A New Technique to Improve the 2-N-PSK Method for Detecting Wireless Pilot Contamination Attacks

DIMITRIYA MIHAYLOVA, ZLATKA VALKOVA-JARVIS, GEORGI ILIEV
Department of Communication Networks
Technical University of Sofia
8 Kliment Ohridski Blvd., Sofia 1000
BULGARIA
dam@tu-sofia.bg http://www.tu-sofia.bg

Abstract: - Wireless communication systems are very vulnerable to pilot contamination attacks, which represents a major physical layer security issue. Hence, it is necessary to apply different approaches and methods to the detection of this type of attack. One effective method proposed in the literature is *2-N-PSK* pilot detection, which consists of training with two random N-PSK pilots. Although the method is broadly effective, it is not able to detect an attack initiated during the transmission of the second pilot of the pair in the case when both the legitimate and non-legitimate pilots coincide. In this paper, an improvement to this method is proposed to detect an intrusion which misses the first pilot transmission and initiates an attack during the second training period. This improved technique is based on channel gain comparison and eliminates the need to use threshold values in the detection – a drawback of previously-existing solutions.

Key-Words: - Wireless communication systems, Physical layer security, Pilot contamination attacks, *2-N-PSK* pilot detection method, Channel state information, Detection statistic.

1 Introduction

One of the major problems in wireless networks relates to ensuring their security. In an endeavour to achieve this, a new strategy, called physical layer security (PLS), has been developed. Instead of using crypto-algorithms, PLS relies on the changes in the physical properties of the channel when an intruder attempts to participate in the communication.

In spite of the fact that PLS improves secrecy without using the complex computational systems that are typical of cryptographic schemes, some of its weaknesses, as observed in [1], [2], [3] require extensive additional research. One of these weaknesses is the capability of the malicious user to interfere with the process of channel estimation. This vulnerability can be exploited in what is known as a pilot contamination attack, a comprehensive description of which can be found in [4].

A time division duplex (TDD) system such as massive MIMO (MaMIMO), where the uplink and downlink channels are reciprocal and the channel state information (CSI) is obtained during a training phase, is particularly vulnerable to such a pilot contamination attack. Different levels of CSI at the transmitter and the eavesdropper (ED), and their influence on the privacy of a system, are discussed in [5], [6]. The process of channel estimation on MaMIMO consists of the receiver sending pilot signals to the transmitter, which then computes the CSI and, based on this result, designs its precoder. The objective of a prospective eavesdropper is to send pilots together with the legitimate receiver and thus to produce incorrect channel estimation at the transmitter end, resulting in an erroneous precoder, which also sends the data signal in the direction of the attacker. Using this active attack an intruder could overcome the passive eavesdropping resistance of a MaMIMO system, as can be seen in [7].

A pilot contamination attack undermines security at the physical layer and consequently has a detrimental effect on the security capability of the whole system. Hence the significance of introducing schemes for the detection of a pilot contamination attack and the need to terminate the communication in the event that one is detected.

2 System Model

The current paper is focused on a technique for the detection of pilot contamination attacks. The system is TDD, composed of a single cell in which a base station (BS) with multiple antennas - *M* in number – communicates with a legitimate user (LU) and where an ED tries to circumvent the security. The model, used for the sake of simplicity, is composed of a single LU and one ED in the cell, both of them equipped with a single antenna transceiver. In

addition, the channels are assumed to be static and subject to Additive White Gaussian Noise (AWGN), while user mobility is disregarded.

The system model is depicted in Fig.1.

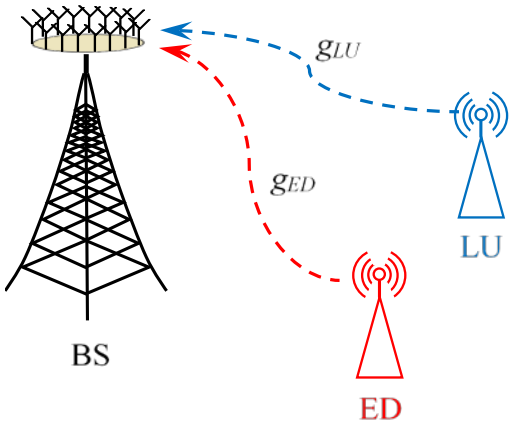

Fig. 1. The system model

During the uplink TDD phase, the LU and ED synchronically send their pilot sequences to the BS, where the CSI is computed. The uplink channels of the LU and ED, denoted as g_{LU} and g_{ED} respectively, follow Eq. 1:

$$\begin{aligned} g_{LU} &= \sqrt{P_{LU} d_{LU}}\, h_{LU} \\ g_{ED} &= \sqrt{P_{ED} d_{ED}}\, h_{ED}, \end{aligned} \tag{1}$$

where P_{LU} and P_{ED} are the transmit powers of the LU and ED, d_{LU} and d_{ED} are scalars for the large-scale fading, and h_{LU} and h_{ED} are $M \times 1$ vectors for the small-scale fading.

3 Two Random N-PSK Pilots Detection Method (*2-N-PSK*)

A simple and effective technique for the detection of a pilot contamination attack is suggested in [8]. This method consists of sending random Phase-Shift Keying (PSK) pilot signals during the uplink channel estimation phase of a TDD system. An 8-PSK constellation is shown in Fig. 2, where the relationship between the coordinates of a complex number, its trigonometric form, and its module and argument representation is given by Euler's equation:

$$q = x + iy = r(\cos\varphi + i\sin\varphi) = re^{i\varphi}. \tag{2}$$

This method makes a decision about the presence of an ED via the following procedure. The LU sends two N-PSK pilot symbols to the BS, the first of which could be publicly known, with the second being chosen at random. The signals received at the BS for the first and second pilots, denoted as y_1 and y_2 respectively, are given in Eq. (3):

$$\begin{aligned} y_1 &= g_{LU} p_1^{LU} + g_{ED} p_1^{ED} + n_1 = \\ &= \sqrt{P_{LU} d_{LU}}\, h_{LU} p_1^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_1^{ED} + n_1 \end{aligned} \tag{3}$$

$$\begin{aligned} y_2 &= g_{LU} p_2^{LU} + g_{ED} p_2^{ED} + n_2 = \\ &= \sqrt{P_{LU} d_{LU}}\, h_{LU} p_2^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_2^{ED} + n_2, \end{aligned}$$

where the pilots sent from the LU during the first and the second training periods are p_1^{LU} and p_2^{LU}, the pilots from the ED are p_1^{ED} and p_2^{ED}, and the AWGN in the first and second time slots are n_1 and n_2 respectively.

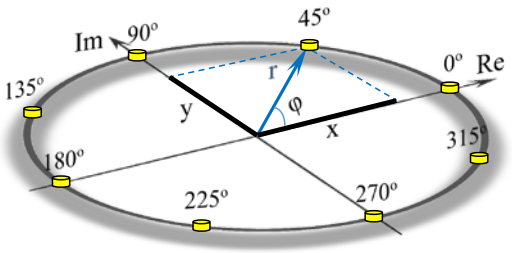

Fig. 2. Eight Phase-Shift Keying (8-PSK) constellation diagram. Geometric representation of a complex number

In the BS the CSI is obtained by processing the received signals. Their correlation is computed by Eq. (4), where $(\cdot)^H$ means Hermitian matrix and n_{12} is the noise result:

$$\begin{aligned} z_{12} &= \frac{y_1^H y_2}{M} = \\ &= \frac{1}{M}\left(\sqrt{P_{LU} d_{LU}}\, h_{LU} p_1^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_1^{ED}\right)^H \times \\ &\left(\sqrt{P_{LU} d_{LU}}\, h_{LU} p_2^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_2^{ED}\right) + n_{12} \end{aligned} \tag{4}$$

The scalar product of the correlation result is then analysed.

If its phase converges to a phase of a valid N-PSK symbol, two possible scenarios exist: either the ED is absent during both of the training periods or the ED is present in only one of the time slots.

If the scalar product of the correlation result has an angle that does not converge to a valid N-PSK phase, a definite conclusion can be reached that the pilot contamination attack appears in both the training periods.

Summarising the simulation results of the *2-N-PSK*, the method reveals the intervention of a non-legitimate user in the channel estimation procedure when either one or both of the ED's pilots differ from the pilots of the LU. When the ED sends a

pilot which equals the one sent from the LU in only one of the training intervals, the *2-N-PSK* technique undertakes additional verification to determine if this intervention is non-legitimate in nature. The worst case scenario, which the method is not able to detect, is when both of the attacker's pilots coincide with the legitimate pilots or when the first is the same and the second is shifted by 180 degrees, i.e. the complex number of the second ED's pilot is reciprocal to that of the LU.

The main advantages and drawbacks of the method are discussed in [9], where other solutions which have been proposed in the literature are also analysed and compared.

4 An improved technique for the *2-N-PSK* detection method

As described in the previous sections, the objective of the pilot contamination attack is to compromise the CSI and thus to expose the legitimate channel information to the malicious user. So, once the ED starts sending pilots to the BS synchronically with the LU this process would continue until all of the information about the channel is revealed. However, the ED could participate in the communication at a later stage and thus miss one or more of the training periods. This is exactly the case when, despite the presence of the ED in the second slot, the angle of the correlation result converges to a valid N-PSK phase if the ED guesses either the pilot of the LU or the reciprocal number.

When this situation occurs, the authors in [10] suggest a revision of the amplitude of the received signals, since the received power of the contaminated pilot will be larger than that of the non-contaminated pilot. To decide if the difference in the received power is a result of a pilot contamination attack in one of the slots or is simply a consequence of the natural imperfections of the channel, the ratio of the received signals is compared to certain thresholds. The decision that a malicious user has sent a pilot during one of the slots is reached if the result of the ratio is outside the range defined by the thresholds. Otherwise, the conclusion is that there is no ED present during the channel estimation procedure.

Since the assignment of thresholds requires previous channel knowledge, the reference values are difficult to obtain and their definition is subject to possible error. Therefore, in the case of pilot contamination during only one of the slots the use of the *2-N-PSK* detection method is not effective.

In the current paper we propose another solution for the detection of a pilot contamination attack initiated during the second training period, which avoids the use of threshold values. We will consider the scenario in which the ED duplicates the pilot of the LU or sends its reciprocal value. Hence, if the phase of the correlation result z_{12} is a valid N-PSK angle, the technique described below is applied. It is illustrated in Fig. 3.

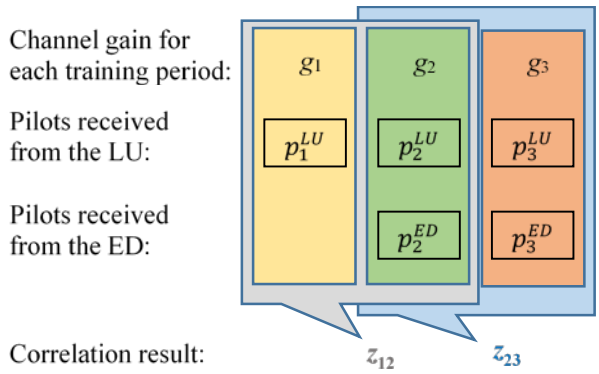

Fig. 3. Channel gain comparison for the received pilots

Considering the first pilot transmission, according to Eq. (3) apart from the noise, the signal received at the BS in the absence of an ED is:

$$y_1 = p_1^{LU} g_{LU}, \tag{5}$$

which defines the value of the channel gain as:

$$g_1 = g_{LU} = \frac{y_1}{p_1^{LU}}. \tag{6}$$

In the second training slot the ED's contamination with $p_2^{ED}=p_2^{LU}$ forms:

$$y_2 = p_2^{LU} g_{LU} + p_2^{ED} g_{ED} = p_2^{LU} \left(g_{LU} + g_{ED}\right), \tag{7}$$

leading to channel gain:

$$g_2 = g_{LU} + g_{ED} = \frac{y_2}{p_2^{LU}}. \tag{8}$$

Since the BS is familiar with both the sent pilots and the received signals, the values of the channel gains can be calculated and the channel knowledge from the two training periods can be compared. Different values correspond to an attack in one of the slots. However, as the impact of noise could give rise to some limited variations, in order to avoid setting thresholds of an acceptable range of alteration, the values of the channel gain could be compared to those calculated during the next training interval.

First, the correlation of the next two pilots is computed. In the worst case, where the ED manages to guess the third pilot, the received signal is:

$$y_3 = p_3^{LU} g_{LU} + p_3^{ED} g_{ED} = p_3^{LU} \left(g_{LU} + g_{ED} \right). \quad (9)$$

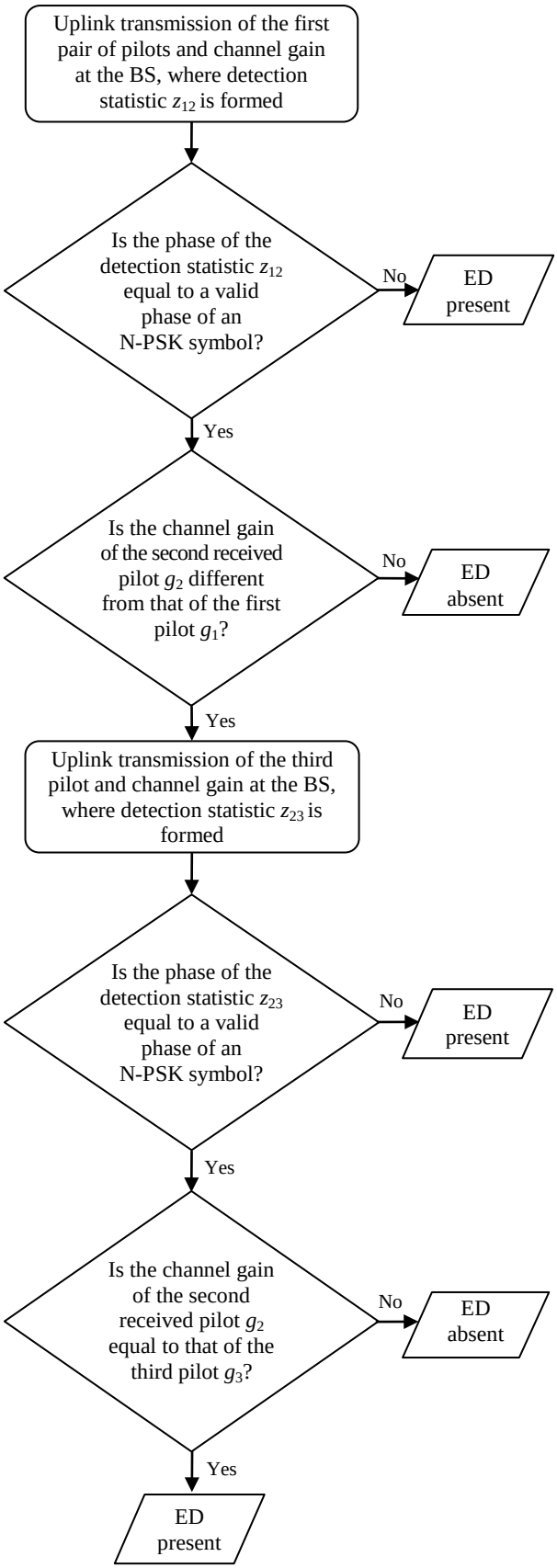

Fig. 4. Flow chart of the improved *2-N-PSK* method

The argument of the correlation z_{23} between the

second and the third pilot is also a valid N-PSK phase. Then the effect of the channel gain for the third received pilot is calculated:

$$g_3 = g_{LU} + g_{ED} = \frac{y_3}{p_3^{LU}} \quad (10)$$

and the intrusion is confirmed in the case of equal channel gain values in the second and the third received pilots, i.e. when $g_2 = g_3$.

The block diagram depicted in Fig. 4 illustrates the proposed approach.

Another interpretation of the proposed technique can be observed in Fig. 5, where a geometric representation of the 8-PSK pilots is shown together with the correlation results. For simplicity, the simulation is carried out with a single antenna BS, a static channel is assumed and noise influence is disregarded. The amplitudes of the pilots from the LU and ED are regarded as being equal and their value is set to 1. For the purposes of the simulation, the channel between the BS and LU is assumed to be g_{LU} =1 and that between the BS and ED to be g_{ED} =0.7.

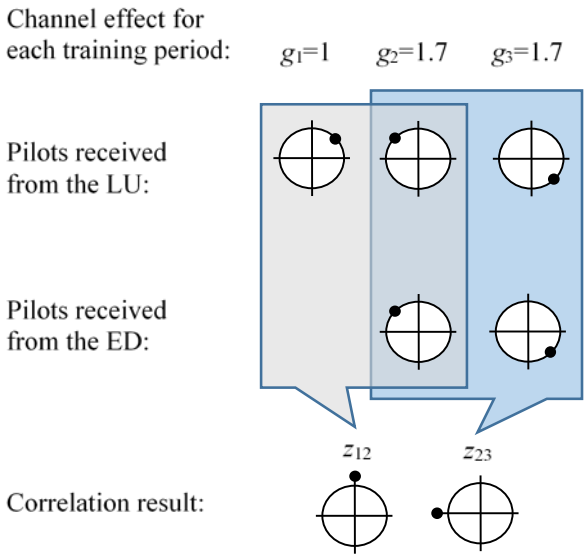

Fig. 5. Example interpretation of the proposed technique

As can be seen from the example in Fig. 5, when no ED is present the channel gain at the BS equals the gain of the legitimate channel. When an attack is under way, the resulting channel gain equals a larger value, which continues to show up during the next pilot sessions. Even in the worst case, when the ED's pilots coincide with those of the LU and the phase of the correlation result is a valid 8-PSK angle, the second appearance of the channel gain g_2 indicates the presence of an intruder.

In addition, the proposed complement to the *2-N-PSK* method can be used to indicate the presence of an attacker whose first pilot repeats the LU's pilot and whose second pilot is reciprocal to the LU's second pilot. This situation could not be detected by the *2-N-PSK* itself, since the phase of the detection statistic coincides with the angle of a symbol from the N-PSK constellation. However, the value of the channel gain computed from the first received pilot differs significantly from the channel gain of the second pilot, which demonstrates the presence of malicious intervention.

5 Experiments

Studying the original *2-N-PSK* method, a number of situations could be observed which the method is not able to detect. The improved technique solves a number of these situations, depending on the value of the third pilot's angle. A description of the relevant scenarios is given below, in which $\varphi(\cdot)$ denotes the angle of each pilot.

1. $\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right)$ and $\varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right)$

In the case where both the ED's pilots equal the LU's pilots, the angle of the correlation result z_{12} coincides with an angle from the N-PSK constellation and the original method does not register the attack. Because the channel gains of the first and the second pilots are the same (g_1=g_2), the improved technique is also unable to detect the malicious intervention in any of the three possible values of the third pilot, as listed below:

1.1. $\varphi\left(p_3^{ED}\right) = \varphi\left(p_3^{LU}\right)$.

1.2. $\varphi\left(p_3^{ED}\right) = \varphi\left(p_3^{LU}\right) + 180^\circ$.

1.3. $\varphi\left(p_3^{ED}\right) \neq \varphi\left(p_3^{LU}\right)$ and $\varphi\left(p_3^{ED}\right) \neq \varphi\left(p_3^{LU}\right) + 180^\circ$.

2. $\varphi\left(p^{ED}\right) = \varphi\left(p^{LU}\right) + 180^\circ$

If one (or both) of the non-legitimate pilots is reciprocal to the legitimate signal and the other is equal to it, the correlation angle is a valid N-PSK phase. The following three subcases exist according to which of the pilots is shifted by 180 degrees. Successful detection by the improved technique is closely related to the value of the angle of the third eavesdropper pilot:

2.1. $\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right)$ and $\varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right) + 180^\circ$.

2.1.1. $\varphi\left(p_3^{ED}\right) = \varphi\left(p_3^{LU}\right)$: when the third pilot of the ED is equal to that of the LU, the improved technique does not identify the intrusion, since the channel gains in the second and the third slots do not coincide, i.e. $g_2 \neq g_3$.

2.1.2. $\varphi\left(p_3^{ED}\right) = \varphi\left(p_3^{LU}\right) + 180^\circ$: in this case $g_2 \neq g_1$, the angle of z_{23} belongs to the constellation but the improved technique perceives the ED, since $g_2 = g_3$.

2.1.3. $\varphi\left(p_3^{ED}\right) \neq \varphi\left(p_3^{LU}\right)$ and $\varphi\left(p_3^{ED}\right) \neq \varphi\left(p_3^{LU}\right) + 180^\circ$:

this situation is again covered by the improvement, since the angle of the second correlation differs from the N-PSK angles: $\varphi(z_{23}) \neq \varphi(N-PSK)$.

2.2. $\varphi(p_1^{ED}) = \varphi(p_1^{LU}) + 180^\circ$ and $\varphi(p_2^{ED}) = \varphi(p_2^{LU})$.

2.2.1. $\varphi(p_3^{ED}) = \varphi(p_3^{LU})$: although the angle of the second correlation is an N-PSK angle, the improved method detects the presence of the ED due to the second and third channel gains being equal ($g_2=g_3$).

2.2.2. $\varphi(p_3^{ED}) = \varphi(p_3^{LU}) + 180^\circ$: the proposed technique is not able to register the attack, owing to the difference in the channel gain values of the second and third pilots.

2.2.3. $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU})$ and $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU}) + 180^\circ$: the improved scheme proposed in the current paper reveals the contamination in the case where the third pilot of the ED differs from the third legitimate pilot or its reciprocal. Successful detection in this case is due to $\varphi(z_{23}) \neq \varphi(N-PSK)$.

2.3. $\varphi(p_1^{ED}) = \varphi(p_1^{LU}) + 180^\circ$ and $\varphi(p_2^{ED}) = \varphi(p_2^{LU}) + 180^\circ$

When both the non-legitimate pilots are reciprocal to the legitimate ones, i.e. their angles are shifted by 180 degrees from the angles of the LU's pilots, neither the original nor the improved scheme is able to detect the attack, since $\varphi(z_{12}) = \varphi(N-PSK)$ and $g_2=g_1$. The possibilities for the ED's and LU's third pilots are:

2.3.1. $\varphi(p_3^{ED}) = \varphi(p_3^{LU})$.

2.3.2. $\varphi(p_3^{ED}) = \varphi(p_3^{LU}) + 180^\circ$.

2.3.3. $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU})$ and $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU}) + 180^\circ$.

3. $p_1^{ED} = 0$

If the ED misses the first pilot session and initiates the contamination during the second training period, the original *2-N-PSK* method does not detect an attack in the case of the two scenarios presented below. The performance of the improved technique in this scenario depends on the third pilot value:

3.1. $p_1^{ED} = 0$ and $\varphi(p_2^{ED}) = \varphi(p_2^{LU})$.

3.1.1. $\varphi(p_3^{ED}) = \varphi(p_3^{LU})$: when the ED pilots in the second and third training intervals coincide with the LU pilots, the technique based on channel gains successfully detects an attack, as $g_2=g_3$.

3.1.2. $\varphi(p_3^{ED}) = \varphi(p_3^{LU}) + 180^\circ$: the channel gains in the second and third time slots are different, which prevents the improved scheme from detecting the ED.

3.1.3. $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU})$ and $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU}) + 180^\circ$: when the ED's pilot is the same as the legitimate pilot in the second training period but not equal to the legitimate pilot or its reciprocal in the third slot, the proposed technique reveals an attack, since $\varphi(z_{23}) \neq \varphi(N-PSK)$.

3.2. $p_1^{ED} = 0$ and $\varphi(p_2^{ED}) = \varphi(p_2^{LU}) + 180^\circ$.

3.2.1. $\varphi(p_3^{ED}) = \varphi(p_3^{LU})$: the different channel gains of the second and third pilots prevent the improved technique from discovering the ED's presence.

3.2.2. $\varphi(p_3^{ED}) = \varphi(p_3^{LU}) + 180^\circ$: the equality of the channel gain values, $g_2=g_3$, results in successful detection of an attack by the proposed improved technique.

3.2.3. $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU})$ and $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU}) + 180^\circ$: if the attacker's third pilot differs from both the legitimate one and its reciprocal, the improved technique reveals an intrusion due to $\varphi(z_{23}) \neq \varphi(N-PSK)$.

4. $\varphi(p_1^{ED}) = \varphi(p_1^{LU}) + x^\circ$ and $\varphi(p_2^{ED}) = \varphi(p_2^{LU}) + x^\circ$

Another shortcoming of the original *2-N-PSK* method is observed when both the pilots of ED are equally shifted from the corresponding legitimate pilots. When this situation occurs, the correlation angle is from the N-PSK constellation and the attack is not discerned. Moreover, the improved technique is also unreliable due to equal values of the channel gains in the first and the second training periods. Since the decision that an attack is not in progress is taken before the transmission of the third pilot, its value does not affect the final decision of the method. Hence, in the next two subcases the improved technique's implementation is not successful:

4.1. $\varphi(p_3^{ED}) = \varphi(p_3^{LU}) + x^\circ$.

4.2. $\varphi(p_3^{ED}) \neq \varphi(p_3^{LU}) + x^\circ$.

The detection probability of both the original and improved methods was analysed by conducting a large number of experiments separated into groups of simulations with random conditions. Ten independent attempts were performed for each group of simulations. The arithmetic mean values of the results are graphically presented in Fig. 6.

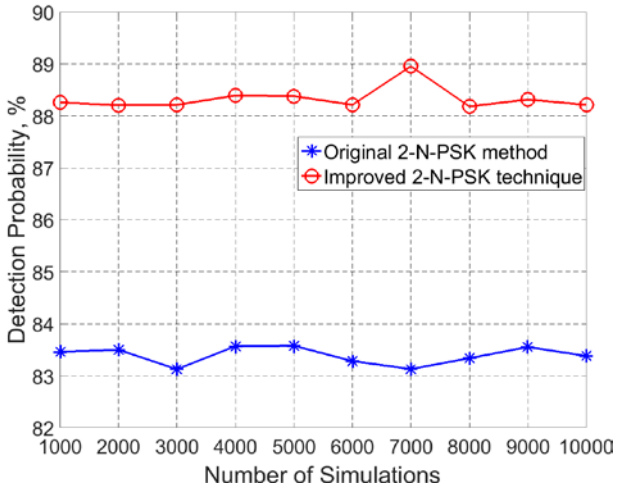

Fig. 6. Detection probability of the original *2-N-PSK* method and the improved technique

As can be seen from the figure, the mean detection probability of the different simulation groups is almost constant. Applying the proposed supplement to the *2-N-PSK* method, the probability of successful detection of pilot contamination attacks improves by about 5% compared to the results of the original *2-N-PSK* method.

The general purpose of the improved technique is to solve the detection problems of the original *2-N-PSK* method for attacks initiated during the second training period, i.e. the situation described in scenario 3) above. For this reason, another group of experiments was conducted which again selected pilots randomly but with ED always absent from the first pilot transmission. The detection probability results of the original method and improved technique for attacks starting with the second legitimate pilot are depicted in Fig. 7.

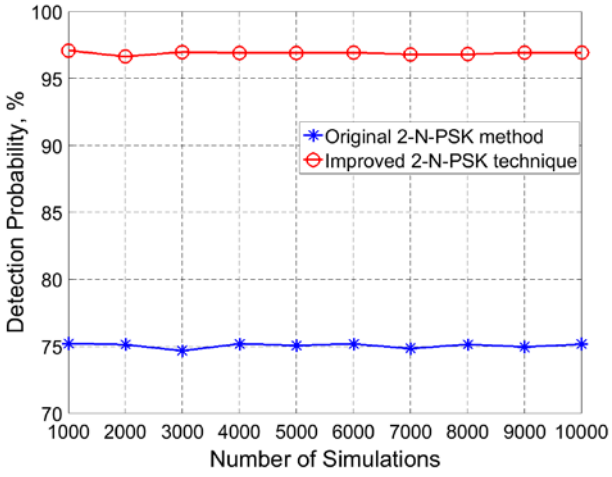

Fig. 7. Detection probability of the original *2-N-PSK* method and the improved technique when ED misses the first pilot transmission

The graphs show that, while the original *2-N-PSK* method detects this type of attack with a probability of around 75%, the improved technique results in a successful detection rate in excess of 96%. The experimental results demonstrate a significant improvement in the performance of the 2-*N-PSK* method when the proposed technique is also applied.

Since the proposed improved technique makes its decision based on three pilot transmissions, it makes sense to define an extended version of the original *2-N-PSK* method (*extended 2-N-PSK method*) that includes two correlations. Several of the four groups of detection problems listed above can be solved by observing the second correlation angle $\varphi(z_{23})$. The *extended 2-N-PSK method* is able to reveal an attack in the case where a third pilot is sent and the angle of the correlation between the second and third pilots differs from the N-PSK angles $\varphi(z_{23}) \neq \varphi(N-PSK)$. This is demonstrated in Table 1, where all of the detection problems listed above are investigated using both the *extended 2-N-PSK method* and the improved technique. The successfully solved problems are denoted as +, while the unresolved situations are denoted as –.

Detection Problem	Extended *2-N-PSK*	Improved Technique
1.1.	–	–
1.2.	–	–
1.3.	+	–
2.1.1.	–	–
2.1.2.	–	+
2.1.3.	+	+
2.2.1.	–	+
2.2.2.	–	–
2.2.3.	+	+
2.3.1.	–	–
2.3.2.	–	–
2.3.3.	+	–
3.1.1.	–	+
3.1.2.	–	–
3.1.3.	+	+
3.2.1.	–	–
3.2.2.	–	+
3.2.3.	+	+
4.1.	–	–
4.2.	+	–

Table 1. Detection problems solved by the extended original *2-N-PSK* method and the improved technique

Although the *extended 2-N-PSK method* significantly improves the performance of the scheme, the original method is designed to work with only two random pilots and hence does not include second correlation. For this reason, the

improved technique needs to be applied in order to increase the method's detection capabilities in certain situations.

6 Conclusion

It is important that effective schemes for the detection of pilot contamination attacks are employed in wireless systems and the communication needs to be suspended if such an attack is discovered.

In this paper an expansion of the original *2-N-PSK* method for the detection of pilot contamination attacks is proposed. The improvement does not cover the case when the attacker repeats both the pilots of the legitimate user and further investigation is needed in this direction. Although the solution improves the accuracy of the detection when the channel is static, its efficiency needs to be tested in the presence of noise.

In the case of low-power noise, it is possible to outline an area around the N-PSK symbols in which there is no ED present. In this situation the proposed technique will provide a good detection performance. When the signal-to-noise ratio is very low, comprehensive information about the noise power at the BS is necessary in order to improve the success rate of the method. These elements are important considerations for future studies.

Acknowledgment: This work was supported by the Scientific Project № 172ПД0016-07 of the Technical University – Sofia, Bulgaria

References:

[1] W. Trappe, The Challenges Facing Physical Layer Security, *IEEE Communications Magazine*, Vol. 53, No.6, 2015, pp. 16-20.

[2] Hui-Ming Wang and Xiang-Gen Xia, Enhancing Wireless Security via Cooperation: Signal Design and Optimization, *IEEE Communications Magazine*, Vol. 53, No. 12, 2015, pp. 47-53.

[3] Boulat A. Bash, Dennis Goeckel, Don Towsley, and Saikat Guha, Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication, *IEEE Communications Magazine*, Vol. 53, No. 12, 2015, pp. 26-31.

[4] X. Zhou, B. Maham, A. Hjorungnes, Pilot Contamination for Active Eavesdropping, *IEEE Trans. Wireless Commun.*, Vol. 11, No.3, 2012, pp. 903-907.

[5] Ta-Yuan Liu, Pin-Hsun Lin, Shih-Chun Lin, Y.-W. Peter Hong, Eduard Axel Jorswieck, To Avoid or Not to Avoid CSI Leakage in Physical Layer Secret Communication Systems, *IEEE Communications Magazine.*, Vol. 53, No. 12, 2015, pp. 19-25.

[6] B. A. Bash, D. Goeckel, D. Towsley, Limits of Reliable Communication with Low Probability of Detection on AWGN Channels, *IEEE JSAC*, Vol. 31, No. 9, 2013, pp. 1921–1930.

[7] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, F. Rusek, Detection of Active Eavesdroppers in Massive MIMO, *Proc. IEEE Int. Symp. Personal Indoor and Mobile Radio Commun. (PIMRC)*, 2014, pp. 585-589.

[8] D. Kapetanovic, G. Zheng, K.-K. Wong, B. Ottersten, Detection of Pilot Contamination Attack Using Random Training and Massive MIMO, *Proc. IEEE Int. Symp. Personal Indoor and Mobile Radio Commun. (PIMRC)*, 2013, pp. 13-18.

[9] D. Mihaylova, G. Iliev, Z. Valkova-Jarvis, Comparison of Methods for the Detection of Pilot Contamination Attacks, *Proc*. *BalkanCom*, Tirana, Albania, 2017.

[10] D. Kapetanovic, G. Zheng, F. Rusek, Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks, *IEEE Commun. Magazine*, Vol. 53, No. 6, 2015, pp. 21-27.