**Secure Transmission against Pilot Spoofing Attack A Two-Way Training-Based Scheme**

**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 beam forming-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.

**EXISTING SYSTEM:**

* In the existing system, the pilot spoofing attack is considered as an active eavesdropping activity launched by an adversary during the reverse channel training phase. By transmitting the same pilot signal as the legitimate user, the pilot spoofing attack is able to degrade the quality of legitimate transmission and, more severely, facilitate eavesdropping. In an effort to detect the pilot spoofing attack and minimize its damages, in the existing system, the system implemented a novel random-training-assisted (RTA) pilot spoofing detection algorithm.
* In particular, the system develops a new training mechanism by adding a random training phase after the conventional pilot training phase. By examining the difference of the estimated legitimate channels during these two phases, the pilot spoofing attack can be detected accurately. If no spoofing attack is detected, the system presents a computationally efficient channel estimation enhancement algorithm to further improve the channel estimation accuracy.
* If the existence of the pilot spoofing attack is identified, a zero-forcing (ZF)-based secure transmission scheme is proposed to protect the confidential information from the active eavesdropper. Extensive simulation results demonstrate that the proposed RTA scheme can achieve efficient pilot spoofing detection, accurate channel estimation, and secure transmission.

**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.

**SYSTEM SPECIFICATION**

**Hardware Requirements:**

* System : Pentium IV 3.5 GHz.
* Hard Disk : 40 GB.
* Monitor : 14’ Colour Monitor.
* Mouse : Optical Mouse.
* Ram : 1 GB.

**Software Requirements:**

* Operating system : Windows XP or Windows 7, Windows 8.
* Coding Language : Java – AWT,Swings,Networking
* Data Base : My Sql
* Documentation : MS Office
* IDE : Eclipse Galileo