International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:8, 2018

Relation of Optimal Pilot Offsets in the Shifted Constellation-Based Method for the Detection of Pilot Contamination Attacks

Dimitriya A. Mihaylova, Zlatka V. Valkova-Jarvis, Georgi L. Iliev

***Abstract*—**One possible approach for maintaining the security of communication systems relies on Physical Layer Security mechanisms. However, in wireless time division duplex systems, where uplink and downlink channels are reciprocal, the channel estimate procedure is exposed to attacks known as pilot contamination, with the aim of having an enhanced data signal sent to the malicious user. The *Shifted 2-N-PSK* method involves two random legitimate pilots in the training phase, each of which belongs to a constellation, shifted from the original N-PSK symbols by certain degrees. In this paper, legitimate pilots' offset values and their influence on the detection capabilities of the *Shifted 2-N-PSK* method are investigated. As the implementation of the technique depends on the relation between the shift angles rather than their specific values, the optimal interconnection between the two legitimate constellations is investigated. The results show that no regularity exists in the relation between the pilot contamination attacks (PCA) detection probability and the choice of offset values. Therefore, an adversary who aims to obtain the exact offset values can only employ a brute-force attack but the large number of possible combinations for the shifted constellations makes such a type of attack difficult to successfully mount. For this reason, the number of optimal shift value pairs is also studied for both 100% and 98% probabilities of detecting pilot contamination attacks. Although the *Shifted 2-N-PSK* method has been broadly studied in different signal-to-noise ratio scenarios, in multi-cell systems the interference from the signals in other cells should be also taken into account. Therefore, the inter-cell interference impact on the performance of the method is investigated by means of a large number of simulations. The results show that the detection probability of the *Shifted 2-N-PSK* decreases inversely to the signal-to-interference-plus-noise ratio.

***Keywords*—**Channel estimation, inter-cell interference, pilot contamination attacks, wireless communications.

I. Introduction

ONE possible attack that an eavesdropper (ED) can initiate against the security of a wireless system is the pilot contamination attack (PCA), introduced in [1]. Systems with time division duplex operation (TDD) are extremely vulnerable to such a type of malicious intervention where, due to reciprocity between uplink and downlink channels, a one way channel estimation procedure is conducted at the base station (BS). The channel gain is computed through the use of pilot signals received from the legitimate user (LU).

During the uplink training phase, ED, who intends to initiate a PCA, starts transmitting to the BS pilot signals from the same sequence as the one used by LU. Consequently, the calculated channel gain represents an estimate of both legitimate and non-legitimate channels and thus the information signal from BS is transmitted in both directions to LU and ED simultaneously.

Several suggested techniques for PCA detection exist, some using secret keys [2] or training by superimposed random sequence [3], [4], others based on large-scale fading comparison [5], or various detection statistics methods, such as the generalised likelihood ratio test method for validating one of two possible hypotheses [6], [7].

Another method for detecting PCAs – *2-N-PSK*, which includes training with two random N-PSK symbols, is described in [8] and evaluated in [9]. According to the *2-N-PSK* detection method, in case of PCA the argument of the correlation between the two training signals is not equal to any N-PSK angle. The correlation result z_{12} is calculated through (1) [8], where M is the number of antennas at BS, $(\cdot)^H$ stands for Hermitian matrix and n_{12} is the noise result. p_1^{LU} and p_2^{LU} denote the first and second legitimate pilots, while the non-legitimate ones are p_1^{ED} and p_2^{ED}. g_{LU} and g_{ED} describe the uplink channel from LU to BS and from ED to BS respectively and are obtained by (2), where $\sqrt{P_{LU}}$ and $\sqrt{P_{ED}}$ are the corresponding transmit power, $\sqrt{d_{LU}}$ and $\sqrt{d_{ED}}$ are the large-scale fading, and h_{LU} and h_{ED} are the small-scale fading, of LU and ED respectively:

$$z_{12} = \frac{1}{M}\left(g_{LU}\, p_1^{LU} + g_{ED}\, p_1^{ED}\right)^H \times \left(g_{LU}\, p_2^{LU} + g_{ED}\, p_2^{ED}\right) + n_{12}\,. \tag{1}$$

$$g_{LU} = \sqrt{P_{LU} d_{LU}}\, h_{LU} \qquad g_{ED} = \sqrt{P_{ED} d_{ED}}\, h_{ED}\,. \tag{2}$$

The *2-N-PSK* method is further studied in [10], where some types of PCAs are shown to be undetectable. These problematic scenarios are described below, with $\varphi(\cdot)$ representing the phase angle of the signal concerned.

1) $\varphi\left(p_1^{ED}\right) = \varphi\left(p_1^{LU}\right)$ and $\varphi\left(p_2^{ED}\right) = \varphi\left(p_2^{LU}\right)$: Both pilots of ED equal the corresponding legitimate pilot.
2) $\varphi\left(p^{ED}\right) = \varphi\left(p^{LU}\right) + 180^{\circ}$: The pilots of ED are reciprocal to the corresponding legitimate pilot or one is reciprocal

Dimitriya A. Mihaylova is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria (corresponding author, e-mail: dam@tu-sofia.bg).

Zlatka Valkova-Jarvis and Georgi Iliev are with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria (e-mail: zvv@tu-sofia.bg, gli@tu-sofia.bg).

and the other is equal.

3) $p_1^{ED}=0$ and $\varphi(p_2^{ED})=\varphi(p_2^{LU})$ or $p_1^{ED}=0$ $\varphi(p_2^{ED})=\varphi(p_2^{LU})+180^\circ$: The contamination is initiated during the second pilot transmission and the pilot of ED is equal or reciprocal to the legitimate.

4) $\varphi(p_1^{ED})=\varphi(p_1^{LU})+\varphi_x(N-PSK)$ and $\varphi(p_2^{ED})=\varphi(p_2^{LU})+\varphi_x(N-PSK)$: both the pilots of ED differ from the corresponding legitimate pilots by the same degrees.

In all types of attacks, listed from 1) to 4), the correlation result angle coincides with an N-PSK phase, i.e. $\varphi(z_{12}) = \varphi_x(N\text{-}PSK)$, which results in a decrease in the PCA detection probability of the *2-N-PSK*. For that reason, a method is proposed in [11] that follows the concept of *2-N-PSK* but works with shifted constellations – the *Shifted 2-N-PSK* method. *Shifted 2-N-PSK* improves the performance of the original *2-N-PSK* method, as proved in [12].

In this paper, the choice of offset values used to shift both legitimate constellations for the *Shifted 2-N-PSK* detection method is studied. Then the PCA detection probability of the method in a multi-cell scenario is analysed.

II. *Shifted 2-N-PSK* Detection Method

The strategy employed in *Shifted 2-N-PSK* consists in shifting the constellations of the two legitimate pilots by certain degrees – x_1 for every odd pilot and x_2 for every even one. This way, the correlation phase in the absence of PCA does not belong to the original and publicly-known N-PSK constellation, but instead coincides with an angle from a reference constellation. Odd and even reference constellations exist – for odd and even correlations, and they are obtained from the original N-PSK constellation by adding $y_1=x_2-x_1$ or $y_2=x_1-x_2$, correspondingly.

Since in *Shifted 2-N-PSK* LU sends pilots from shifted constellations, their repetition by ED is impossible and hence an intrusion of types 1) to 4) does not affect the detection system. However, the same PCAs with modified conditions may still escape detection by *Shifted 2-N-PSK*. For cases 1), 2) and 3), the attack can be undetectable if ED sends a pilot signal (or its reciprocal) whose angle is the closest N-PSK value to the argument of the shifted legitimate pilot. In order to successfully attack the system in accordance with 4), the adversary must send the N-PSK symbols closest in phase to the corresponding shifted legitimate pilots, increased by the same N-PSK angle. The analytical expression of this is given in (3), where i denotes the running number of the pilot in the pair, i.e. i=1 for the first pilot signal and i=2 for the second pilot:

$$\varphi^*(p_i^{LU})+\frac{360^\circ}{2N}\geq\varphi_{xi}(N-PSK)\geq\varphi^*(p_i^{LU})-\frac{360^\circ}{2N}. \quad (3)$$

The analogous description of the modified forms of 1), 2), 3), and 4), in the case of *Shifted 2-N-PSK*, is as follows:

1*) $\varphi(p_1^{ED})=\varphi_{x1}(N-PSK)$ и $\varphi(p_2^{ED})=\varphi_{x2}(N-PSK)$.

2*) $\varphi(p_i^{ED})=\varphi_{xi}(N-PSK)+180^\circ$.

3*) $p_1^{ED}=0$ and $\varphi(p_2^{ED})=\varphi_{x2}(N-PSK)$ or $p_1^{ED}=0$ и $\varphi(p_2^{ED})=\varphi_{x2}(N-PSK)+180^\circ$.

4*) $\varphi(p_1^{ED})=\varphi_{x1}(N-PSK)+\varphi_x(N-PSK)$ and $\varphi(p_2^{ED})=\varphi_{x2}(N-PSK)+\varphi_x(N-PSK)$.

The PCA detection probability depends on the choice of offset combination (x_1, x_2). The implementation of the following three scenarios is studied in [12], where $\varphi^*(\cdot)$ denotes the legitimate pilot's argument after the offset:

A. $x_1\neq x_2\neq\varphi_x(N-PSK)$ *and* $|x_1-x_2|\neq\varphi_x(N-PSK)$

When neither the legitimate nor the reference constellations coincide with the original N-PSK constellation, all detection problems from 1*) to 4*) are successfully solved.

B. $x_1=\varphi_x(N-PSK)$ *or* $x_2=\varphi_x(N-PSK)$

In the case where one of the shift values equals an N-PSK angle, while attacks of types 1*), 2*) and 4*) are always discoverable, 3*) can be only detected if the PCA is initiated during the transmission of a legitimate pilot which does not belong to the N-PSK constellation.

C. $|x_1-x_2|=\varphi_x(N-PSK)$

If both legitimate constellations differ from each other by an N-PSK angle, only attacks of types 2*) and 3*) are detectable. In this case, *Shifted 2-N-PSK* is not able to discover attacks of types 1*) and 4*).

III. Examination of Optimal Pilots Offset Relation in the *Shifted 2-N-PSK* Detection Method

The analysis of the variable behaviour of the *Shifted 2-N-PSK* detection method in scenarios *A*, *B* and *C*, formulated in Section II, indicates a need for a consequent investigation of the relation between both offsets of the legitimate pair's pilots. Thus a large number of experiments are conducted, where different values of the offset pairs (x_1, x_2) are chosen at a random.

Initially, specific N-PSK legitimate pilots shifted by different degrees are studied while all types of attacks listed from 1*) to 4*) in Section II are simulated. Two important trends are observed: The exact offset value does not influence the performance of the *Shifted 2-N-PSK* detection method in a consistent manner, and in certain situations the argument of the correlation result equals an angle whose value is very close to a phase from the reference constellation. This requires another study on whether any relation exists between the absolute value $\Delta=|x_1-x_2|$ and the location of the correlation result within the reference constellation. In order to achieve reliable results, again plenty of simulations are conducted, where fixed N-PSK legitimate pilots are shifted so that the impact of different values of Δ can be observed. No relation is found between the value of Δ and the similarity of contaminated correlations to the reference angles.

For simplicity, the experiments are implemented in a scenario where the presence of noise and interference is ignored. However, in a real system, if the signal to-interference and noise ratio (SINR)is not large enough, this could lead to an incorrect decision by the detection scheme. Especially susceptible to such a misinterpretation are correlations whose argument converges on a phase from the reference constellation. Due to the effect of noise or interference, the correlation angle may change and move closer to the reference angle so that both could be erroneously accepted as being equal. As a result, the capabilities of *Shifted 2-N-PSK* to detect PCA decrease substantially.

Another problem can arise in systems with limited computational capabilities when the correlation angle is close to a reference angle. In such systems, the calculated results are subject to rounding errors, which can also lead to judging that the correlation argument coincides with a reference phase when in reality it does not. Thus, it is reasonable to investigate different random values of the offset pairs (x_1, x_2) and the *Shifted 2-N-PSK* detection probability of PCAs in systems with differing precision. The system's precision is expressed by a distinguishing angle, which is used to indicate the largest angle in degrees by which a correlation phase can differ from the reference argument while both still being accepted as equal. The bigger the distinguishing angle, the smaller the accuracy of the system is. Hence the poorer the performance of the *Shifted 2-N-PSK* detection method is.

In the following simulations, the legitimate pilots before the offset, as well as the pilots of ED, are random signals, while the shift values of the legitimate constellations under study are fixed. The PCA detection probability of each combination (x_1, x_2) is calculated based on ten thousand simulations. Several examples of different offset pairs (x_1, x_2) can be observed in Fig. 1.

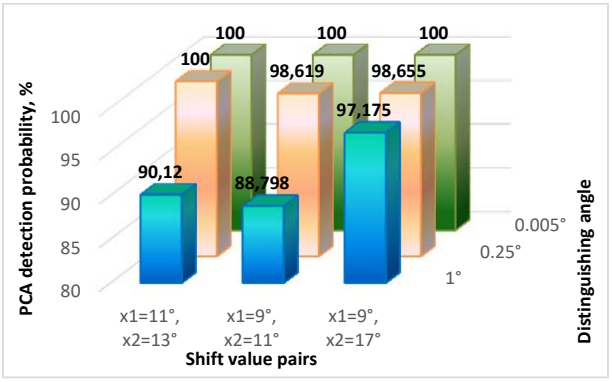

Fig. 1 PCA detection probability of Shifted 2-N-PSK with different offset pairs and distinguishing angles

The results in Fig. 1 prove that there is no relation between the shift values and the PCA detection probability of the system. While some combinations (x_1, x_2) lead to better results than others when examined at certain distinguishing angles, the opposite behaviour is observed in situations with different distinguishing angles. More specifically, the pair (x_1=11°, x_2=13°) gives better results than (x_1=9°, x_2=17°) at a distinguishing angle of 0.25° but when the distinguishing angle increases to 1°, the combination (x_1=9°, x_2=17°) improves the PCA detection probability of the method, compared to (x_1=11°, x_2=13°), by around 7%.

Another important conclusion that is confirmed by Fig. 1 is that none of the values of Δ influences the detection capabilities of the *Shifted 2-N-PSK* detection method. Keeping Δ constant and changing the shift values of the legitimate pilots does not maintain the same PCA detection probability, as can be seen from a comparison of the results with pairs (x_1=11°, x_2=13°) and (x_1=9°, x_2=11°).

The only relation between the alteration in offsets and the performance of the detection method is found in the case of 8-PSK modulation and lack of noise and interference. When an offset pair (x_1, x_2) results in a PCA detection probability of 100%, its derivative pairs (x_1+i45°, x_2+i45°) achieve the same results, where i = 1÷8. An 8-PSK modulation example is presented in Fig. 2.

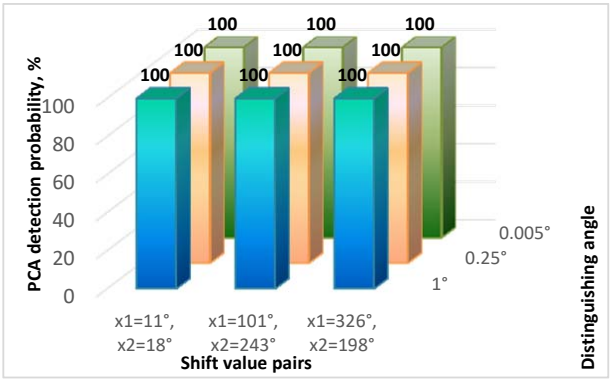

Fig. 2 An example offset pair, which gives a PCA detection probability of 100%, together with some of its derivative pairs for 8-PSK modulation scheme

The conducted experiments show that although some offset combinations (x_1, x_2) demonstrate better results than others, no relation can be found between the shift values alteration and the PCA detection probability achieved by the *Shifted 2-N-PSK* detection method. Only the recommendations following from scenarios *A*, *B* and *C* in Section II remain valid, namely that the best performance of the method is observed when neither the shifted legitimate constellations nor the reference ones coincide with the original N-PSK constellation. These conclusions are favourable from the point of view of security, as the only type of attack aiming at the discovery of the offset values which could succeed is a brute-force attack. However, a large number of combinations (x_1, x_2) that follow the abovementioned recommendations exist, which significantly hinders the successful implementation of such a type of attack. The number of advantageous shift value pairs can be further increased by degrading the step of their alteration to less than a degree.

As noted above, notwithstanding the lack of a logical interconnection, some offset combinations lead to improved

performance of the *Shifted 2-N-PSK* compared to others. For that reason, another useful experiment is conducted which ascertains the number of optimal shift value pairs (x_1, x_2) for different distinguishing angles, where a pair is recognized as optimal, if in absence of noise the method achieves PCA detection probability of 100%. Since in some systems lower requirements may be acceptable for the optimal pairs, the optimal pairs are also counted for an achieved PCA detection probability of 98%.

The investigation is completed for integer offset values x_1 and x_2 and an alternation step equal to one degree. Each of the shift values gradually changes from 0° to 359° and all possible combinations (x_1, x_2), 360×360=129 600 in number, are simulated. The PCA detection probability is computed based on ten thousand random simulations for each possible pair for different distinguishing angles. Only the number of optimal shift value pairs (x_1, x_2) is then extracted. The collected results are summarised in Fig. 3.

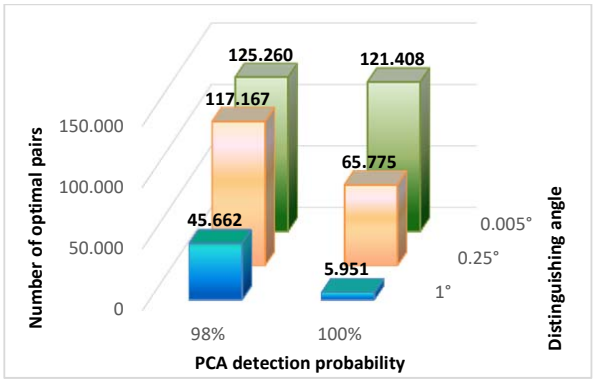

Fig. 3 Number of optimal offset pairs of *Shifted 2-N-PSK* with different distinguishing angles

According to the content of Fig. 3, the number of optimal combinations is highly dependent on the distinguishing angle. An increase in the distinguishing angle results in degradation of the system performance. In systems with precise computational capabilities, where the distinguishing angle is 0.005°, 100% PCA detection probability is observed in 121 408 offset combinations while 125 260 pairs (x_1, x_2) result in a PCA detection probability of more than 98%. A rough-scale system with distinguishing angle of 1° reaches 100% PCA detection probability by 5 951 number of optimal pairs, while 45 662 number of offset combinations achieves PCA detection probability of more than 98%.

IV. The Influence of Intercell Interference on the PCA Detection Probability of the *Shifted 2-N-PSK* Detection Method

The presence of intercell interference (ICI) represents a severe problem in multi-cell wireless systems. While the interference between users in a cell can be excluded by employing the orthogonal frequency division multiple access scheme (OFDMA), the signal received at the BS from users in neighbouring cells still influences the uplink training phase. This can cause some inaccuracy in the performance of the PCA detection method since, due to the presence of ICI, the correlation result may move further or closer to the reference constellation. In other words, a PCA initiated by a malicious user in the cell may be erroneously accepted as an effect of ICI, or vice versa. Hence, it is of great importance to estimate the detection capabilities of *Shifted 2-N-PSK* when the impact of interference is also considered.

The different variations of *Shifted 2-N-PSK*, explained in Section II, are separately studied together with the original 2-*N-PSK* method, so that their behaviour can be compared. The system model consists of multiple cells and only one of them – with the BS of interest, is observed. The only users in the cell of the serving BS are a single antenna LU and a single antenna ED. An example of the system model is illustrated in Fig. 4.

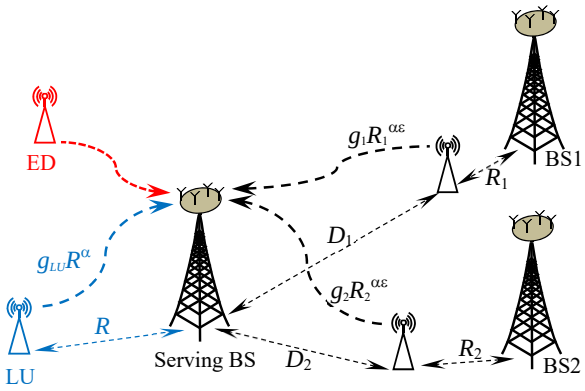

Fig. 4 An example of a multi-cell system model, where two users from adjacent cells interfere with the communication

An equation for defining SINR in uplink communication channels is suggested in [13]. The main components that take part in the analytical expression are the path loss exponent, denoted by α, and the power control factor – ε.

Typically the value of the power control factor is a fraction in the range [0, 1] where 0 means that all users in the cell transmit with the same power and 1 describes the case where the path loss is completely balanced. The main purpose of using power control management is to overcome the difference in received signal strength at the BS which is a consequence of unequal distances between the BS and users at different locations in the cell.

The decrease in signal power for specific propagation environments is expressed by the path loss exponent. Its value in wireless systems varies in the interval (2, 4) with 2 corresponding to free-space and 4 to a lossy environment.

The experiments conducted investigate the PCA detection probability of the *Shifted 2-N-PSK* method as a function of SINR, which is determined according to (3) [13]:

$$SINR = \frac{g_{LU} R^{\alpha(\varepsilon-1)}}{\sigma^2 + \sum_{u \in U} \left(R_u^{\alpha}\right)^{\varepsilon} g_u D_u^{-\alpha}}, \quad (3)$$

where the power of noise is expressed as σ^2, the desired signal receive power is $g_{LU}R^{-\alpha}$ and the distance from LU to the BS is denoted by R. U designates the set of interfering users and interfering user $u \in U$ is located at distances R_u and D_u from its serving BS and BS of interest, respectively.

The simulations are carried out assuming the following conditions: α=3.7, ε=0.75, $g_{LU}R^{-\alpha}$=-60.46 dBm, and σ^2=100 dBm. Typical SINR values are studied with varying ICI power. The results are graphically presented in Fig. 5.

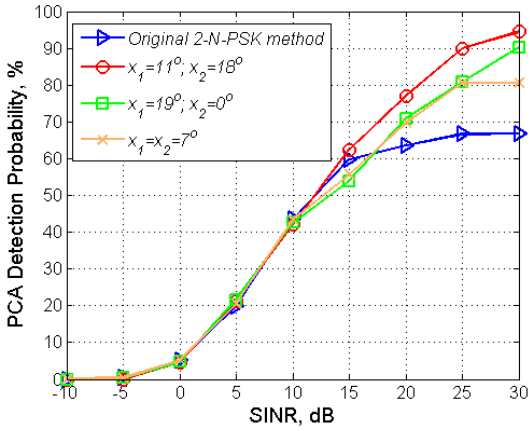

Fig. 5 Original *2-N-PSK* method and three different variations of *Shifted 2-N-PSK* method - PCA detection probability as a function of SINR

The experimental results confirm that in the low SINR range, where the impact of ICI is dominant, both detection methods demonstrate degraded performance and are not able to discover PCA initiated during the training phase. When the SINR value is less than 10dB, the PCA detection probability achieved by the different schemes is approximately the same. However, in the region where the signal power exceeds that of noise plus interference, such that SINR surpasses 10dB, improved detection capabilities of *Shifted -2-N-PSK* are apparent. As explained in Section II, the most favourable scenario of the *Shifted -2-N-PSK* detection method is the one described in case *A* which in the experiments conducted is represented by the combination (x_1=11°, x_2=18°).

V. Conclusion

In this paper the relation between the offset values of the Shifted 2-N-PSK method is studied, as well as the number of optimal combinations (x_1, x_2) for systems with different precision. In a future study, the behaviour of the method could be examined for more complex types of system accuracy.

As best secrecy of the shift value pairs can be achieved if they change for every training period, another future direction could include an algorithm for computing them at both the BS and LU sides.

Acknowledgment

The paper is published with the support of the project No BG05M2OP001-2.009-0033 "Promotion of Contemporary Research Through Creation of Scientific and Innovative Environment to Encourage Young Researchers in Technical University - Sofia and The National Railway Infrastructure Company in The Field of Engineering Science and Technology Development" within the Intelligent Growth Science and Education Operational Programme co-funded by the European Structural and Investment Funds of the European Union.

References

[1] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, March 2012.

[2] S. Tomasin, I. Land and F. Gabry, "Pilot Contamination Attack Detection by Key-Confirmation in Secure MIMO Systems", in *Proc. IEEE Globecom*, Washington, U.S.A, Dec. 2016.

[3] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, Oct. 2015.

[4] J. K. Tugnait, "Detection and identification of spoofed pilots in TDD/SDMA systems," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 550–553, Aug. 2017.

[5] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, "Detection of Active Eavesdroppers in Massive MIMO", *Proc. IEEE Int. Symp. PIMRC*, pp. 585-589, 2014.

[6] Sanghun Im, Hyoungsuk Jeon, Jinho Choi, and Jeongseok Ha, "Secret Key Agreement under an Active Attack in MU-TDD Systems with Large Antenna Arrays", in *Proc. Globecom*, 2013, pp. 1849–1855.

[7] J. M. Kang, C. In, and H. M. Kim, "Detection of pilot contamination attack for multi-antenna based secrecy systems," *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, 2015.

[8] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE Int. Symp. (PIMRC)*, pp. 13–18, Sept. 2013.

[9] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, June 2015.

[10] D. Mihaylova, Z. Valkova-Jarvis, and G. Iliev, "A New Technique to Improve the 2-N-PSK Method for Detecting Wireless Pilot Contamination Attacks", *WSEAS Trans. Commun.*, vol. 16, pp. 176-183, 2017.

[11] D. Mihaylova, Z. Valkova-Jarvis, G. Iliev, and V. Poulkov, "Shifted Constellation-Based Detection of Pilot Contamination Attacks", *Global Wireless Summit (GWS) 2017*, Cape Town, South Africa, 15-18 Oct. 2017.

[12] D. Mihaylova, Z. Valkova-Jarvis, and G. Iliev, "Detection Capabilities of a Shifted Constellation-based Method against Pilot Contamination Attacks", *Advances in Wireless and Optical Communications 2017 (RTUWO'17)*, Riga, Latvia, 2-3 Nov. 2017.

[13] T. Novlan, H. Dhillon, J. Andrews, "Analytical modeling of uplink cellular networks", *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2669-2679, June 2013.