MATEC Web of Conferences **125**, 03007 (2017)
*CSCC 2017*
DOI: 10.1051/matecconf/201712503007

# An improved technique for the detection of pilot contamination attacks in TDD wireless communication systems

*Dimitriya* Mihaylova[1,*], *Zlatka* Valkova-Jarvis[1], and *Georgi* Iliev[1]

[1]Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria

**Abstract.** One of the problems phasing the physical layer security of a wireless system is its vulnerability to pilot contamination attacks and hence schemes for its detection need to be applied. A method proposed in the literature consists of training with two N-PSK pilots. Although the method is effective in most of the cases, it is not able to discover an attack initiated during the transmission of the second pilot from the pair if both the legitimate and non-legitimate pilots coincide. In this current paper, an improvement to this method is proposed which detects an intruder who misses the first pilot transmission. The suggested improvement eliminates the usage of threshold values in the detection – a main drawback of previously existing solution.

## 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], 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 [2].

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 confidentiality of a system are discussed in [3]. 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. By this active attack the intruder could overcome the passive eavesdropping resistance of a MaMIMO system, as is observed in [4].

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), and user mobility is not included.

The system model is depicted in Fig.1.

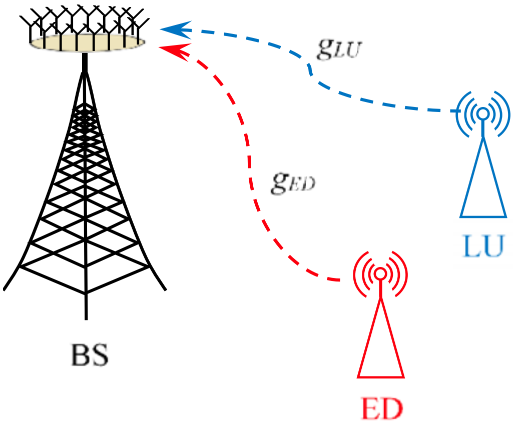

**Fig. 1.** The system model.

[*] Corresponding author: dam@tu-sofia.bg

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 [5]. This method consists in sending random 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:

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

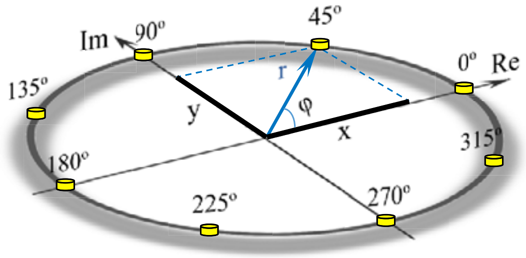

**Fig. 2.** Eight Phase Shift Keying (8-PSK) constellation diagram. Geometric representation of a complex number.

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):

$$\begin{aligned} y_1 &= g_{LU}\, p_1^{LU} + g_{ED} p_1^{ED} + n_1 = \\ &= \sqrt{P_{LU} d_{LU}}\, h_{LU}\, p_1^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_1^{ED} + n_1 \\ y_2 &= g_{LU}\, p_2^{LU} + g_{ED} p_2^{ED} + n_2 = \\ &= \sqrt{P_{LU} d_{LU}}\, h_{LU}\, p_2^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_2^{ED} + n_2, \end{aligned} \tag{3}$$

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.

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 decision is taken 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 [6], 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 reveal the legitimate channel 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 [7] 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

DOI: 10.1051/matecconf/201712503007

consequence of the natural imperfections of the channel, the ratio of the received signals is compared with some thresholds. A decision that a malicious user has sent a pilot during one of the slots is made 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.

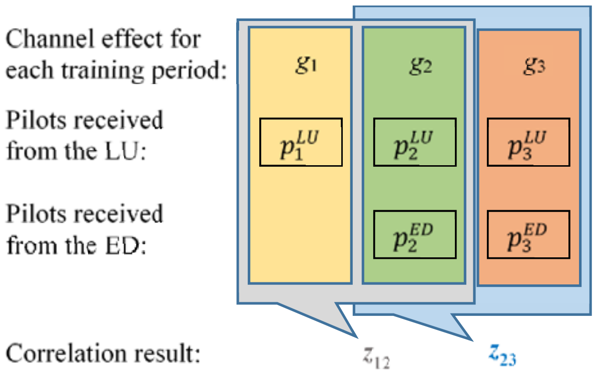

**Fig. 3.** Channel gain comparison for the received pilots.

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:

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

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

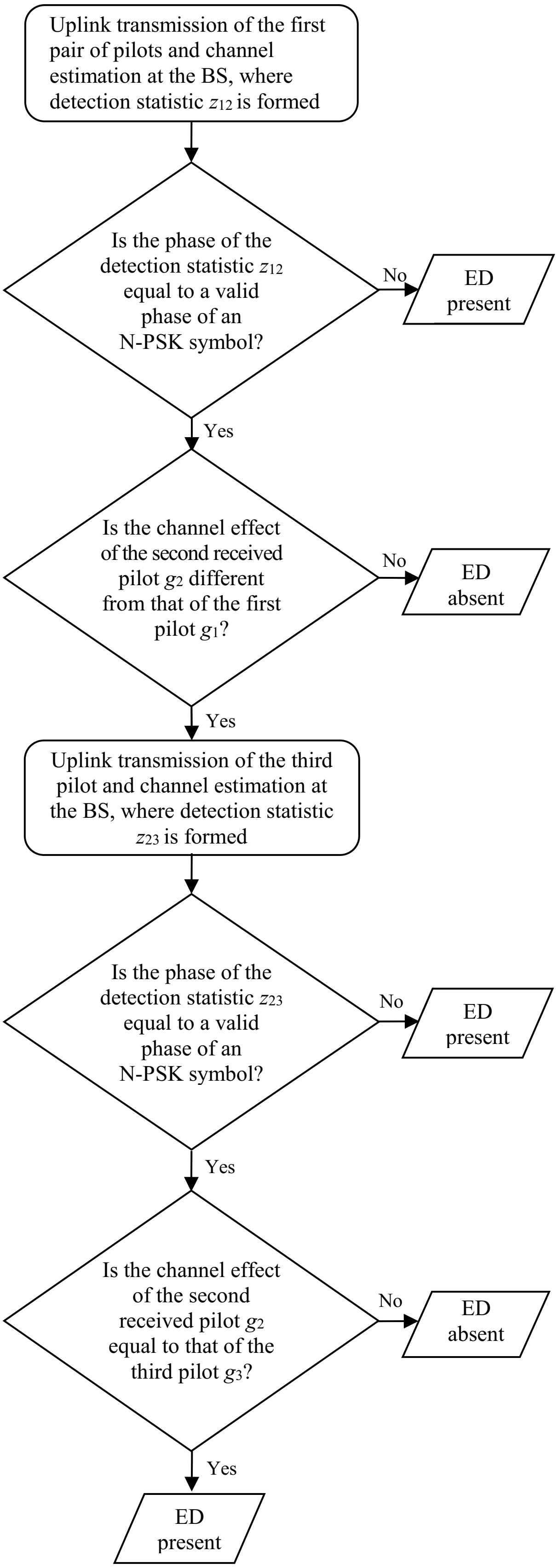
Uplink transmission of the first pair of pilots and channel estimation at the BS, where detection statistic $z_{12}$ is formed
Is the phase of the detection statistic $z_{12}$ equal to a valid phase of an N-PSK symbol?
No
ED present
Yes
Is the channel effect of the second received pilot $g_2$ different from that of the first pilot $g_1$?
No
ED absent
Yes
Uplink transmission of the third pilot and channel estimation at the BS, where detection statistic $z_{23}$ is formed
Is the phase of the detection statistic $z_{23}$ equal to a valid phase of an N-PSK symbol?
No
ED present
Yes
Is the channel effect of the second received pilot $g_2$ equal to that of the third pilot $g_3$?
No
ED absent
Yes
ED present

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

DOI: 10.1051/matecconf/201712503007

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:

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

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:

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

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 not taken into account. 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 $g_{ED} = 0.7$.

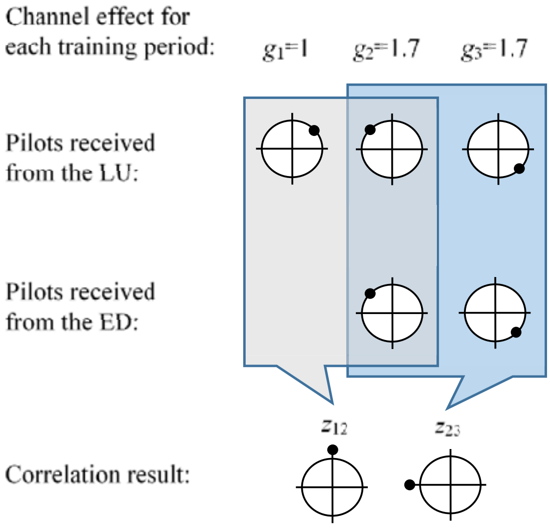
Channel effect for each training period:
$g_1$=1
$g_2$=1.7
$g_3$=1.7
Pilots received from the LU:
Pilots received from the ED:
$z_{12}$
$z_{23}$
Correlation result:

**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 could 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 Conclusion

Effective schemes for the detection of pilot contamination attacks are recommended for use in wireless systems and the communication needs to be interrupted if such an attack is discovered.

In this paper a complement of the 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 is supported by the Project № BG05M2OP001-2.009-0033-C01

## References

1. W. Trappe, IEEE Commun. Mag., **53**, 16-20, (2015)
2. X. Zhou, B. Maham, A. Hjorungnes, IEEE TWC, **11**, 903–907, (2012)
3. Ta-Yuan Liu, Pin-Hsun Lin, Shih-Chun Lin, Y.-W. Peter Hong, Eduard Axel Jorswieck, IEEE Commun. Mag., **53**,19–25, (2015)
4. D. Kapetanovic, A. Al-Nahari, A. Stojanovic, F. Rusek, *Proc. IEEE Int. Symp. PIMRC*, 2014
5. D. Kapetanovic, G. Zheng, K.-K. Wong, B. Ottersten, *Proc. IEEE Int. Symp. PIMRC*, 2013
6. D. Mihaylova, G. Iliev, Z. Valkova-Jarvis, *Proc. BalkanCom* (Tirana, Albania 2017)
7. D. Kapetanovic, G. Zheng, F. Rusek, IEEE Commun. Mag., **53**, 21–27, (2015)