Comparison of Methods for the Detection of Pilot Contamination Attacks

Dimitriya Mihaylova[1], Georgi Iliev[2], and Zlatka Valkova-Jarvis[3]

Abstract – **In the current paper, four different methods for the detection of pilot contamination attacks are examined and a comparison of their performance is provided. The main problem with the scheme with two pilots, its low detection probability, is solved when more pilots are used, but at the cost of reduced robustness against noise. The biggest disadvantage of the method which analyses the energy of the received signal is its large-scale fading dependence, which makes it vulnerable to attacks which imitate the natural channel improvement. Although the performance of the method based on secret key confirmation is not related to noise or fading, the technique significantly increases the computational complexity of the system.**

Keywords – **Pilot contamination attack, Channel estimation, Detection statistic, Key-confirmation.**

I. Introduction

Security is a fundamental topic in the new wireless networks. Conventionally, secure communication between wireless devices is provided by different cryptographic schemes, used on the upper layers of the OSI model. Another recently investigated strategy, which overcomes the computational complexity of crypto-algorithms, relates to the physical properties of the wireless channel.

A number of problems facing physical layer security (PLS) are emphasised in [1]. One such weakness is the assumption that channel prediction or estimation is difficult for a malicious user to carry out; this is not valid for simple environments with poor scattering. Such a scenario is discussed in [2], where the adversary (attacker) overcomes the passive eavesdropping resistance of a massive MIMO (MaMIMO) system by placing himself physically close to the legitimate receiver and using the correlation between the channels. However, the case in [2] also presents an active attack, known as pilot contamination, which the eavesdropper could mount against the channel estimation procedure.

A detailed description of a pilot contamination attack is given in [3]. In the PLS literature it is assumed that a legitimate user knows all the channel state information (CSI). For a time-division duplex (TDD) system, the CSI is obtained during the training phase when the transmitter estimates the legitimate channel by means of a pilot signal sent from the receiver. The pilot contamination attack consists in the eavesdropper sending pilots at the same time that the legitimate receiver does. The result is an erroneous channel estimation, leading to the incorrect design of the transmitter's precoder. As a consequence, there is an improvement in the data signal sent by the transmitter to the malicious user.

The pilot attack undermines security at the physical layer and could have a detrimental effect on the secrecy capability. Hence the significance of introducing schemes for the detection of a pilot contamination attack and the need to interrupt the communication if one is discovered.

The rest of the paper is organised as follows: in Section II the system mode is presented; section III describes different solutions proposed in the literature, which rely on the detection statistic of the received signal or require the use of secret keys. In Section IV the analysed methods are compared and section V concludes the paper.

II. System model

The current paper is focussed on a couple of studies based on different algorithms. The common scenario, used for simplicity, comprises a single cell, channels with Additive White Gaussian Noise (AWGN) and no user mobility. In addition, the models examine the situation depicted in Fig. 1, where a base station (BS) with multiple antennas M communicates with only one single-antenna legitimate user (LU), while one single-antenna eavesdropper (ED) tries to eavesdrop on the information exchange.

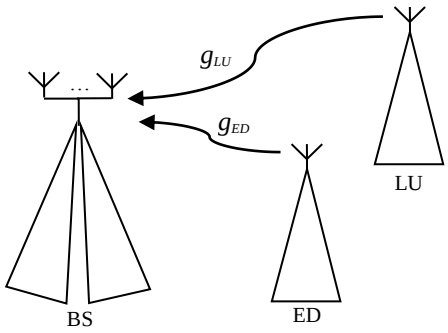

Fig. 1. System model

We assume a TDD system where reciprocity between uplink and downlink channels holds. During the uplink TDD phase both the LU and the ED synchronically send their pilot signals to the BS that undertakes channel estimation. After obtaining the CSI, the BS computes its precoder to match the characteristics of the estimated channel and performs beamforming in the downlink TDD phase.

The uplink channel from the LU to the BS is denoted as

[1]Dimitriya Mihaylova is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: dam@tu-sofia.bg.

[2]Georgi Iliev is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: gli@tu-sofia.bg.

[3]Zlatka Valkova-Jarvis is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: zvv@tu-sofia.bg.

$g_{LU} = \sqrt{P_{LU} d_{LU}}\, h_{LU}$ and includes the influence of the transmit power of the LU – P_{LU}, the large-scale fading which is a scalar - d_{LU}, and the small-scale fading h_{LU} which is a $M \times 1$ vector. Likewise, the channel from the ED to the BS is represented as $g_{ED} = \sqrt{P_{ED} d_{ED}}\, h_{ED}$, where P_{ED} is the ED's transmit power, d_{ED} is the large-scale fading and h_{ED} is a $M \times 1$ vector for the small-scale fading.

III. Detection Methods

A. Detection Statistic Schemes

The first group of methods is based on the detection statistic of the signal received at the BS. As the channel estimation of all three methods unified in this group is undertaken at the BS, they are resistant to attacks by jamming the LU.

1) *Two Random N-PSK Pilots Detection Scheme (2-N-PSK)*

One of the methods proposed in the literature is based on sending two random N-PSK symbols during the channel estimation phase [4]. A geometric constellation of the 8-PSK is depicted in Fig. 2, where a vector representation of a complex number q by its module and phase is shown.

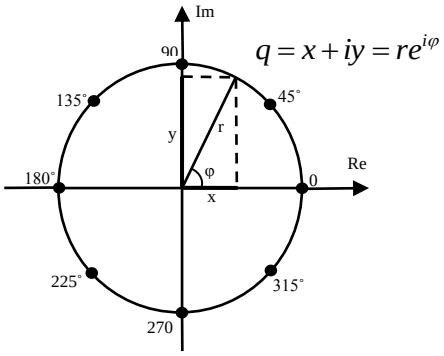

Fig. 2. Geometric representation of a complex number

The pilot symbols are publicly known, so the ED can send the same pilot sequence as the LU and its behaviour would not be recognised by the BS during the process of obtaining the CSI. For that reason, to enable detection of the malicious user at the BS an analysis is made of the scalar product of the correlation between the two received N-PSK vectors. The signals received at the BS for each of the two training periods are given by Eq. (1):

$$\begin{aligned} y_1 &= g_{LU} p_1^{LU} + g_{ED} p_1^{ED} + n_1 = \\ &= \sqrt{P_{LU} d_{LU}}\, h_{LU} p_1^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_1^{ED} + n_1, \\ y_2 &= g_{LU} p_2^{LU} + g_{ED} p_2^{ED} + n_2 = \\ &= \sqrt{P_{LU} d_{LU}}\, h_{LU} p_2^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_2^{ED} + n_2, \end{aligned} \quad (1)$$

where p_1^{LU} and p_1^{ED} are the pilots sent from the LU and the ED respectively during the first training slot and p_2^{LU} and p_2^{ED} are the pilots from the second training interval. n_1 and n_2 denote the AWGN in the first and the second slot respectively.

The correlation follows Eq. (2), which forms the detection statistic z as the phase of $y_1^H y_2$. $(\cdot)^H$ stands for Hermitian matrix and n_{12} is the noise result:

$$\begin{aligned} z_{12} = \frac{y_1^H y_2}{M} = \frac{1}{M} &\left(\sqrt{P_{LU} d_{LU}}\, h_{LU} p_1^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_1^{ED}\right)^H \times \\ &\left(\sqrt{P_{LU} d_{LU}}\, h_{LU} p_2^{LU} + \sqrt{P_{ED} d_{ED}}\, h_{ED} p_2^{ED}\right) + n_{12} \end{aligned} \quad (2)$$

Depending on the correlation result and the angle of its vector, we could detect the presence of the ED. If the angle of z_{12} does not converge to an angle of a valid N-PSK symbol, the non-legitimate user is present in both the training slots. Otherwise, we conclude that the ED appears in only one of the intervals if z_{12} converges to a valid N-PSK phase but the power received at the BS during one of the slots is larger than that during the other. Only when the angle of the correlation result converges to a valid N-PSK phase and the received powers at the BS during both the slots coincide will there be no ED in either of the training slots. The approach is summarised in Fig. 3.

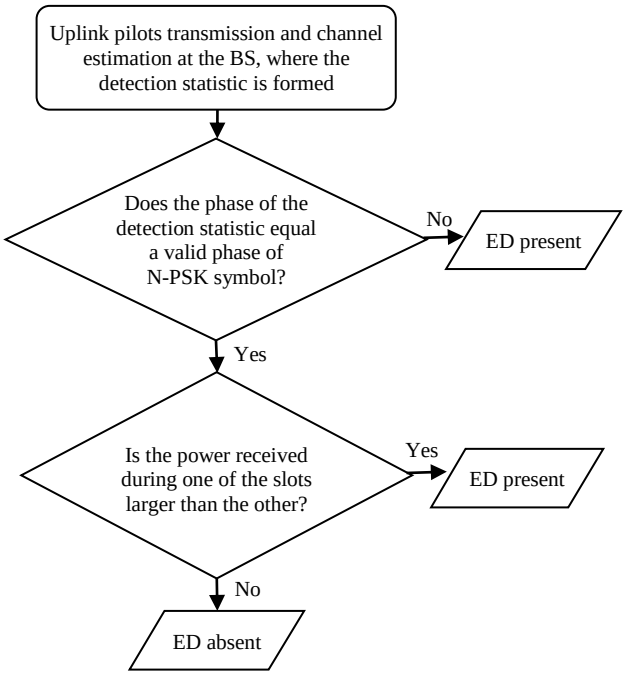

Fig. 3. Flow chart of the *2-N-PSK* method

2) *L Random N-PSK Pilots Detection Scheme (L-N-PSK)*

The second method studied for discovering a pilot contamination attack repeats the logic of the two random pilots detection scheme but is applied to L number of pilots, aiming at better performance. The block diagram of the method is shown in Fig. 4.

The main idea is to construct the matrix R as it is shown in Eq. (3) and analyse its rank. If R converges to a rank-one matrix, then the ED is absent. When there is an intervention from a non-legitimate user, R converges to a full-rank matrix.

$$R = \frac{y^H y}{M} + W \,, \tag{3}$$

where $y = [y_1, y_2, ..., y_L]$ is a $1 \times L$ row-vector composed of the signals received at the BS from the sent pilots, and W is an $L \times L$ noise matrix.

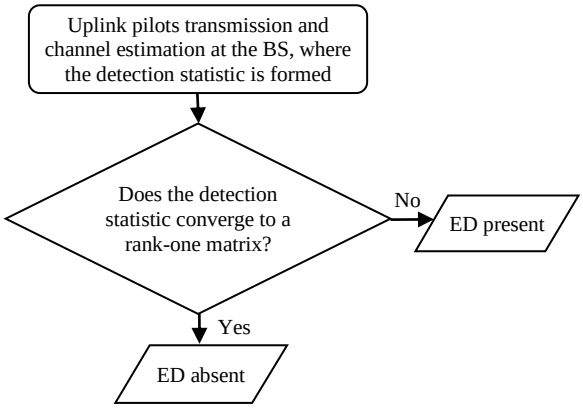

Fig. 4. Flow chart of the L-N-PSK method

3) *Generalised Likelihood Ratio Test (GLRT) Scheme*

Another method, introduced in [5] and [6] and expanded in [7], could be applied in the case of a system with multiple legitimate receivers. This technique employs the GLRT for distinguishing between two models, each of which has no unknown parameters. Therefore, the model is applicable only when the large-scale fading of every LU is determined in advance. On the other hand, the large-scale fading of the ED is not revealed to the BS and the LUs, and for the purposes of GLRT its influence should be replaced with its maximum-likelihood estimate (MLE).

During the uplink phase all the LUs, K in number, simultaneously send their training sequences ψ to the BS at the beginning of each coherence block. The pilot sequences of the users are orthonormal to one another and thus enable individual channel estimation at the BS. Each training sequence consists of L number of pilots and represents a $1 \times L$ vector that for the k-th user is denoted as $\sqrt{L}\psi_k$.

In the case where an ED contaminates the pilot sequence of the l-th LU, the signal received at the BS is:

$$Y = \sum_{k=1}^{K} \sqrt{P_{LU} d_{LU_k}} L h_{LU_k} \psi_k + \sqrt{P_{ED} d_{ED}} L h_{ED} \psi_l + W \,, \tag{4}$$

where P_{LU} is the transmit power of each LU and W is a M x L noise matrix.

The signal received at the BS for the l-th user is given by Eq. (5), where $c_l = P_{LU} d_{LU_l} L$, $\omega = \sqrt{\frac{P_{ED} d_{ED}}{P_{LU} d_{LU_l}}}$ is the degree of direction steering toward the ED, and $w_l = W \psi_l^H$ is the noise vector:

$$y_l = Y \psi_l^H = \sqrt{c_l} \left(h_{LU_l} + \omega h_{ED} \right) + w_l \,. \tag{5}$$

The GLRT algorithm defines two models: the Null and Alternative hypotheses, H_0 and H_1 respectively. The Null hypothesis considers that the ED is absent, the Alternative that the ED is present. Both the hypotheses are formulated by the detection statistic at the BS - y_l, which indicates the variance of the energy in the two cases. A larger variance is observed in H_1:

$$\begin{aligned} H_0 &: y_l = \sqrt{c_l} h_{LU_l} + w_l; \\ H_1 &: y_l = \sqrt{c_l} \left(h_{LU_l} + \omega h_{ED} \right) + w. \end{aligned} \tag{6}$$

As ω is dependent on the ED's large-scale fading, which is an unknown parameter, its value in the GLRT equation should be replaced by its MLE. By doing so, the final decision for validating one of the hypotheses follows Eq. (7), where λ is the sensitivity of the detector:

$$\ln \Lambda_1(y_l) = \frac{\|y_l\|^2}{(1+c_l)M} - \ln \left\{ \frac{\|y_l\|^2}{(1+c_l)M} \right\} - 1 \underset{H_0}{\overset{H_1}{\gtrless}} \frac{\ln \lambda}{M} \,. \tag{7}$$

A brief interpretation of the method can be seen in Fig. 5.

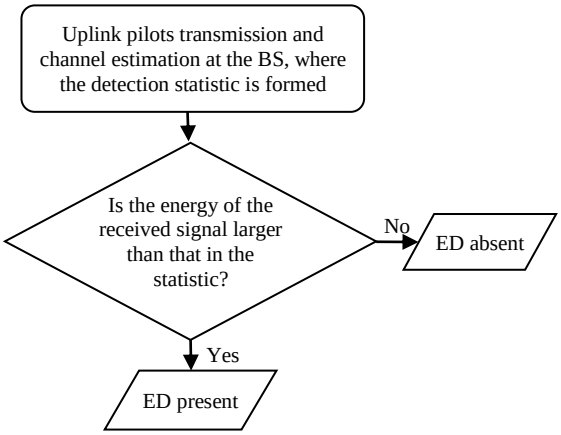

Fig. 5. Flow chart of the *GLRT* method

B. Secret Keys (SKs) Confirmation Scheme

A method, explored in [8], reveals the presence of the ED by means of bilateral channel estimation. In the first training phase, the BS sends publicly-known pilots to the LU, which obtains the CSI of g_{LU}. During the second training phase, the LU sends pilots to the BS where another assessment of the legitimate channel is made. Then both the estimations are compared following a key-confirmation procedure, explained briefly in Fig. 6.

From their estimation results both the BS and the LU extract their secret keys (SKs) in the form of N-bit numbers – a and b respectively. Thereafter, the BS generates a random sequence of bits in the same length – r, which is added modulo-two to the BS's SK and the result $x = r + a$ is sent to the LU. The LU decrypts the message, applying modulo-two sum with its SK, and gets $r' = x + b$, which is given to the input of an invertible non-identity function $f(r')$. The encrypted result $y = f(r') + b$ is then transmitted to the BS. At the BS, the random bit sequence r is processed with the same

function *f(r)* and the mapped value is compared with the decrypted message received from the LU - $z = y + a$. If, apart from noise, both the values coincide, i.e. $f(r) = z$, the SKs of the BS and the LU are the same and the BS concludes that there is no active ED contaminating the pilots. Conversely, if the ED is present in one of the training periods both the CSIs differ more than the noise level and the SKs of the BS and the LU are different.

In a scenario when the ED attacks the two pilot phases, the SKs do not coincide because the obtained CSIs at the BS and the LU are influenced by two different channels - the channel between the ED and the BS and that between the ED and the LU.

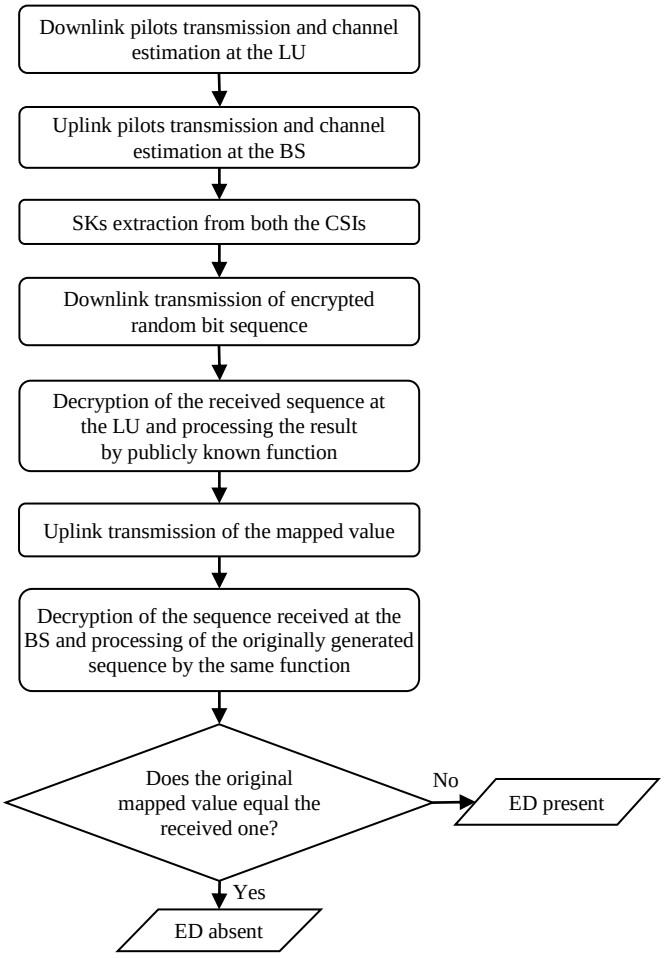

Fig. 6. Flow chart of the *SKs* method

IV. Comparison of the Proposed Solutions

In this section a comparison of the proposed solutions is given, observing some of their substantial advantages and drawbacks.

The common requirement for the proper implementation of all the techniques discussed is the large antenna array at the BS, as increasing the number of its antennas significantly improves the detection probability of all the methods. However, a good performance of the *GLRT* and the *SKs* methods is feasible even in a conventional MIMO system, while the *2-N-PSK* and *L-N-PSK* schemes are reliable only in a MaMIMO scenario. Another feature, validated in the literature, is that the four reviewed solutions are resistant to variations of the ED's transmit power and the more powerful the ED, the more detectible, and hence the better the performance of the detection schemes.

One main advantage of the *2-N-PSK* detection strategy over the others is its reduced complexity. No prior channel knowledge is needed and the performance is robust against noise, so good results are obtained at low SNRs.

The *L-N-PSK* technique demonstrates better detection probability at moderate to high SNRs, at the cost of an increase in the number of pilots, the complexity and the time needed for the training phase. Another drawback of the *L-N-PSK* scheme is its sensitivity to noise.

Overviewing the *GLRT* method, we could say that this is the only one of the discussed methods that does not require any special changes to the general MIMO system model. Moreover, although prior channel knowledge is needed, no overhead is introduced during the training phase. However, the period for training is long, which means that more resources like time and energy are required.

A main disadvantage of this method is its dependence on the large-scale fading coefficients. The analysis that the ED is present is based on the energy allocation of the signal received at the BS, i.e. the increased variance of the contaminated signal compared to the non-contaminated one. The authors in [2] present a strategy that the ED could employ to deceive any detection scheme reaching a decision only from the estimation of the large-scale fading enlargement.

The posited behaviour of the ED consists of imitating the natural channel improvement. That is to say, the ED starts sending pilots at low power and increases them gradually over the separate coherence intervals of the large-scale fading. As the value of d_{LU} changes slowly over time and frequency, the BS cannot detect the intervention of the ED and concludes that no pilot contamination attack is underway.

Apart from the *GLRT* technique none of the other three methods discussed in the current paper utilises the knowledge of the large-scale fading coefficients to reveal the ED's presence.

A drawback common to all the three schemes that obtain the CSI by detection statistics is that their decision rules mainly use the phase information of the signal received at the BS. In consequence, they are vulnerable to phase noise induced due to hardware imperfections. In contrast, the *SK* technique is based only on theoretical principles and exhibits strong phase noise resistance.

Looking closely at the *SKs* method, its main benefit is reliable detection without the need for any prior knowledge of the channel. Since the technique does not rely on signal processing mechanisms, it is resistant to noise and interference. Its main disadvantages include increased complexity, a long training period, large overhead, and vulnerability to jamming of the signal at the LU due to its participation in the channel estimation procedure.

For comparison purposes the most important features of the methods discussed are given in Table I, where the degree of relation between each technique and the given properties is denoted by *L* for *low* and *H* for *high*. *N* is used for *none* to

indicate that the method does not depend on the current feature.

TABLE I
COMPARISON OF THE DETECTION METHODS

	2-N-PSK	*L-N-PSK*	*GLRT*	*SKs*
SNR dependence	*L*	*H*	*H*	*L*
Knowledge of large-scale fading necessity	*N*	*N*	*H*	*N*
Phase noise dependence	*H*	*H*	*H*	*N*
Number of antennas dependence	*H*	*H*	*H*	*H*
MaMIMO necessity	*H*	*H*	*N*	*N*
Prior channel knowledge necessity	*N*	*N*	*H*	*N*
System model changes necessity	*H*	*H*	*N*	*H*
Complexity	*L*	*L*	*H*	*H*
Long training period	*L*	*L*	*H*	*H*
Overhead induced	*L*	*L*	*N*	*H*
Robustness to ED's power variations	*H*	*H*	*H*	*H*
Robustness to jamming the LU	*H*	*H*	*H*	*N*

The execution of the different solutions could be compared by the basic performance parameters of each detection scheme. The performance parameter for the three techniques that are based on the statistics of the contaminated training is the probability of detection of the ED's presence which is denoted as p_{DP}. While the execution of both the *N-PSK* schemes is strongly dependent on the SNR, the crucial parameter for the *GLRT* method is the degree of direction steering toward the ED – ω, which is related to the transmission power and the large-scale fading of the LU and the ED. Since the fundamental principles of the *SKs* algorithm are based more on information from theoretical approaches rather than signal processing, the performance of the system could be analysed by the secrecy outage probability (SOP) – p_{OUT}. The SOP is defined as the probability that the ED knows something about the secret message or key and is affected by the degree of correlation between the legitimate and non-legitimate channels, measured by the correlation factor – ζ.

Some interesting values of the performance parameters of the different schemes are given in Table II:

TABLE II
SYSTEM PERFORMANCE OF THE DETECTION METHODS

	2-N-PSK	*L-N-PSK*	*GLRT*	*SKs*
Crucial parameter	SNR = 0dB	SNR = 0dB	ω^2 = -10dB	$\zeta = 1$
Performance parameter	$p_{DP} \to 0.5$	$p_{DP} \to 1$	$p_{DP} \to 1$	$p_{OUT} \to 10^{-2}$

An overview of the data in Table II shows that for SNR = 0dB the detection probability of the *2-N-PSK* scheme converges to 0.5 while at the same level of SNR the probability of successful discovery the presence of an ED with the *L-N-PSK* scheme converges to 1. However, at low SNRs in the order of -10dB, the behaviour of the *2-N-PSK* is significantly better than that of the *L-N-PSK* technique. The detection probability of the *GLRT* scheme converges to 1 when the square of the steering toward the ED is -10dB. When the value of the critical parameter for the *SKs* method, i.e. the correlation factor, is high, the outage probability of the model converges to 0.01 leading to quite weak system performance.

V. CONCLUSION

The current paper reviews four methods for detecting a pilot contamination attack. All the solutions are discussed for a single-cell model, AWGN and no users' mobility. A future study could be aimed at a more realistic scenario with multi-cell system where users' mobility holds and the noise has complex distribution. Other research could investigate to what extent increasing the number of pilots in the *L-N-PSK* scheme achieves a related improvement in detection performance.

ACKNOWLEDGEMENT

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 Commun. Mag.*, vol. 53, no. 6, pp. 16–20, June 2015.

[2] 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.

[3] 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.

[4] 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)*, Sept 2013, pp. 13–18.

[5] 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.

[6] Sanghun Im, Hyoungsuk Jeon, Jinho Choi, and Jeongseok Ha, "Robustness of Secret Key Agreement Protocol with Massive MIMO under Pilot Contamination Attack," in *Proc. ICTC*, 2013, pp. 1053–1058.

[7] Sanghun Im, Hyoungsuk Jeon, Jinho Choi, and Jeongseok Ha, "Secret Key Agreement with Large Antenna Arrays under the Pilot Contamination Attack,"*IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6579–6594, Dec. 2015.

[8] 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.