good analysis of the *ROC* curve for the whole threshold range can be a helpful tool to choose the decision threshold whose values of *sensitivity* and *fall-out* best suit the application scenario. Best effectiveness of the classification method is achieved when all actual positive samples are labeled TP and at the same time no FP exists, which corresponds to the point in the upper left corner of the *ROC* area with coordinates (0, 1). Classification performance can be evaluated as high when its *ROC* curve comes close to that point.

Comparing the behavior of different *ROC* curves is difficult, since for some thresholds, one of the classification models may dominate over the other, while for other decision values this tendency may change. A parameter that is computed like the area under the *ROC* curve—accordingly named *ROC AUC* and having a value in the range [0, 1]—can be used instead [25]. The higher the *ROC AUC* value, the greater the assessment of classification model.

2.3.9. PR Curve and PR AUC

The *PR* curve is ordinarily used as a representation of the inversely proportional relation between the *precision* and the value of *recall*. The dependency from one another of *PPV* and *TPR* consists of the growth in one of them leading to a fall-off in the other. Meanwhile, a reliable classification model is expected to demonstrate trustworthy predictions about positives of the minority class together with strong abilities to discover the actual positive samples. In other words, perfect performance is achieved when no FP or FN exist, setting the *precision* and *recall* to their maximal values—i.e., both *PPV* and *TPR* equal one, which is the upper right corner of the *PR* graph. The closer the *PR* curve is to the point with coordinates (1, 1), the more powerful the classification model [23]. Another option to analyze the overall relation between *precision* and *recall* is by the *PR AUC*, which, as with the *ROC AUC*, measures the area under the *PR* curve and summarizes the *PR* results for all decision thresholds into a single value. The *PR AUC* could range between [0, 1] with its most advantageous significance at its maximum.

When considering whether to apply either *PR* or *ROC* analysis, the following observations must be taken into account: although both the curves can be used for imbalanced datasets, in the case of a large gap between classes, the *PR* curve that lays emphasis on the minority class through precision is more appropriate than the *ROC* curve, which gives equal attention to both classes; furthermore, in *ROC* analyses, the same weight is given to both Type I and Type II errors, making the *PR* curve more informative in case of significant importance of the error of the first kind.

3. Simulation Results

In this study, the performance of *2-N-PSK* and *Shifted 2-N-PSK* detection methods is evaluated by conducting a large number of computer simulations with the following conditions. In all simulations, the fading coefficients of the legitimate and non-legitimate channels are generated as independent complex Gaussians with zero mean and unit variance. The pilot signals of LU and ED are also randomly selected from the corresponding constellation diagram—8-PSK alphabet is used for the pilots of both the users in *2-N-PSK*, while in *Shifted 2-N-PSK*, the LU shifts the 8-PSK angles to obtain the legitimate constellation. The shift values adopted for the experiments of realization *A* of *Shifted 2-N-PSK* are $x_1 = 11^\circ$ and $x_2 = 18^\circ$; case *B* is implemented with $x_1 = 19^\circ$ and $x_2 = 0^\circ$; and for case *C*, $x_1 = x_2 = 7^\circ$ is used.

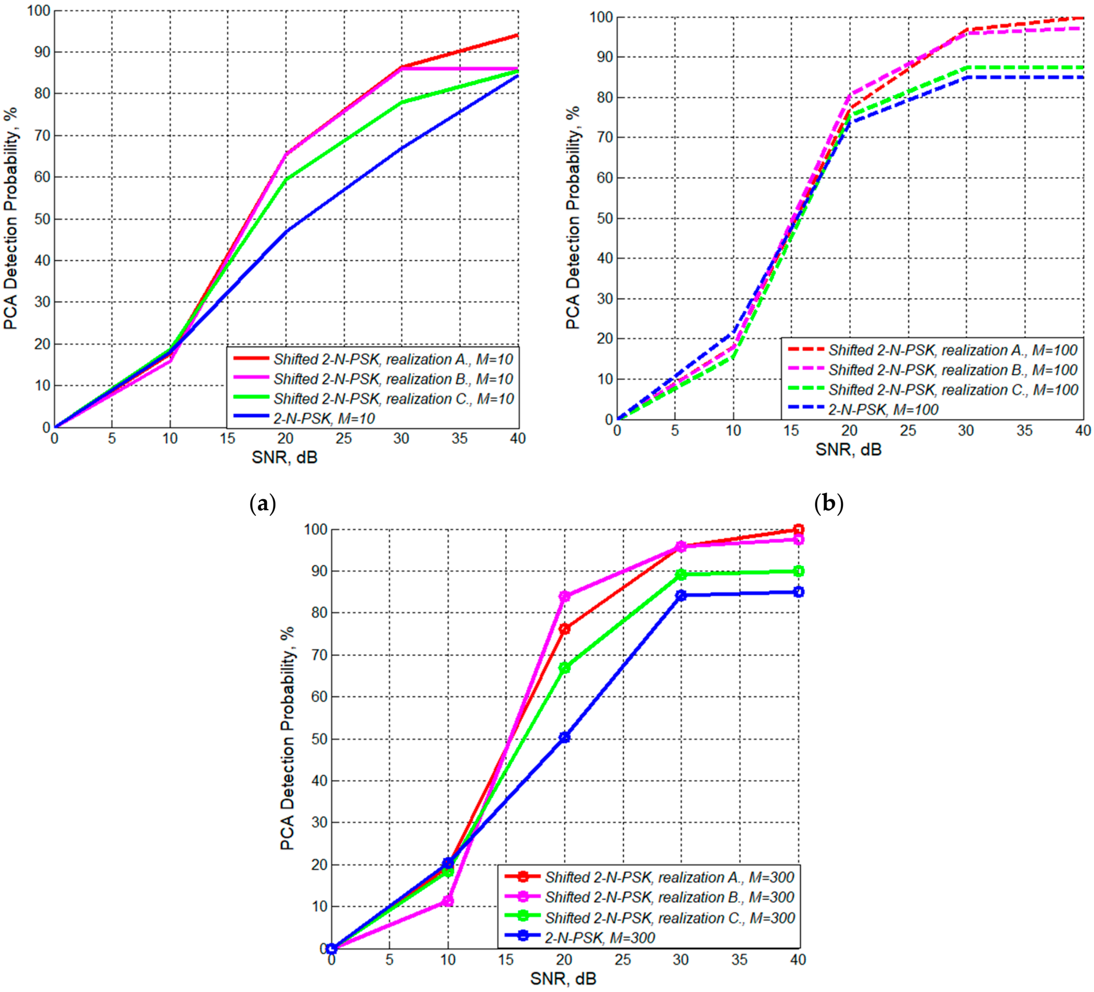
Since the correlation result as well as the detection region are both computed according to the size of the BS antenna array, most of the experiments are conducted in antenna numbers $M = 10$, $M = 100$, and $M = 300$ in order to investigate the influence of the increment on system performance.

For the purposes of the *ROC* and *PR* analyses, the curves are plotted when changing the decision criterion, referred to as a threshold value. When the *2-N-PSK* and the different implementations of *Shifted 2-N-PSK* are investigated, the decision threshold is actually the size of the detection region, which determines whether the test outcomes are positive or negative. In this study, the threshold values are chosen to vary between 0 and 0.2 in increments of 0.001. When the *ROC* and *PR* curves are evaluated in varying SNRs, the results of 10,000 computer simulations are averaged for each threshold, while for the investigation of the curves with different antennae, the mean value of 200,000 simulation results is taken.

3.1. Evaluation of 2-N-PSK and Shifted 2-N-PSK Detection Methods Through Probability Metrics

The DP and FAP of *2-N-PSK* and the three different realizations of *Shifted 2-N-PSK* are investigated in scenarios with different number of antenna elements at the BS. For each signal to noise ratio (SNR) and antenna implementation, the results of 200,000 computer simulations are analyzed. An important consideration in such a study is that the detection region must be fine-tuned for the different antenna arrays. This could be achieved by the proper selection of the scaling factor *c*, used in Equation (2), where the detection region *r* is defined. The larger the antenna number, the higher the value of the scaling coefficient needed.

The DP results as a function of the SNR for three different massive MIMO systems with $M = 10$, $M = 100$ and $M = 300$ antennae at BS are illustrated in Figures 2 and 3. While Figure 2 shows the DP of all method realizations in separate antenna array scenarios, Figure 3 gives individual representations of each method realization for the differing antenna values. The corresponding FAPs are represented in Figure 4, where each antenna case is studied for all the methods, and Figure 5, where the methods are separately studied for all values of *M*.

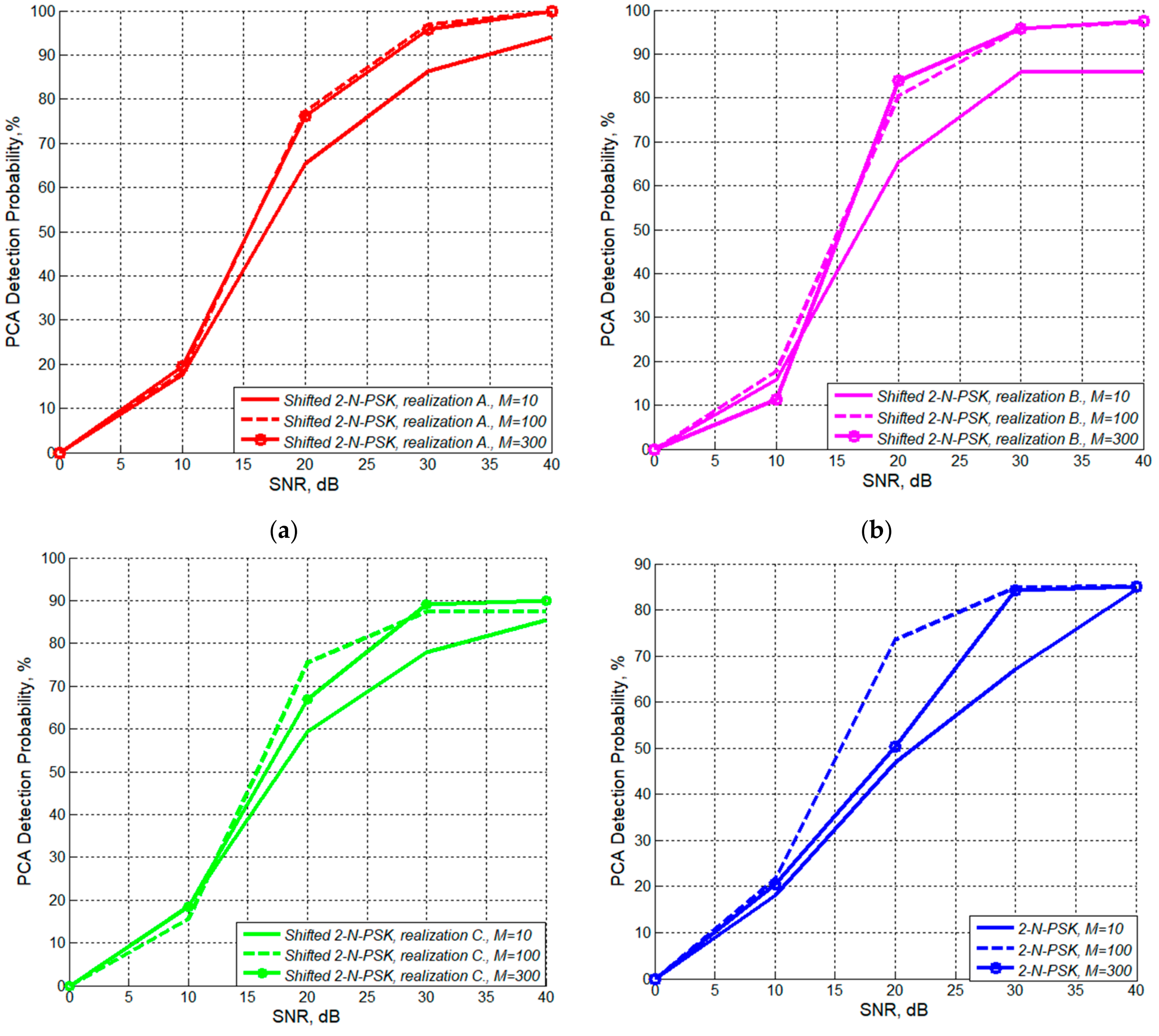


(**a**) (**b**)

(**c**)

Figure 2. PCA DP of *2-N-PSK* and the realizations of *Shifted 2-N-PSK* for different numbers of antenna elements at the BS: (**a**) $M = 10$; (**b**) $M = 100$; (**c**) $M = 300$.

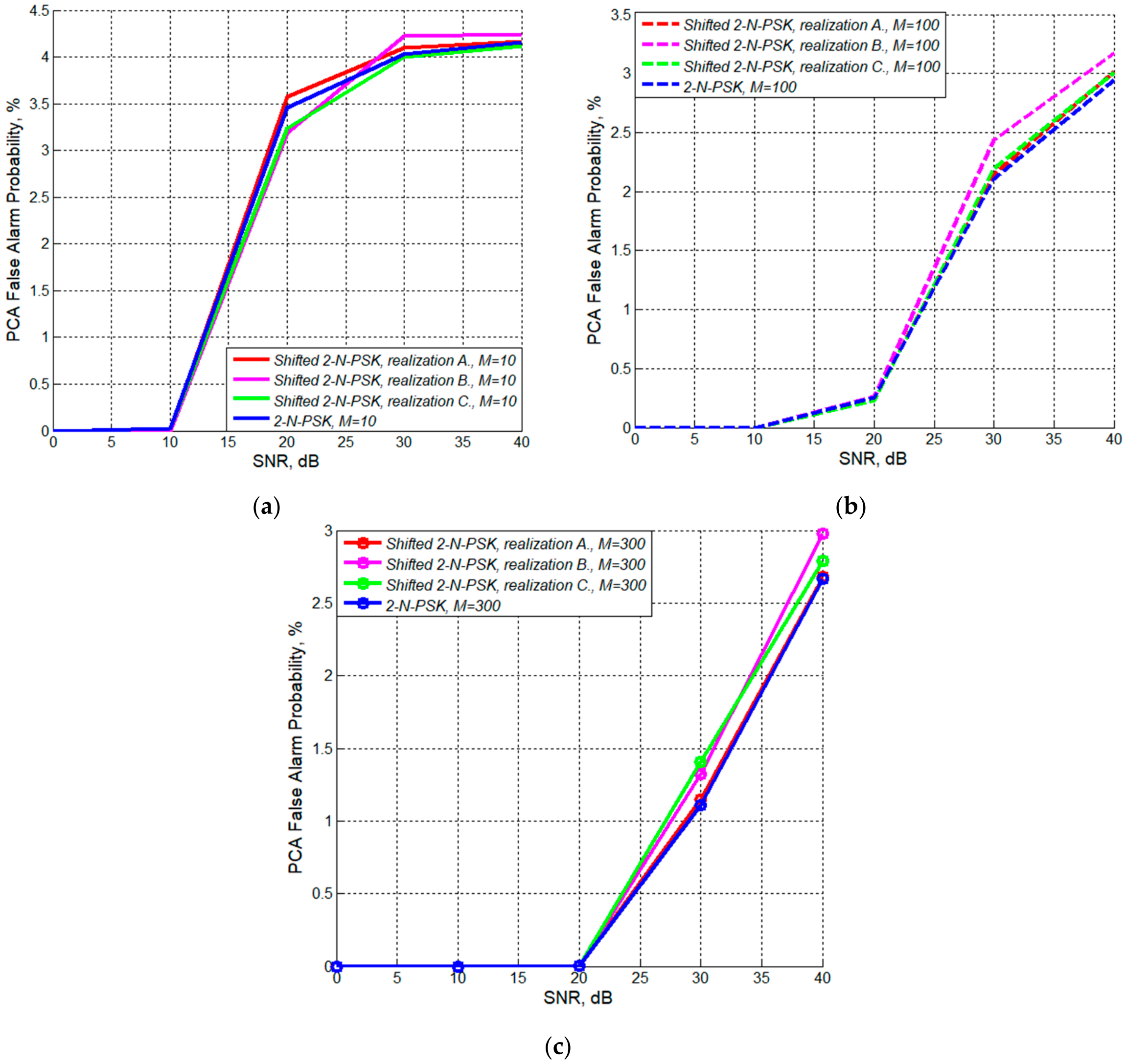
Most of the results illustrated in Figure 2 confirm the observations in [16] that the *Shifted 2-N-PSK* method is superior to the original *2-N-PSK*, and its realization *A* demonstrates the best DP among the other realizations, followed by case *B* and scenario *C*, which relates to the weakest *Shifted 2-N-PSK* implementation with respect to DP. However, the system model in [16] incorporates a single antenna BS. As a consequence of increasing the antenna array size, a rearrangement is observed in the results of Figure 2 in the lower SNR region. The change concerns mostly the behavior of realization *B*, whose results in SNR = 10 dB deteriorate compared to the other methods. Surprisingly, when SNR = 20 dB, especially in the scenarios of *M* = 100 and *M* = 300, the DP of case *B* outnumbers that of *A*. Regardless of the antennae number, in the higher SNR region, the DP results of the different methods improve in the order: *2-N-PSK*, *Shifted 2-N-PSK*, realization *C*; *Shifted 2-N-PSK*, realization *B*; *Shifted 2-N-PSK*, realization *A*.



(**a**) (**b**)

(**c**) (**d**)

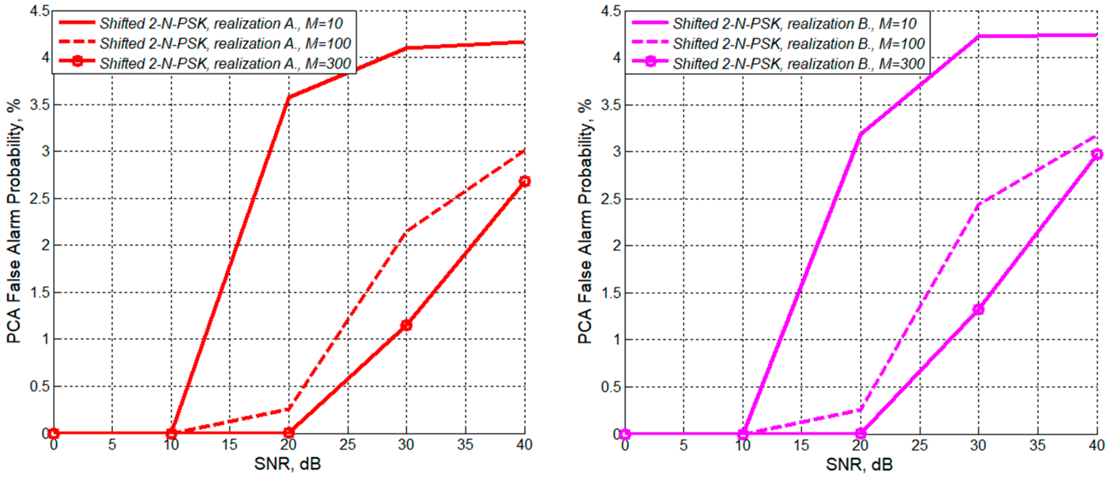
Figure 3. PCA DP for different numbers of antenna elements at the BS—individual representation of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK*: (**a**) *2-N-PSK*; (**b**) *Shifted 2-N-PSK*, realization *A*; (**c**) *Shifted 2-N-PSK*, realization *B*; (**d**) *Shifted 2-N-PSK*, realization *C*.



(**a**) (**b**)

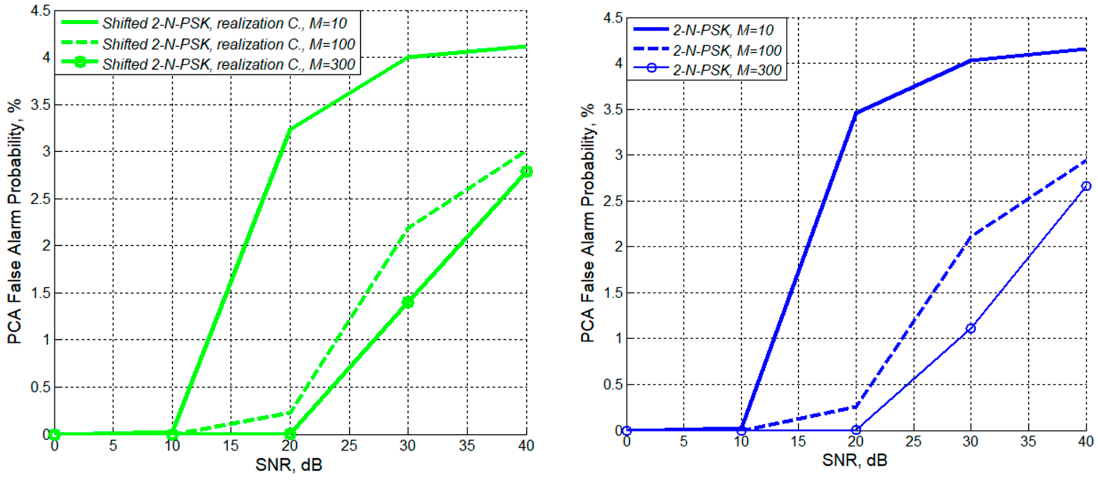
(**c**)

Figure 4. PCA FAP of *2-N-PSK* and the realizations of *Shifted 2-N-PSK* for different numbers of antenna elements at the BS: (**a**) *M* = 10; (**b**) *M* = 100; (**c**) *M* = 300.



(**a**) (**b**)

Figure 5. *Cont.*



(**c**)

(**d**)

Figure 5. PCA FAP for different numbers of antenna elements at the BS—individual representation of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK*: (**a**) *Shifted 2-N-PSK*, realization *A*; (**b**) *Shifted 2-N-PSK*, realization *B*; (**c**) *Shifted 2-N-PSK*, realization *C*; (**d**) *2-N-PSK*.

Summarizing the simulation results in Figure 2, several very significant observations can be emphasized. While in most SNR scenarios, the DP of all *Shifted 2-N-PSK* realizations improve over the one of *2-N-PSK*, an exception is the scenario with SNR = 10 dB, in which for all antenna numbers the original *2-N-PSK* demonstrates improved results compared to the realizations of *Shifted 2-N-PSK*. More specifically, for M = 100 and SNR = 10 dB, the DP of *2-N-PSK* is 3.86% more than the DP of realizations *A* and *B* and is 6.12% more than the DP of realization *C*. When SNR = 20 dB, the reverse tendency is observed, where realization *B* leads, outperforming *A*, *C*, and *2-N-PSK* by 3.26%, 4.98% and 6.94%, respectively. Increasing the SNR to 30 dB results in the highest DP of realization *A*, which approaches 96.81% and improves the results of *B*, *C* and *2-N-PSK* by 1.04%, 9.47%, and 11.86%, respectively.

The results in Figure 3 show the influence of M on the DP of each of the methods studied. When SNR = 20 dB, the DP of realization *B* improves by 15.19% when increasing the antenna number from M = 10 to M = 100. However, only 3.46% improvement in the DP is observed with the increase in M from 100 to 300. When realization *A* is considered, the increase in M from 10 to 100 improves the DP by 11.93%, while raising the antennae from 100 to 300 shows a DP reduction of 0.98%. On the one hand, indisputable improvement in the detection capabilities of the methods is observed when the antenna number increases from 10 to 100. On the other hand, the small difference between the PCA DP obtained with M = 100 and M = 300, being in some SNR cases in favor of M = 100, brings up the question whether it is reasonable to expand the antenna array up to several hundred elements, leading to higher system complexity and energy consumption.

When referring to Figure 4, small variations in the FAP of the different PCA detection methods can be observed for each of the antenna scenarios. Although these variations are mostly in favor of *2-N-PSK*, the fluctuations between the FAP of all the methods are less than 1%, a difference that could be a consequence of the random nature of the channels and the influence of complex Gaussian random noise in the simulations and hence may be ignored. More specifically, comparing the FAP values, again for M = 100, when SNR = 10 dB, all methods have a false alarm rate that approaches 0%. When SNR = 20 dB, a negligible difference of several centesimal in FAP results is observed. In the case of SNR = 30 dB, the best FAP of 2.105% is demonstrated by *2-N-PSK*. However, the value of the worst result, given by realization *B*, raises the FAP by only 0.33%, while *C* and *A* worsen the FAP of *2-N-PSK* by 0.08% and 0.07%, respectively. Therefore, compared to the difference in the DPs of the methods, the FAPs variations are relatively small and may be disregarded.

As opposed to the faltering DP results in Figure 3, where in some SNRs the DP of M = 100 improves on the one obtained with M = 300, Figure 5 proves the expectations that the higher the antenna number, the better the FAP. Even though increasing the antennae from 10 to 100 provides a several percent decrease in the FAP value, around 3% for each method realization in SNR = 20 dB scenario, only a slight increase of approximately 0.2% is observed when M grows from 100 to 300.

Since it is difficult to evaluate the overall performance of PCA detection methods by two distinct parameters that are mutually bounded to a certain extent—DP and FAP, a more exhaustive assessment of the methods' performance that facilitates their comparison is needed. One promising approach is to study the binary classification metrics commonly used for the assessment of IDSs.

3.2. Evaluation of 2-N-PSK and Shifted 2-N-PSK Detection Methods Through Binary Classification Metrics

In order to obtain the binary classification metrics of *2-N-PSK* and *Shifted 2-N-PSK* together with the different realizations of the latter, their confusion matrices are firstly needed. In this study, the confusion matrices are retrieved from the execution of ten independent experiments, each with a large number of computer simulations, 200,000. The original *2-N-PSK* detection method shows TP results that fluctuate in a wide range between 49% and 75% of all actually positive values. In order to present objective results, the outcomes of the different experiments are averaged. The experimental results whose *2-N-PSK* TP value is closest to the averaged one are chosen to be given next. It is worth noting that all implementation scenarios—*A*, *B*, and *C*—of the *Shifted 2-N-PSK* detection method demonstrate stable operation with only slight variations in the predicted results. In this attempt, all simulations are executed with the number of antenna elements at the BS M = 100, and a fixed SNR value of 20 dB applied.

The confusion matrices of *2-N-PSK* and realizations *A*, *B*, and *C* of *Shifted 2-N-PSK* can be correspondingly observed in Tables 2–5.

Table 2. Confusion matrix of *2-N-PSK* detection method.

Total Number of Simulations = 200,000		**Test Outcome**	
		Positive	**Negative**
Actual Class	**Positive**	TP = 57,628	FN = 42,372
	Negative	FP = 557	TN = 99,443

Table 3. Confusion matrix of *Shifted 2-N-PSK* detection method in realization *A*.

Total Number of Simulations = 200,000		**Test Outcome**	
		Positive	**Negative**
Actual Class	**Positive**	TP = 77,613	FN = 22,387
	Negative	FP = 559	TN = 99,441

Table 4. Confusion matrix of *Shifted 2-N-PSK* detection method in realization *B*.

Total Number of Simulations = 200,000		**Test Outcome**	
		Positive	**Negative**
Actual Class	**Positive**	TP = 82,992	FN = 17,008
	Negative	FP = 600	TN = 99,400

Table 5. Confusion matrix of *Shifted 2-N-PSK* detection method in realization *C*.

Total Number of Simulations = 200,000		**Test Outcome**	
		Positive	**Negative**
Actual Class	**Positive**	TP = 64,180	FN = 35,820
	Negative	FP = 557	TN = 99,443

According to the results in the confusion matrices, all the methods demonstrate similar prediction capabilities with respect to the negative class. This can be related to the values of FAP, which are almost equal for all the methods, as stated above. Though the methods result in an identical number of Type I errors, they exhibit diverse capabilities to predict the samples of the positive class, and the corresponding Type II error varies. The largest gap of around 25,000 successfully revealed attacks is observed between the TP values of the original *2-N-PSK* and *Shifted 2-N-PSK* in case *B*.

Having the confusion matrices of the PCA detection methods, the other crucial parameters for statistical evaluation of IDSs are easy to acquire. The computed classification metrics—namely the *accuracy*, *precision* and *recall*, *F1-score*, *specificity*, and *fall-out*—of *2-N-PSK* and *Shifted 2-N-PSK* are illustrated in Figure 6.

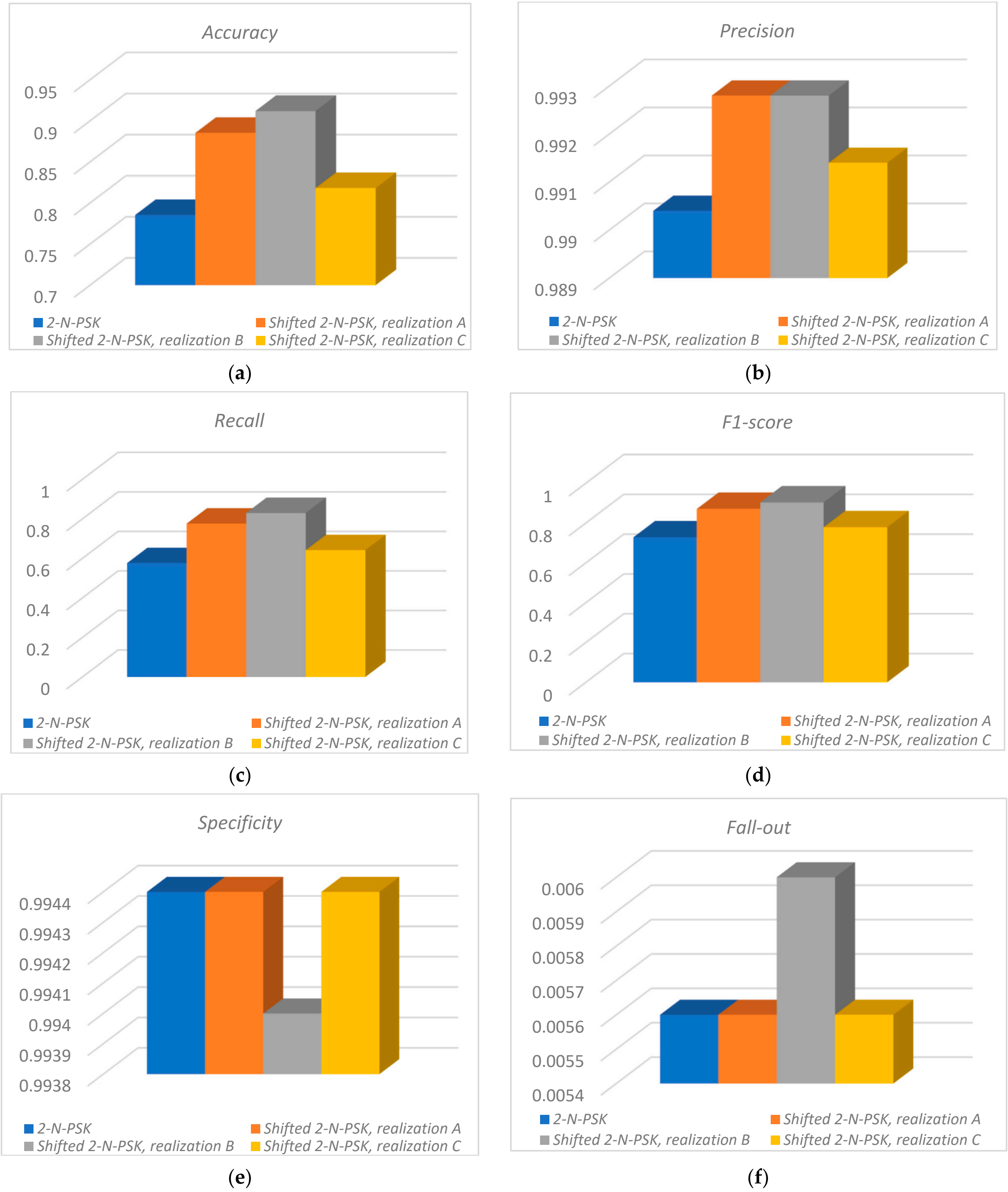
An overview of the parameters included in Figure 6 gives a very informative insight into the methods' performance. Undoubtedly, scenarios *A* and *B* of *Shifted 2-N-PSK* surpass the other methods in accuracy. Their dominating behavior is additionally proved by the values of *precision*, *recall* and their balanced joint representation *F1-score*. While scenarios *A* and *B* demonstrate equal *precision*, a slight superiority can be observed in the *accuracy*, *recall*, and *F1-score* of *Shifted 2-N-PSK* in realization *B*. Despite the smallest *specificity* and largest *fall-out* of the method in case *B*, the difference in these metrics between *B* and the other methods is only of the order of 0.0004, which is negligible compared to the excellence of scenario *B* to the other methods when the rest of the metrics are considered.

Following next is another important study of the joint evaluation of interconnected classification metrics. As discussed in Section 2, finding an appropriate balance between *sensitivity* and *fall-out* and between *precision* and *recall* is a challenge. To solve this problem and find a suitable trade-off between these pairs of metrics, their relationship can be graphically presented by the *ROC* and *PR* curves. Figure 7 illustrates the *ROC* curves of the methods for SNR scenarios varying from 0 to 40 dB.

The *ROC* curves in Figure 7 show that only if the power of noise equals that of the signal does *2-N-PSK* compete with the method with shifted constellations. For all SNRs, the *ROC* curve of the original method is commensurate with implementation *C* of *Shifted 2-N-PSK*, and the *ROC* results of realizations *A* and *B* go together with a small superiority of *B* over *A* when SNR = 10 dB and a reverse tendency in the other SNR cases.

In Figure 8, the *ROC* curves for the different SNR values are separately given for each of the methods. Not surprisingly, the higher the SNR, the better the *ROC*.

For comparison purposes, it may be difficult to follow the behavior of the curves as their tendency can vary with the distinguishing decision criteria used to plot the curves. For that reason, the *ROC AUC* values for the different SNRs are given in Table 6. In spite of the similarity in the *ROC* curves of cases *A* and *B* of *Shifted 2-N-PSK*, the *ROC AUC* results in the table confirm that SNR = 10 dB is the only scenario in which *B* outperforms *A* by 0.85%. The *ROC* evaluation over all SNR cases is in favor of realization *A*. The results of SNR = 20 dB could serve as an example—in this case, realization *A* improves the *ROC AUC* of realizations *B* and *C* and the original *2-N-PSK* by 0.36%, 4.57%, and 4.44%, respectively.

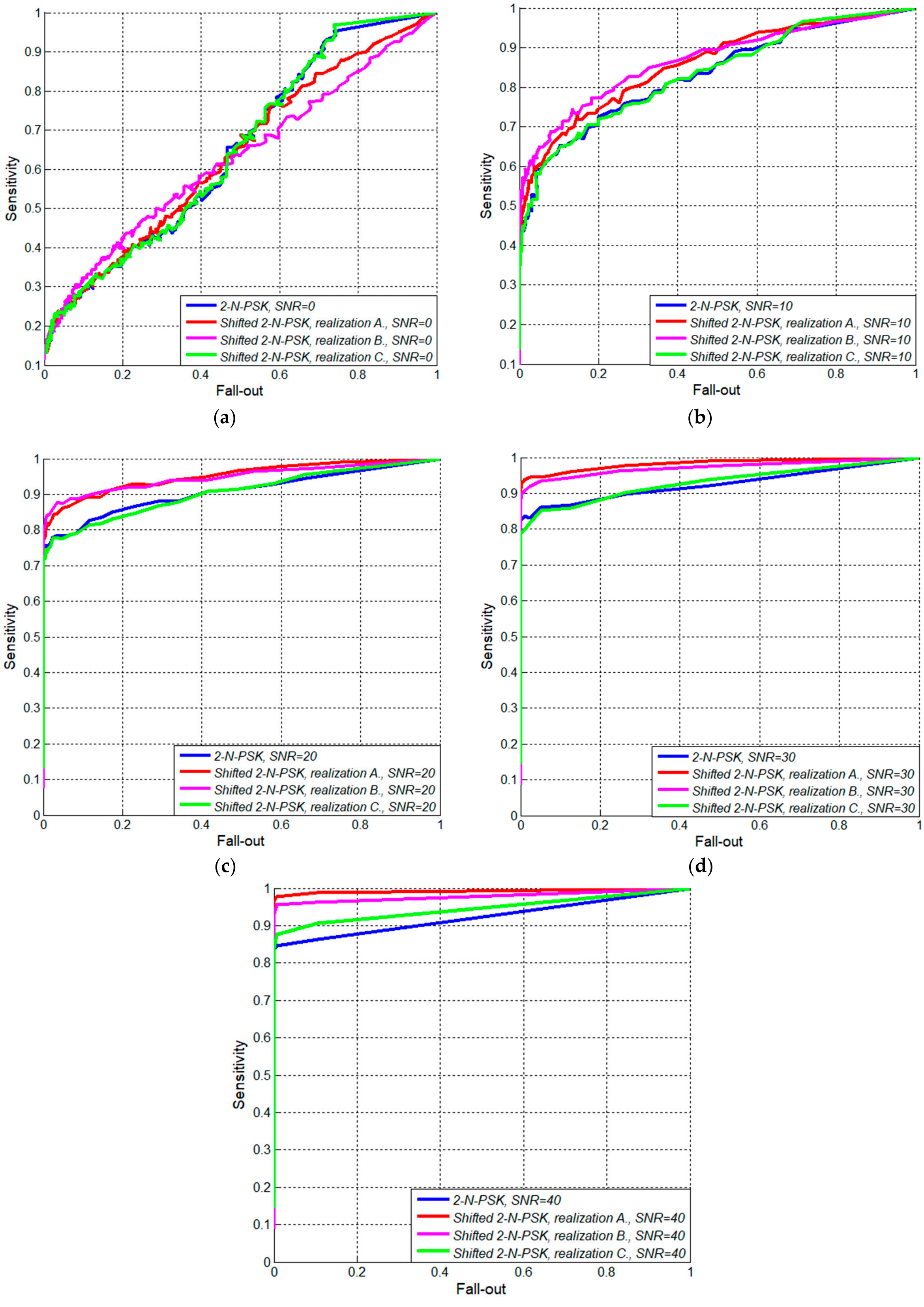


(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

Figure 6. Classification metrics of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK*: (**a**) *Accuracy*; (**b**) *Precision*; (**c**) *Recall*; (**d**) *F1-score;* (**e**) *Specificity*; (**f**) *Fall-out*.

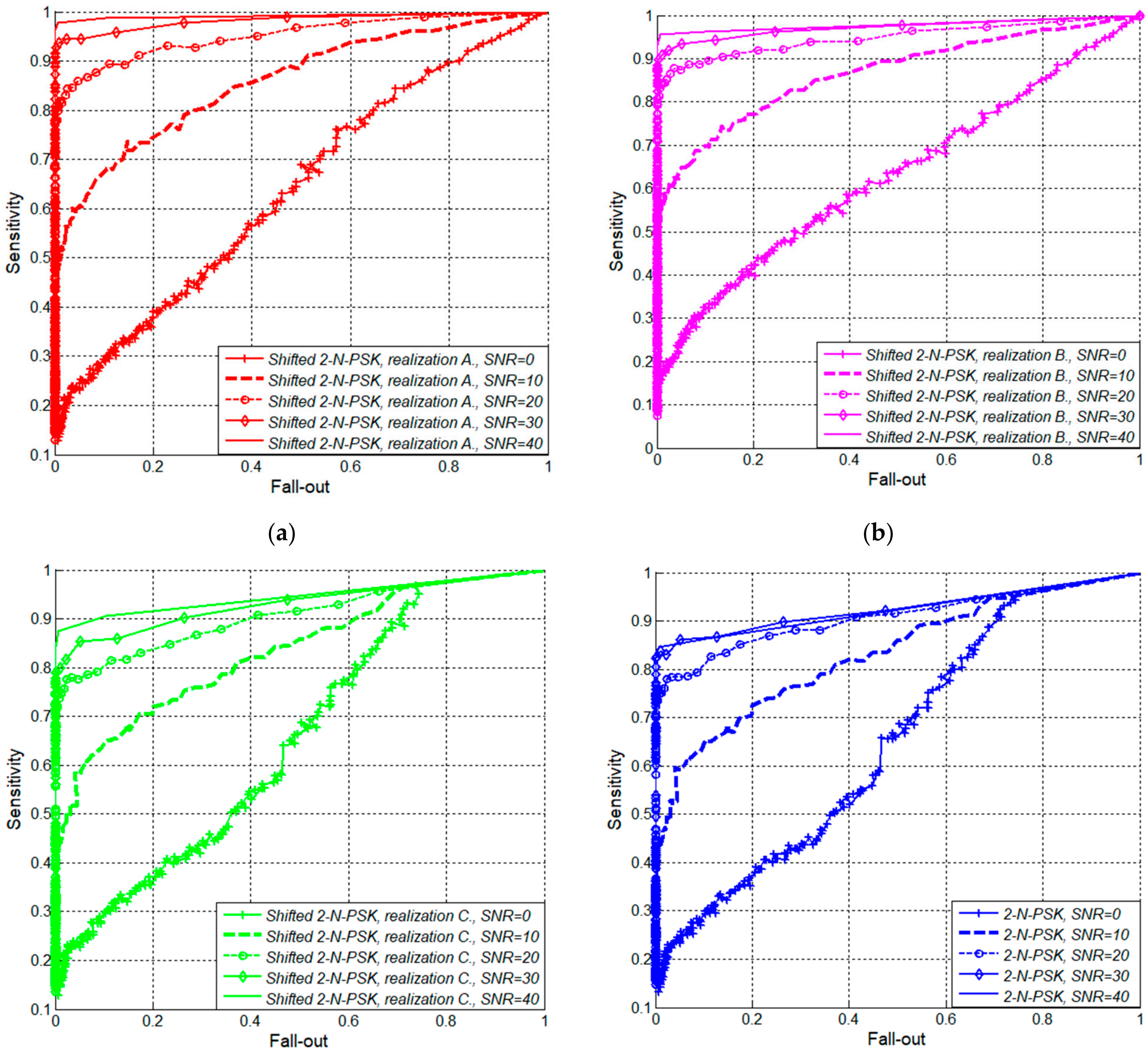


(**a**) (**b**)

(**c**) (**d**)

(**e**)

Figure 7. *ROC* curves for different SNR scenarios: (**a**) SNR = 0 dB; (**b**) SNR = 10 dB; (**c**) SNR = 20 dB; (**d**) SNR = 30 dB; (**e**) SNR = 40 dB.



(**a**) (**b**)

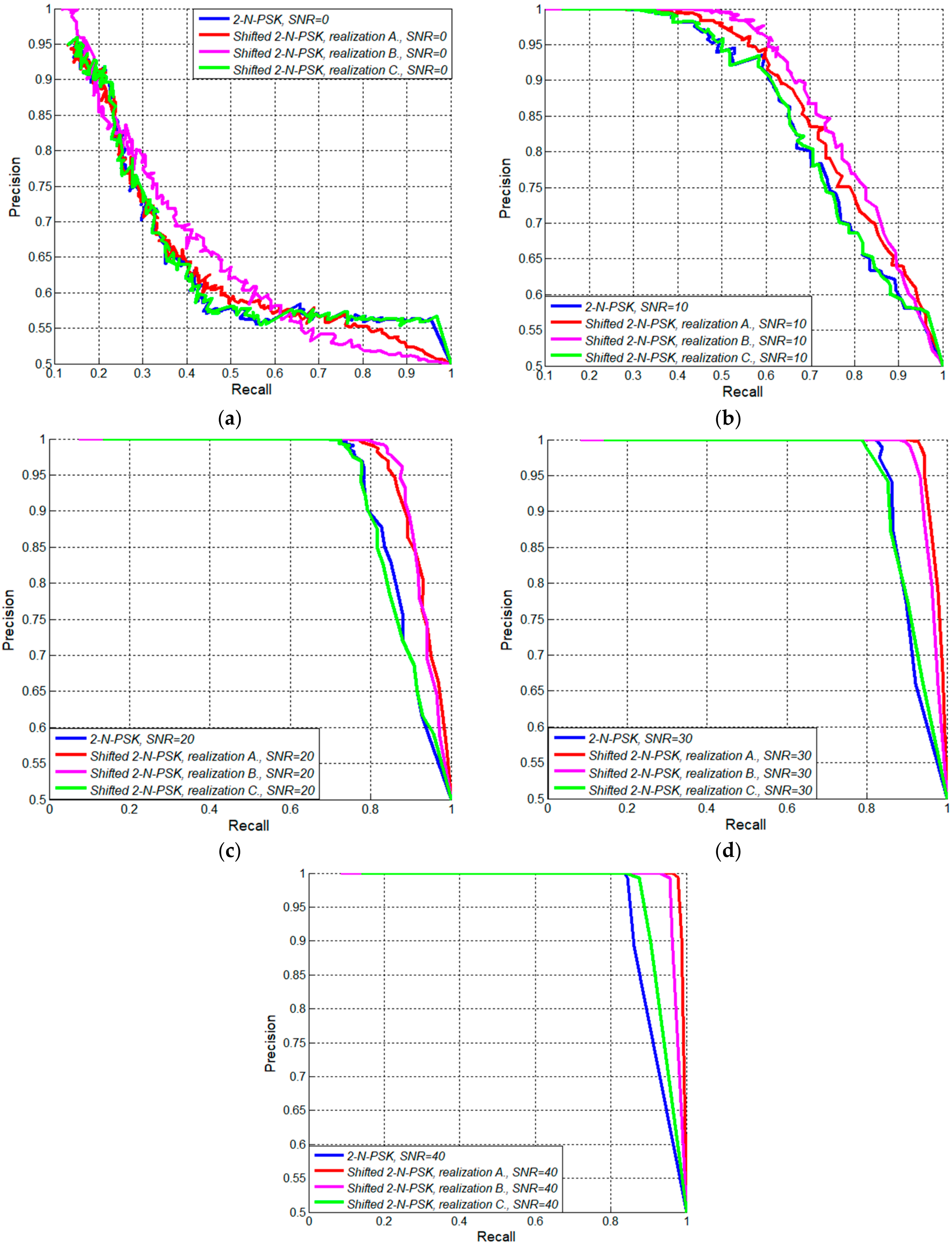
(**c**) (**d**)

Figure 8. *ROC* curves—individual representation of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK*: (**a**) *Shifted 2-N-PSK, realization A*; (**b**) *Shifted 2-N-PSK, realization B*; (**c**) *Shifted 2-N-PSK, realization C*; (**d**) *2-N-PSK*.

Table 6. *ROC AUC* of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* in different SNR scenarios.

ROC AUC	**Signal-to-Noise-Ratio**				
	SNR = 0 dB	**SNR = 10 dB**	**SNR = 20 dB**	**SNR = 30 dB**	**SNR = 40 dB**
2-N-PSK	0.6499	0.8318	0.9075	0.9257	0.9230
Shifted 2-N-PSK, realization A	0.6368	0.8586	0.9519	0.9829	0.9924
Shifted 2-N-PSK, realization B	0.6298	0.8673	0.9483	0.9721	0.9786
Shifted 2-N-PSK, realization C	0.6517	0.8333	0.9062	0.9305	0.9464

A similar study is conducted for the *PR* curves of the methods in varying SNRs. The resultant curves for each SNR case are given in Figure 9, with their corresponding *PR AUCs* in Table 7. In this examination, the curves of *2-N-PSK* and *Shifted 2-N-PSK* in scenario *C* go together with a small *PR AUC* increase in *C* over *2-N-PSK* that increments between 0.32% and 3.74% depending on the SNR value. Similarly to their *ROC* curves, the *PR* curves of implementations *A* and *B* again show close proximity, however in the *PR* analyses realization *B* shows the best *AUC* results. Thus, for SNR = 20 dB, *B* surpasses the *PR AUC* of *A*, *C* and *2-N-PSK* respectively by 5.51%, 9.05% and 10.15%.



(**a**)

(**b**)

(**c**)

(**d**)

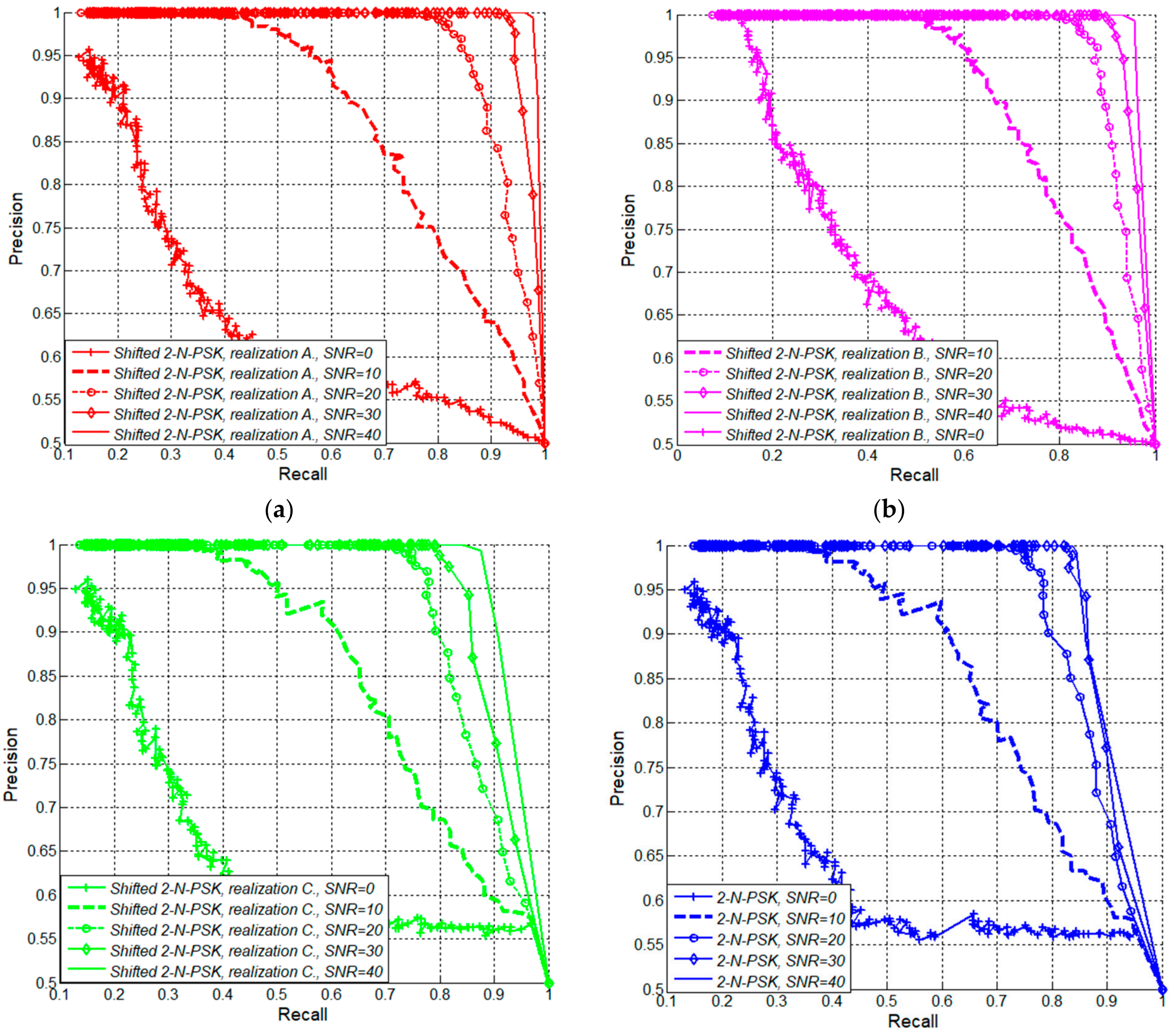
(**e**)

Figure 9. *PR* curves for different SNR scenarios: (**a**) SNR = 0 dB; (**b**) SNR = 10 dB; (**c**) SNR = 20 dB; (**d**) SNR = 30 dB; (**e**) SNR = 40 dB.

Table 7. *PR AUC* of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* in different SNR scenarios.

PR AUC	Signal-to-Noise Ratio				
	SNR = 0 dB	**SNR = 10 dB**	**SNR = 20 dB**	**SNR = 30 dB**	**SNR = 40 dB**
2-N-PSK	0.5535	0.7133	0.7890	0.7766	0.7861
Shifted 2-N-PSK, realization A	0.5543	0.7476	0.8354	0.8277	0.8413
Shifted 2-N-PSK, realization B	0.5695	0.7981	0.8905	0.8947	0.8995
Shifted 2-N-PSK, realization C	0.5567	0.7211	0.8000	0.8047	0.8235

Figure 10 represents the *PR* curves of each method individually for all SNR cases. An increase in the SNR results in improved *PR* relation and curve that comes nearer to the upper-left corner of the plot.



(**a**) (**b**)

(**c**) (**d**)

Figure 10. *PR* curves—individual representation of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK*: (**a**) *Shifted 2-N-PSK*, realization *A*; (**b**) *Shifted 2-N-PSK*, realization *B*; (**c**) *Shifted 2-N-PSK*, realization *C*; (**d**) *2-N-PSK*.

ROC and *PR* analyses are also carried out for differing number of antennae at the BS. The *ROC* and *PR* curves of all the methods under research for M = 10, M = 100, and M = 300 are illustrated in Figures 11 and 12, respectively, and their relevant *AUC* values follow in Tables 8 and 9.

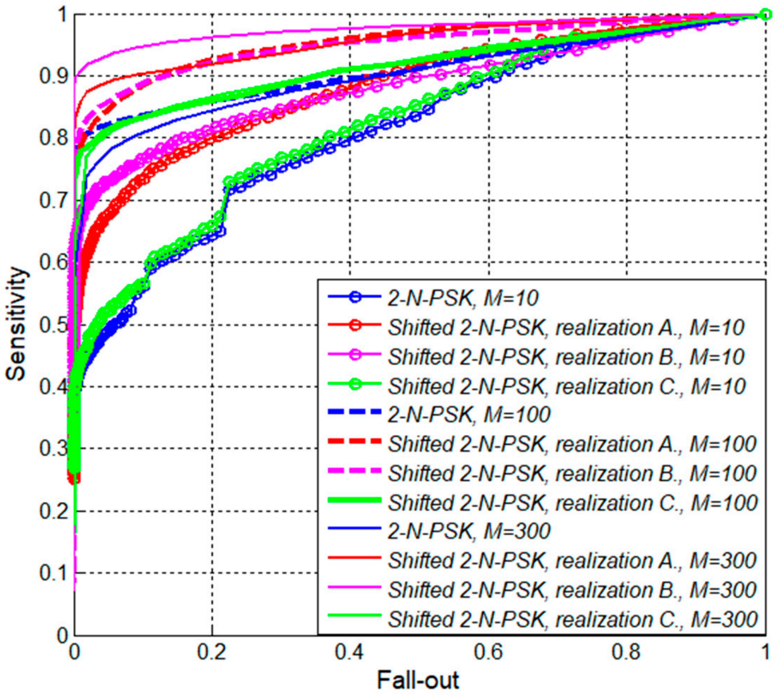


Figure 11. *ROC* curves of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* for different numbers of antennae at the BS.

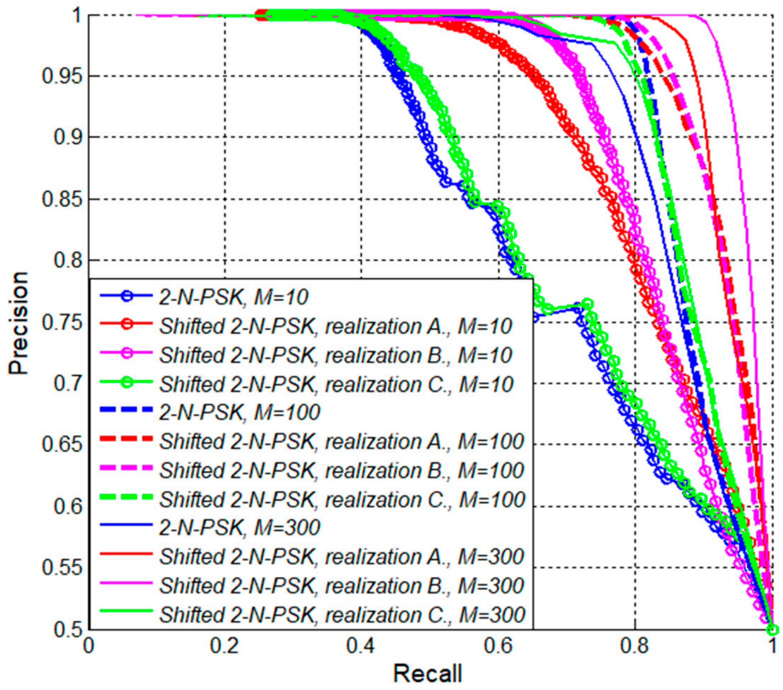


Figure 12. *PR* curves of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* for different numbers of antennae at the BS.

Table 8. *ROC AUC* of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* with different numbers of antenna elements at the BS.

ROC AUC	**Antennae Number**		
	***M* = 10**	***M* = 100**	***M* = 300**
2-N-PSK	0.8112	0.9115	0.9006
Shifted 2-N-PSK, realization A	0.8850	0.9548	0.9567
Shifted 2-N-PSK, realization B	0.8830	0.9506	0.9756
Shifted 2-N-PSK, realization C	0.8234	0.9161	0.9167

Table 9. *PR AUC* of *2-N-PSK* and the different realizations of *Shifted 2-N-PSK* with different numbers of antenna elements at the BS.

PR AUC	**Antennae Number**		
	***M* = 10**	***M* = 100**	***M* = 300**
2-N-PSK	0.5603	0.7775	0.7649
Shifted 2-N-PSK, realization A	0.6605	0.8257	0.8035
Shifted 2-N-PSK, realization B	0.5981	0.8818	0.9128
Shifted 2-N-PSK, realization C	0.5890	0.7800	0.7662

Both the *ROC* and *PR* results of each method show improvement when the antenna number rises from 10 to 100. A strange trend, however, can be observed in the *ROC AUC* of *2-N-PSK* and most of the *PR AUC* results when the value of *M* increases from 100 to 300. Not only does the improvement vanish but also the *PR AUC* lessens in most methods' implementations. Only realization *B* of *Shifted 2-N-PSK* keeps improving its *PR* results to a certain extent when expanding the antenna number from 100 to 300. For instance, realization *A* demonstrates *ROC AUC* and *PR AUC* improvements of 6.98% and 16.52% respectively with the increase in *M* from 10 to 100, while only 0.19% growth in *ROC AUC* is noted when the number of *M* changes from 100 to 300, and a decrease in the *PR AUC* result by 2.22% is observed. These considerations once more raise the question of the benefits in growing the size of the antenna array up to several hundred. Comparing the *ROC AUC* of realization *A* to the *ROC AUC* of the original *2-N-PSK* detection method, improvements of 7.38%, 4.33%, and 5.61% are observed for *M* = 10, *M* = 100, and *M* = 300, respectively. The same comparison between *PR AUC* of realization *A* and *PR AUC* of *2-N-PSK* for 10, 100, and 300 antennae at the BS gives difference of 10.02%, 4.82%, and 3.86%, respectively, always in favor of realization *A* of the *Shifted 2-N-PSK* detection method.

4. Distribution of the Legitimate Constellations Shift Values Problem

The improved performance of *Shifted 2-N-PSK* compared to the original *2-N-PSK* from a DP point of view is due to the strategy involved of shifting the legitimate constellations. This way, repetition of the signal of LU or sending its reciprocal is avoided as the malicious user contaminates the training phase with pilots from the N-PSK constellation. However, as stated above, undetectable attacks are still possible in a modified manner, if ED aims at the N-PSK angle that is closest to the related legitimate pilot after the offset. Assuming the different realizations of *Shifted 2-N-PSK* and their aforementioned detection capabilities, in the absence of noise, a modified attack of type 2 is always revealed by the method, regardless of the realization scenario, i.e., no matter whether *A*, *B*, or *C* is implemented, the method successfully discovers attacks of type 2. The other types of PCAs that are undiscoverable by *2-N-PSK*—that is, the modified types 1, 3, and 4—can be detected by *Shifted 2-N-PSK* depending on the choice of offset values. The most effective scenario of *Shifted 2-N-PSK* from a DP point of view is observed when the requirements in realization *A* are covered and neither the legitimate nor the reference constellations coincide with the original N-PSK constellation.

If ED obtains information about the offset values used to shift the pilots of legitimate constellations, it can initiate its PCA sending signals from the same alphabet as the LU. This action degrades the detection probability of *Shifted 2-N-PSK* and makes system operation similar to that of the original *2-N-PSK* method. Thus, a need to secure the shift values and their exchange follows. In order to ensure the privacy of the information concerning the offset values, they can be changed dynamically so that for each pilot signal a different legitimate constellation is used. However, such a strategy increases the need for an algorithm for secure key exchange at the physical layer, where the offset values can be treated as keys. For the proper operation of existing algorithms that generate keys from the properties of the physical layer, a priori CSI is required, making them unsuitable for the purposes of *Shifted 2-N-PSK*, which must be applied during the channel estimation procedure.

In this paper, an algorithm that solves the problem of secure distribution of the legitimate constellations shift values is proposed. By simple mathematical operations applied simultaneously at both the BS and LU, the offset angles for the next training phase can be extracted only from physical layer parameters. Namely, the shift values from the current training phase and the currently obtained channel transfer function serve as input parameters for the calculation of the shift values intended for the next training phase. Therefore, the algorithm can be employed only after the transmission of the first pair of pilots and assumes that the values of x_1 and x_2, used for the first training phase are negotiated in advance through a cryptography approach on the upper layers of the protocol stack.

Following next is the description of the steps involved in the whole training process, including the algorithm proposed to compute the legitimate constellations shift values.

Step 1: Using a random number generator, the LU sets up the values x_1 and x_2 used to shift the legitimate constellations of the first and the second pilot signals. The generated values are sent to the BS through a secure channel and upper layers approach. In order to achieve the best performance, the values of x_1 and x_2 have to meet the requirements in A, i.e., $\mid x_1 - x_2 \mid \neq \varphi_x$ (*N-PSK*) and $x_1 \neq x_2 \neq \varphi_x$ (*N-PSK*).

Step 2: The *i*-th training phase takes place. LU sends to the BS two uplink pilot signals from shifted constellations—${p_{2i-1}}^{LU}$ belongs to a constellation shifted from the original N-PSK symbols by x_{2i-1} degrees and the constellation of $p_{2i}{}^{LU}$ is shifted by x_{2i} degrees.

Step 3: The BS estimates the channel and shares with LU the computed channel transfer function from the *i*-th training phase, K_i, via a protocol from the upper layers of the reference model. Meanwhile, the *Shifted 2-N-PSK* method is applied. In cases where PCA is detected, the communication process is interrupted.

Step 4: The LU and the BS simultaneously compute the values used to shift the legitimate constellations for the next pair of pilots, i.e., x_{2i+1} and x_{2i}, in accordance with the algorithm proposed below.

Steps 2, 3, and 4 are repeated for each subsequent estimate of the channel K_{i+1}, K_{i+2}, K_{i+3} and so on.

The algorithm used in **Step 4**, whose block diagram is illustrated in Figure 13, is based on the following considerations: due to the random nature of wireless channels and the positioning of ED at a different location from the LU, the malicious user explores channel conditions that are not identical to those of LU. Consequently, no information about the legitimate channel transfer function K_i is available at ED and it is reasonable to use the phase of the currently estimated legitimate channel, denoted $\varphi(K_i)$, for computing the legitimate constellations shift values for the next training interval, with running number $i + 1$, i.e., x_{2i+1} and x_{2i+2}. In order to reduce the digital processing, which would make the algorithm applicable in resource-constrained devices, x_{2i+1} and x_{2i+2} are computed as the sum of the shift values from the current training phase, x_{2i-1} and x_{2i}, and the current legitimate channel argument, $\varphi(K_i)$. Despite its simplicity, even if the algorithm is publicly available, it is secure due to the random nature of the channel and the securely shared offset values for the first training interval.

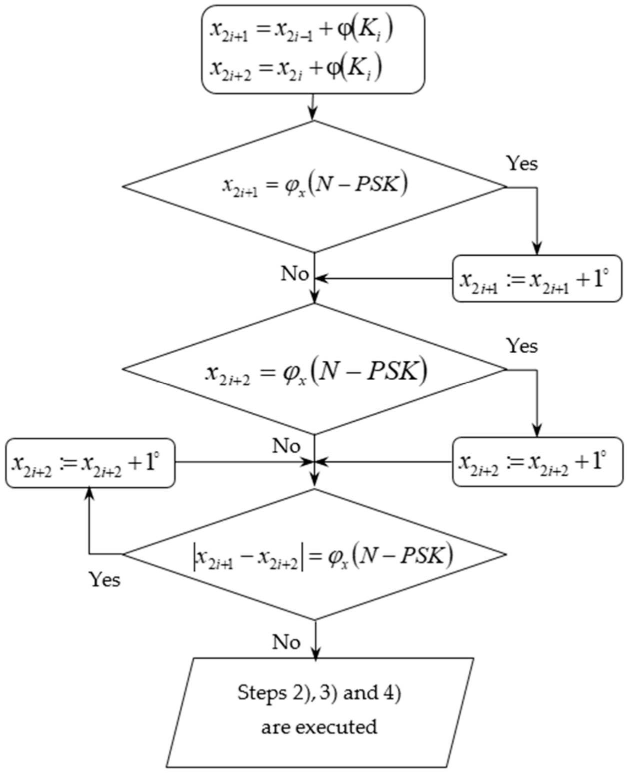

$x_{2i+1} = x_{2i-1} + \varphi(K_i)$
$x_{2i+2} = x_{2i} + \varphi(K_i)$
$x_{2i+1} = \varphi_x(N-PSK)$
Yes
$x_{2i+1} := x_{2i+1} + 1^{\circ}$
No
$x_{2i+2} = \varphi_x(N-PSK)$
Yes
$x_{2i+2} := x_{2i+2} + 1^{\circ}$
No
$x_{2i+2} := x_{2i+2} + 1^{\circ}$
$|x_{2i+1} - x_{2i+2}| = \varphi_x(N-PSK)$
Yes
No
Steps 2), 3) and 4)
are executed

Figure 13. Flow chart of the algorithm for calculating the legitimate constellations' shift values x_{2i+1} and x_{2i+2} [17].

As discussed before, and as is proven from the experimental results presented in this paper, *Shifted 2-N-PSK* demonstrates the most advantageous operation when the conditions of realization A are met. Thus, in the ith training phase the algorithm aims to compute the shift values for the next training interval, x_{2i+1} and x_{2i+2}, so as to correspond to the following criteria: $| x_{2i+1} - x_{2i+2} | \neq \varphi_x$ (*N-PSK*) and $x_{2i+1} \neq x_{2i+2} \neq \varphi_x$ (*N-PSK*). In case the condition $| x_{2i-1} - x_{2i} | \neq \varphi_x$ (*N-PSK*) is fulfilled for the current legitimate pilots and the next ones are calculated through $x_{2i+1} = x_{2i-1} + \varphi(K_i)$ and $x_{2i+2} = x_{2i} + \varphi(K_i)$, for certain x_{2i+1} and x_{2i+2} comply with the condition $| x_{2i+1} - x_{2i+2} | \neq \varphi_x$ (*N-PSK*). However, the newly computed values must be checked to determine whether they meet the criterion not to equal an N-PSK phase. If a calculated shift value coincides with an N-PSK argument, its value is incremented by one. In an effort to ensure the conditions $x_{2i+1} \neq \varphi_x$ (*N-PSK*) and $x_{2i+2} \neq \varphi_x$ (*N-PSK*) it is possible to increment the shift values in such a way that the result no longer fulfils the criterion for a reference constellation that differs from the N-PSK, i.e., $| x_{2i+1} - x_{2i+2} | \neq \varphi_x$ (*N-PSK*) can be violated. Hence, a corresponding check is made, and if needed, the shift value of the even pilot is incremented by one. Then, another verification determines whether the new value of x_{2i+2} differing from the N-PSK angles is needed. Only after all the criteria are met can it proceed to the execution of **Steps 2, 3, and 4** for the next training phase, the one with running number i + 1.

5. Discussion

The vulnerability of channel estimation procedures to PCAs represents a major security concern in contemporary wireless systems, especially those incorporating small-scale sensors and devices that suffer from hardware and software limitations. In such systems, cryptography-based approaches, traditionally implemented on the upper layers of the reference model, are non-applicable due to their complex computational algorithms and the subsequent requirements for large memory, high processing capabilities and energy supply [27,28]. In networks with resource-constrained devices, PLS solutions are extremely suitable for strong and reliable system protection established thoroughly on information theory.

An attractive PLS approach, called *2-N-PSK*, that is able to detect PCAs by studying the constellation diagram and analyzing the correlation of received pilot signals was first proposed in [15]. As discussed in Section 2, several attack scenarios exist, which the *2-N-PSK* detection method is not able to correctly detect as being present. These observations motivated our previous studies in [16,17], where we proposed and studied a method, called *Shifted 2-N-PSK*, to improve the performance efficiency of *2-N-PSK*. Though *Shifted 2-N-PSK* successfully reveals most parts of the attacks that are undetectable by *2-N-PSK*, the operation of the method with shifted constellations is highly related to the choice of offset angles to change the original N-PSK diagram. In Section 2, the three different implementation scenarios of *Shifted 2-N-PSK* are described as realizations *A*, *B*, and *C*. Despite studying the probability metrics of *2-N-PSK* and realization *A* of *Shifted 2-N-PSK* in our previous work [17], until now, realizations *B* and *C* have not been investigated in scenarios with different antenna numbers. Moreover, except for our recent work in [26] where *ROC* analysis of realization *A* and *2-N-PSK* for different SNRs is made, there is still a lack of research on the statistical classification metrics of *2-N-PSK* and all the implementations of *Shifted 2-N-PSK*. All these considerations motivated this study.

The main contributions of the paper are summarized as follows:

- The major probability measures, namely DP and FAP of *2-N-PSK* and *Shifted 2-N-PSK* are examined in scenarios with different numbers of antenna elements at the BS. In this study, all three of the different realizations of the method with shifted constellations are considered.
- A holistic view of the overall performance of *2-N-PSK* and *Shifted 2-N-PSK* is accomplished through statistical evaluation parameters, such as *accuracy*, *precision*, *recall*, *F1-score*, *specificity*, and *fall-out*. Moreover, *ROC* and *PR* curves together with their corresponding *area under curve* (*AUR*) are also included in this analysis. Both the curves are obtained for different sizes of the antenna array at the BS.
- Using probability and classification metrics, the *2-N-PSK* and *Shifted 2-N-PSK* methods for PCA detection are exhaustively studied and their performance is compared.
- A lightweight PLS algorithm that can be used to compute the shift values of legitimate pilots for *Shifted 2-N-PSK* detection method is proposed. The algorithm is applicable at the LU and BS simultaneously, hence eliminating the need for secure exchange of the offset values.

Summarizing the behavior of the probability metrics, it can be concluded that all the realizations of *Shifted 2-N-PSK* outperform the DP results of *2-N-PSK* at the expense of a small worsening of FAP results. Increasing the size of the antenna array to a certain extent improves the DP in most SNR scenarios and successfully reduces the value of FAP. However, only small benefits in probability metrics are observed when increasing the antenna number above one hundred.

Considering the classification metrics, realizations *A* and *B* of the *Shifted 2-N-PSK* detection method surpass the others and which of them is superior depends on the SNR scenario. As the decision criterion of the methods is connected with the noise power, the results of both *ROC* and *PR* analysis confirm significant improvement in the methods' performance in enhanced SNR conditions. The study of *ROC* and *PR* curves in different numbers of antenna elements at the BS proves the conclusion of the research on the probability metrics that more effective performance of detection methods is demonstrated when raising the size of the antenna array. However, in cases of as many as 300 antennae, the *PR* analysis does not show the desired improvement and even a small reverse effect is observed. Therefore, a study of to what extent it is reasonable to increase the antenna number at the BS may be considered as a future research direction.

6. Conclusions

In this paper, two PCA detection methods that distinguish between the presence or absence of an attack based on a constellation diagram analysis are exhaustively studied. First, the DP and FAP of both the methods are investigated. Then, large varieties of classification metrics, that provide a broad-spectrum view on the different aspects of effective operation, are explored. Summarizing the simulation results, it should be noted that realization *A* of *Shifted 2-N-PSK* improves the efficiency of *2-N-PSK* according to *ROC AUC* and *PR AUC* analyses, as follows: for $M = 10$, 7.38% and 10.02% a respective increase in *ROC AUC* and *PR AUC*; for $M = 100$, 4.33% and 4.82% a respective increase in *ROC AUC* and *PR AUC*; for $M = 300$, 5.61% and 3.86% a respective increase in ROC *AUC* and *PR AUC*. These results show that the larger the antenna array at the BS, the narrower the difference in both methods' operation. At the end of this research, an algorithm is proposed that can be used at the LU and the BS simultaneously to compute the shift values of legitimate constellations in *Shifted 2-N-PSK*, thus eliminating the need for key exchange at the upper layers of the reference model.

As mentioned in Section 5, a possible future line of research can investigate the precise upper bounds of the antenna number that gives a significant improvement of the methods' efficiency. Another subject of future analyses can be the evaluation of the detection capabilities of the methods with an extended system model. This can include user mobility, a more complex distribution of the noise variables, and a change in the modulation diagram from the originally used N-PSK constellation.

Author Contributions: Conceptualization, D.M. and G.I.; methodology, D.M.; software, D.M.; validation, V.S. and Z.V.-J.; formal analysis, Z.V.-J. and G.I.; investigation, D.M.; resources, Z.V.-J.; data curation, V.S. and D.M.; writing—original draft preparation, D.M.; writing—review and editing, Z.V.-J., G.I. and V.S.; visualization, V.S.; supervision, Z.V.-J.; project administration, G.I.; funding acquisition, G.I. All authors have read and agreed to the published version of the manuscript.

Funding: This study is financed by the European Union—NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, project No. BG-RRP-2.004-0005.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Zhang, S.; Zhu, D.; Liu, Y. Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities. *Comput. Netw.* **2024**, *242*, 110255. [CrossRef]
4. Busari, S.A.; Huq, K.M.S.; Mumtaz, S.; Rodriguez, J. Terahertz Massive MIMO for Beyond-5G Wireless Communication. In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019. [CrossRef]
5. Zhou, X.; Maham, B.; Hjorungnes, A. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 903–907. [CrossRef]
6. Elijah, O.; Leow, C.Y.; Rahman, T.A.; Nunoo, S.; Iliya, S.Z. A comprehensive survey of pilot contamination in massive MIMO—5G system. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 905–923. [CrossRef]
7. Xu, W.; Yuan, C.; Xu, S.; Ngo, H.Q.; Xiang, W. On pilot spoofing attack in massive MIMO systems: Detection and countermeasure. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1396–1409. [CrossRef]
8. Xu, S.; Xu, W.; Gan, H.; Li, B. Detection of pilot spoofing attack in massive MIMO systems based on channel estimation. *Signal Process.* **2020**, *169*, 107411. [CrossRef]
9. Tugnait, J.K. Self-contamination for detection of pilot contamination attack in multiple antenna systems. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 525–528. [CrossRef]
10. Xiong, Q.; Liang, Y.-C.; Li, K.H.; Gong, Y.; Han, S. Secure transmission against pilot spoofing attack: A two-way training-based scheme. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1017–1026. [CrossRef]
11. Zeng, J.; Wang, D.; Xu, W.; Li, B. An efficient detection algorithm of pilot spoofing attack in massive MIMO systems. *Signal Process.* **2021**, *182*, 107962. [CrossRef]

12. Qiu, J.; Xu, K.; Xia, X.; Shen, Z.; Xie, W.; Zhang, D.; Wang, W. Secure transmission scheme based on fingerprint positioning in cell-free massive MIMO systems. *IEEE Trans. Signal Inf. Process. Over Netw.* **2022**, *8*, 92–105. [CrossRef]
13. Darsena, D.; Gelli, G.; Iudice, I.; Verde, F. Design and performance analysis of channel estimators under pilot spoofing attacks in multiple-antenna systems. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3255–3269. [CrossRef]
14. Wang, H.-M.; Huang, K.-W.; Tsiftsis, T.A. Multiple antennas secure transmission under pilot spoofing and jamming attack. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 860–876. [CrossRef]
15. Kapetanović, D.; Zheng, G.; Wong, K.-K.; Ottersten, B. Detection of Pilot Contamination Attack Using Random Training and Massive MIMO. In Proceedings of the IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), London, UK, 8–11 September 2013. [CrossRef]
16. Mihaylova, D.; Valkova-Jarvis, Z.; Iliev, G.; Poulkov, V. Shifted 2-N-PSK method for the detection of pilot contamination attacks. *Wirel. Pers. Commun.* **2021**, *118*, 1945–1970. [CrossRef]
17. Mihaylova, D.; Stoynov, V.; Iliev, G.; Valkova-Jarvis, Z.; Poulkov, V. Performance Evaluation of Constellation Diagram Analysis-based Methods for PCA Detection. In Proceedings of the 29th National Conference with International Participation (TELECOM), Sofia, Bulgaria, 28–29 October 2021. [CrossRef]
18. Song, J.; Wang, X.; He, M.; Jin, L. CSK-CNN: Network intrusion detection model based on two-layer convolution neural network for handling imbalanced dataset. *Information* **2023**, *14*, 130. [CrossRef]
19. Alkhudaydi, O.A.; Krichen, M.; Alghamdi, A.D. A deep learning methodology for predicting cybersecurity attacks on the Internet of Things. *Information* **2023**, *14*, 550. [CrossRef]
20. Charmanas, K.; Mittas, N.; Angelis, L. Exploitation of vulnerabilities: A topic-based machine learning framework for explaining and predicting exploitation. *Information* **2023**, *14*, 403. [CrossRef]
21. Almseidin, M.; Alzubi, M.; Kovacs, S.; Alkasassbeh, M. Evaluation of Machine Learning Algorithms for Intrusion Detection System. In Proceedings of the IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 14–16 September 2017. [CrossRef]
22. Rashid, A.; Siddique, M.J.; Ahmed, S.M. Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System. In Proceedings of the 3rd International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 17–19 February 2020. [CrossRef]
23. Brownlee, J. *Imbalanced Classification with Python: Better Metrics, Balance Skewed Classes, Cost-Sensitive Learning*, 1st ed.; Independently published by Machine Learning Mastery: Vermont, VIC, Australia, 2020; pp. 35–85. ISBN 979-8468452240.
24. Branco, P.; Torgo, L.; Ribeiro, R. A survey of predictive modeling on imbalanced domains. *ACM Comput. Surv.* **2016**, *49*, 31. [CrossRef]
25. Kamaldeep; Dutta, M.; Granjal, J. Towards a secure internet of things: A comprehensive study of second line defense mechanisms. *IEEE Access* **2020**, *8*, 127272–127312. [CrossRef]
26. Mihaylova, D.; Valkova-Jarvis, Z.; Iliev, G.; Stoynov, V. Statistical Evaluation of Classification Models for PCA Detection. In Proceedings of the 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES 2023), Plovdiv, Bulgaria, 23–25 November 2023. [CrossRef]
27. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
28. Rojas, P.; Alahmadi, S.; Bayoumi, M. Physical Layer Security for IoT Communications—A Survey. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14 June–31 July 2021. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.