IMPLEMENTING EFFICIENT MECHANISM FOR SECURE TRANSMISSION AGAINST SPOOFING ATTACK

[1]Karpagam.T
Assistant Professor

[2]Kamatchi.S
kamusweeton94@gmail.com
PG student

[3]Divya M
Assistant Professor

Department of Computer Science and Engineering
T.J.S. Engineering College

Abstract

The pilot spoofing attack is one kind of active eavesdropping activities conducted by a malicious user during the channel training phase. By transmitting the identical pilot (training) signals as those of the legal users, such an attack is able to manipulate the channel estimation outcome, which may result in a larger channel rate for the adversary but a smaller channel rate for the legitimate receiver. With the intention of detecting the pilot spoofing attack and minimizing its damages, we design a two-way training-based scheme. The effective detector exploits the intrusive component created by the adversary, followed by a secure beamforming-assisted data transmission. In addition to the solid detection performance, this scheme is also capable of obtaining the estimations of both legitimate and illegitimate channels, which allows the users to achieve secure communication in the presence of pilot spoofing attack. The detection probability is evaluated based on the derived test threshold at a given requirement on the probability of false alarming. The achievable secrecy rate is utilized to measure the security level of the data transmission. Our analysis shows that even without any pre-assumed knowledge of eavesdropper, the proposed scheme is still able to achieve the maximal secrecy rate in certain cases. Numerical results are provided to show that our scheme could achieve a high detection probability as well as secure transmission.

1. Introduction

AS WIRELESS networks are bearing larger and larger responsibilities of our essential activities, it is crucial to protect the wireless transmission against either passiveor active attack from any adversary. Classic cryptographic methods achieved secure communication by encrypting the confidential message as the unreadable cipher message, only the authentic receiver with valid secret key could decrypt and obtain the correct information. However, another method dedicated to achieve secure transmission based on the physical layer property, named as physical layer security, has been proposed even before the cryptographic method.

Other than the passive eavesdropping, the adversary could choose the active attack instead. One intelligent attack is called the spoofing attack, in which the adversary pretends to be the legitimate transmitter to spread false messages, or be the legitimate receiver to filch confidential information. This spoofing attack is originally studied in cyber network. Though some related detection algorithms are designed based on utilizing the physical layer properties, e.g., comparing the channel state information in neighbouring time slots. However, recent study illustrates that spoofing attack could also happen in the physical layer of communication systems.

Due to that the CSI is essential for data transmission and reception, a pilot-assisted channel estimation method is widely used in practical systems. For example, in a time duplex division (TDD) system, the legal receiver is required to send the assigned pilot signals to the transmitter, and the CSI can be estimated based on the received pilot signals due to the reciprocity of the uplink and downlink channels. The pilot signal set is pre-designed and known by the transmitter and receiver, and different pilot signals are usually orthogonal to each other to avoid contamination phenomenon. Because of being repeatedly used and publicly known, the knowledge.of pilot signals could easily be learned by an adversary, and the spoofing attack to the transmitter becomes possible by broadcasting the identical pilot signal as that of a legitimate receiver. By doing so, the adversary could manipulate the channel estimation result and benefit from the attack. If the transmitter is equipped with

multiple antennas to perform beamforming during downlink transmission.

2.Preliminaries

Channel Model

The transmitter Alice has multiple antennas and both the receiver Bob and the eavesdropper Eve are equipped with a single antenna. In a TDD system, Bob sends the assigned pilot signal to let Alice estimate the channel. Meantime, Eve conducts the pilot spoofing attack by sending the same pilot signals to Alice. In this work, we assume that the channels are block fading, i.e., the CSI remains constant during a given time frame length (denoted as N) and changes independently among different time frames. As shown in Fig. 2, the coherence time length N is mainly splitting into three parts: uplink training with N_1, downlink training with N_2 and data transmission for N_d . D_1 indicates the data information of the channel estimation result from Alice. The length of D_1 and result feedback are assumed to be short enough therefore negligible.

Threshold value

Two way training detector is used to detect the attack. It is done based on the threshold value. If the presence of attack is confirmed then it can estimate the channels of both the legitimate and illegitimate users. It produces an approximate value with more accuracy compared to Energy Ratio Detector

Beam forming

It uses MIMO technique Multi-input-Multi-output.It gives a maximum positive secrecy rate in the legitimate as well as illegitimate channel. Maximizing the beam forming with the use of artificial noise. It leads to unavailable of eavesdropper in their respective channels.

3.Literature Review

3.1Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information

In this letter, we consider physical layer security in multiple-input single-output (MISO) fading wiretap channels, where the transmitter utilizes a jamming-aided precoding transmission strategy to maximize the achievable secrecy rate of the channel. The instantaneous channel state information (CSI) of the eavesdropper's channel is considered unavailable at the transmitter. We derive the closed-form expression of the ergodic secrecy rate, based on which we find that there exists an optimal power allocation ratio between the information signal and the jamming signal.

3.2Pilot contamination for active eavesdropping

In this letter, we discuss how an active eavesdropper can attack the training phase in wireless communication to improve its eavesdropping performance. We derive a new security attack from the pilot contamination phenomenon, which targets at systems using reverse training to obtain the CSI at the transmitter for precoder design. This attack changes the precoder used by the legitimate transmitter in a controlled manner to strengthen the signal reception at the eavesdropper during data transmission. Furthermore, we discuss an efficient use of the transmission energy of an advanced full-duplex eavesdropper to simultaneously achieve a satisfactory eavesdropping performance whilst degrading the detection performance of the legitimate receiver.

3.3Detection of pilot contamination attack using random training and massive MIMO

In this paper, we devise a technique which employs random pilots chosen from a known set of phase-shift keying (PSK) symbols to detect pilot contamination. The scheme only requires two training periods without any prior channel knowledge. Our analysis demonstrates that using the proposed technique in a massive MIMO system, the detection probability of pilot contamination attacks can be made arbitrarily close to Simulation results reveal that the proposed technique can significantly increase the detection probability and is robust to noise power as well as the eavesdropper's power.

3.4A semi-blind two-way training method for discriminatory channel estimation in MIMO systems

Discriminatory channel estimation (DCE) is a recently developed strategy to enlarge the performance difference between a legitimate receiver (LR) and an unauthorized receiver (UR) in a multiple-input multiple-output (MIMO) wireless system. Specifically, it makes use of properly designed training signals to degrade channel estimation at the UR which in turn limits the UR's eavesdropping capability during data transmission. In this paper, we propose a new two-way training scheme for DCE through exploiting a whitening-rotation (WR) based semiblind method. To characterize the performance of DCE, a closed-form expression of the normalized mean squared error (NMSE) of the channel estimation is derived for both the LR and the UR. Furthermore, the developed analytical results on NMSE are utilized to perform optimal power allocation between the training signal and artificial noise.

3.5Channel based detection of Sybil attacks in wireless networks

Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to

Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. We propose an enhanced physical-layer authentication scheme to detect Sybil attacks, exploiting the spatial variability of radio channels in environments with rich scattering, as is typical in indoor and urban environments. We build a hypothesis test to detect Sybil clients for both wideband and narrowband wireless systems, such as WiFi and WiMax systems. Based on the existing channel estimation mechanisms, our method can be easily implemented with low overhead, either independently or combined with other physical-layer security methods, e.g., *spoofing* attack detection. The performance of our Sybil detector is verified, via both a propagation modeling software and field measurements using a vector
network analyzer, for typical indoor environments.

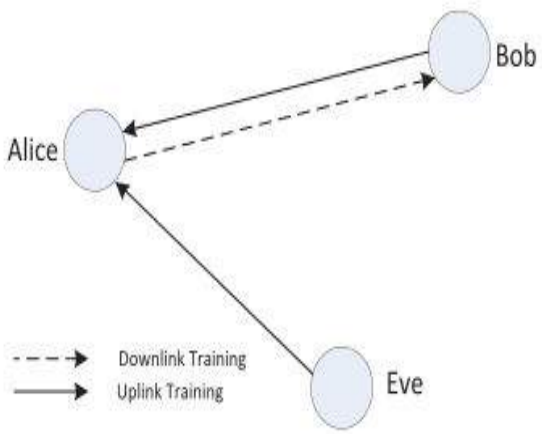

Fig 5: System Architecture

4. Existing System

The knowledge of pilot signals could easily be learned by an adversary, and the spoofing attack to the transmitter becomes possible by broadcasting the identical pilot signal as that of a legitimate receiver. By doing so, the adversary could manipulate the channel estimation result and benefit from the attack. If the transmitter is equipped with multiple antennas to perform beamforming during downlink transmission, e.g., maximum ratio transmission (MRT), the main beam of the data signal might be directed to the adversary or other unwanted destinations. This attack is named as pilot spoofing attack and obviously it could create terrible consequences. However, due to variable purposes of attacks, the pilot spoofing attack may not be the worst-case attack as the definition of worst-case could be subjective.

5. Proposed System

The main contributions of our work are summarized in four aspects: 1) our proposed scheme needs no drastic modification to current transmission structure. For example, in the LTE-TDD system, the uplink pilot time slot (UpPTS) and downlink pilot time slot (DwPTS) are already implemented; 2) the TWTD could achieve even higher detection probability than that of the ERD. Similar to the ERD, the threshold derived for the TWTD is also not dependent on the instantaneous channel conditions, which suggests such threshold could be used among different time frames; 3) unlike the ERD, our scheme is able to estimate both channels, switch to secure beamforming almost immediately and finally achieve positive secrecy rate within the same time frame; 4) even without any prior information about Eve, our scheme is able to obtain the maximal secrecy rate in some cases, e.g., the adversary utilizes relatively large power.

6. Conclusion

In this paper, we have studied an active eavesdropping problem, i.e., pilot spoofing attack. A two-way training based scheme has been proposed to defend such attack. The scheme first detects the attack by the unbalance of channel estimations at Alice and Bob, and then formats the secure beamforming based on the estimations of legitimate and illegitimate channels. It is shown that the proposed scheme could achieve a high detection probability. Moreover, according to the two way channel estimation, the positive secrecy rate is proven to be achievable. With the further validation of numerical results, our two-way training based scheme has been proven to be able to protect the confidential communication against the pilot spoofing attack. In order to apply the scheme to practical communication systems, some issues need to be considered, such as the design of the proper reference signal patterns and the feedback procedure. These interesting topics may fall in our future studies.

7. References

1.Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357–360, Aug. 2014.

2. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channelbased detection of Sybil attacks in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.

3. X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 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. 24th PIMRC*, Sep. 2013, pp. 13–18.

5. J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang. (2014). "A semiblind two way training method for discriminatory channel estimation in MIMO systems." [Online]. Available: http://arxiv.org/abs/1405.4626v1

6.A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

7. Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

8. L. Xiao *et al.*, "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. GLOBECOM*, 2010, pp. 1–6.

9. Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 793–808, Dec. 2007.

10. T.-Y. Liu, S.-C. Lin, T.-H. Chang, and Y. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. ICC*, Jun. 2012, pp. 4782–4787.