Secure Transmission Against Pilot Spoofing Attack: Using Beam – Forming Technique

[1]Uma R
umaharish18@gmail.com
Assistant Professor

[2]Harikrishnan M
harikrish@hotmail.com

[3]Devanandakumar P
devo1243@gmail.com

[4]Jayakumar RM
srmkjay@gmail.com

[2][3][4]UG students
Department of Computer Science and Engineering
T.J.S. Engineering College

Abstract

The pilot spoofing attack is one type of lively eavesdropping activities performed through a malicious user all through the channel education section. through transmitting the identical pilot (schooling) indicators as those of the felony customers, such an assault is able to manage the channel estimation outcome, which might also bring about a larger channel rate for the adversary but a smaller channel price for the legitimate receiver. With the goal of detecting the pilot spoofing assault and minimizing its damages, we design a two-manner education-based scheme. The powerful detector exploits the intrusive element created by the adversary, observed by way of a relaxed beam forming-assisted facts transmission. similarly to the stable detection overall performance, this scheme is likewise able to acquiring the estimations of each legitimate and illegitimate channels, which permits the customers to acquire comfy conversation inside the presence of pilot spoofing attack.

Index Terms – Physical layer security, pilot spoofing attack, active eavesdropping, two-way training method.

1. Introduction

Manuscript received June 3, 2015; revised October 27, 2015 and December 2, 2015; accepted December 19, 2015. Date of publication January 12, 2016; date of current version February 24, 2016. This work was supported by the National Science Foundation of China under Grant 61571100. The associate editor coordinating the review of this manu-script and approving it for publication was Dr. Walid Saad. *(Corresponding author: Ying-Chang Liang.)* 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 [1]. 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 [2].

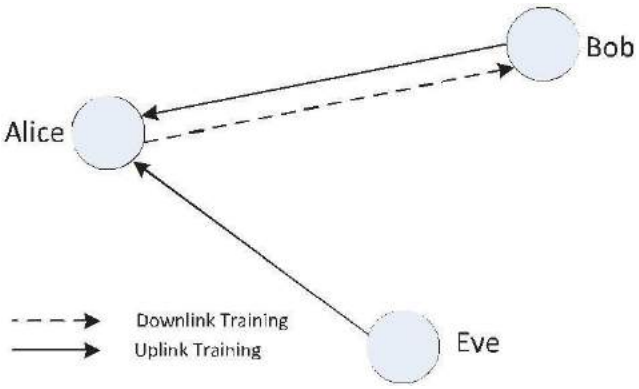


Fig 1: Two-way training based scheme

Motivated by this demand, we propose a two-way training based scheme to achieve the goals of detecting the pilot spoofing attack and securely re-transmitting the data signal. As shown in Fig. 1, the basic process is that the reverse training is still operating as usual to allow the transmitter to estimate the CSI. Before confidential data transmission in the downlink phase, the transmitter first sends the channel estimation results to the receiver, and then conducts the traditional receiver, which allows it to make a test based on the difference between two estimation results. The detection outcome will be fed back to the transmitter together with the downlink channel estimation if needed. The simulation performance shows that our detector, named as two-way training detector (TWTD),.

2. Preliminaries

2.1 Problem Statement

Given a graph G= (V,E) with a vertex set V and an edge set E, we can represent the graph as adjacency matrix A such that $A_{ij} = e_{ij}$ where e_{ij} is the edge weight. $A_{ij}=0$ if there is no edge. The goal of super imposed community detection problem is to find the super imposed clusters whose union is equal to the entire vertex set V.

2.2 Measures of cluster quality

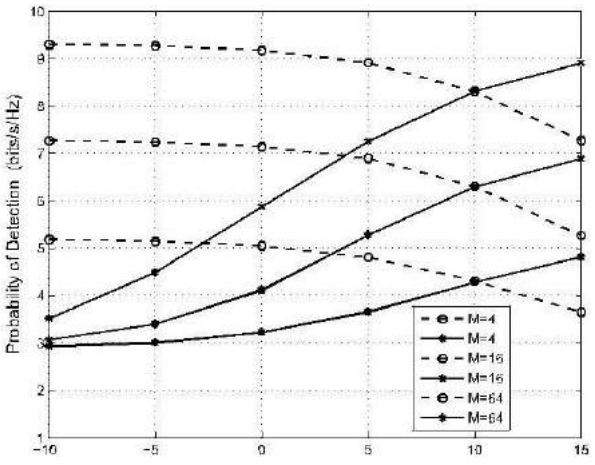
There are some popular measures for the quality of clusters. Let us define ***links (C_p,C_q)*** to be the sum of edge weights between the vertex sets C_p and C_q.

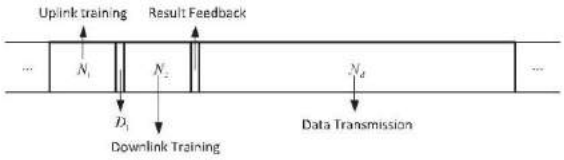
$$\hat{\mathbf{h}}_B = \mathbf{Y}_a \mathbf{A} = \overline{P_B}\mathbf{h}_B \mathbf{x}_{up}\mathbf{A} + \overline{P_{E\_1}}\mathbf{h}_E \mathbf{x}_{up}\mathbf{A} + \mathbf{U}\mathbf{A},$$

$$\mathbf{A} = \sqrt{\frac{\mathbf{x}_{up}^H}{P_B \sigma^2}} \frac{1}{P_B \beta_B} + \frac{\mathbf{x}_{up}\mathbf{x}_{up}^H}{},$$

$$\sigma_{\varepsilon u}^2 = \sigma^2 + \frac{P_B \beta_B^2 \sigma^2}{P_B \beta_B N_1}$$

$$SNR_E = \frac{\left| \mathbf{h}_B^H \mathbf{w} \right|^2}{P_{A\_} \mathbf{h}_E^H \mathbf{w}_{\_}^2},$$





3. Literature Review

The problems of cryptography and secrecy systems furnish an interesting application of communication theory. In this paper a theory of secrecy systems is developed . The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography. There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems. A Gaussian multiple-input single-output (MISO) fading channel is considered. We assume that the transmitter, in addition to the statistics of all channel gains, is aware instantaneously of a noisy version of the channel
to the legitimate receiver. On the other hand, the legitimate receiver is aware instantaneously of its channel to the transmitter, where as the eavesdropper instantaneously knows all channel gains. We evaluate an achievable rate using a Gaussian input without indexing an auxiliary random variable. A sufficient condition for beam forming to be optimal is provided.

4. Existing System

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information called plaintext.

5. Proposed System

Beam forming or spatial filtering is a signal processing technique used in sensor arrays for directional signal transmission or reception. The development of multi-input-multi output (MIMO) techniques (e.g.,beam forming) provides a great opportunity to achieve a positive secrecy rate even when the legitimate channel is worse than the illegitimate one..

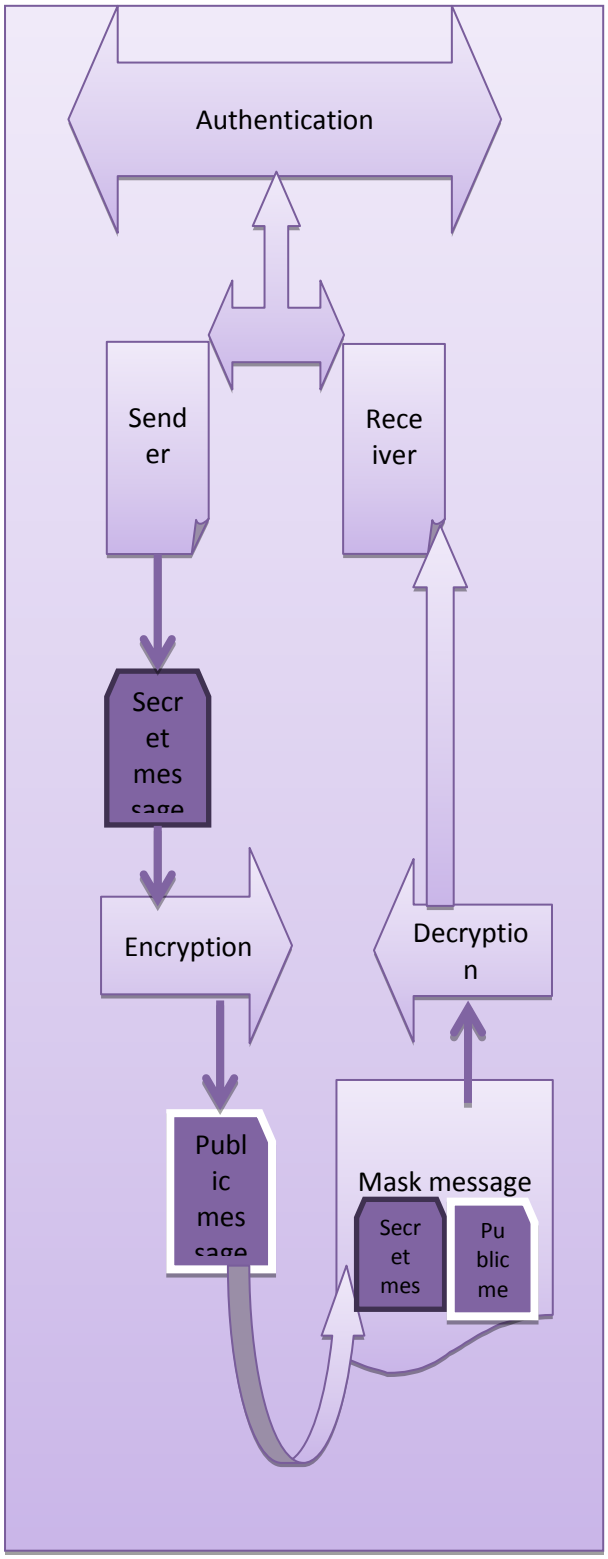
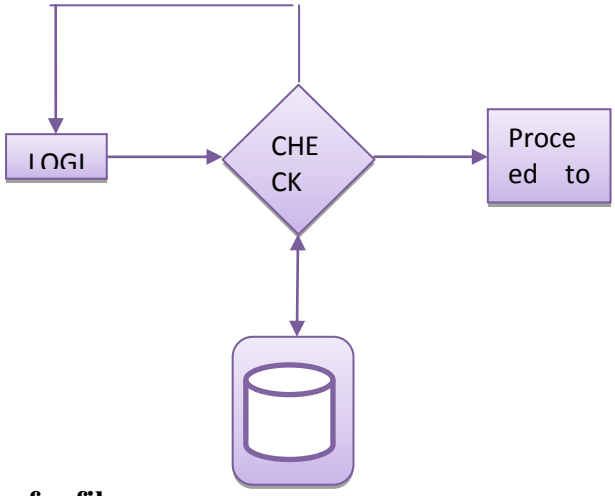


Fig 5: System Architecture

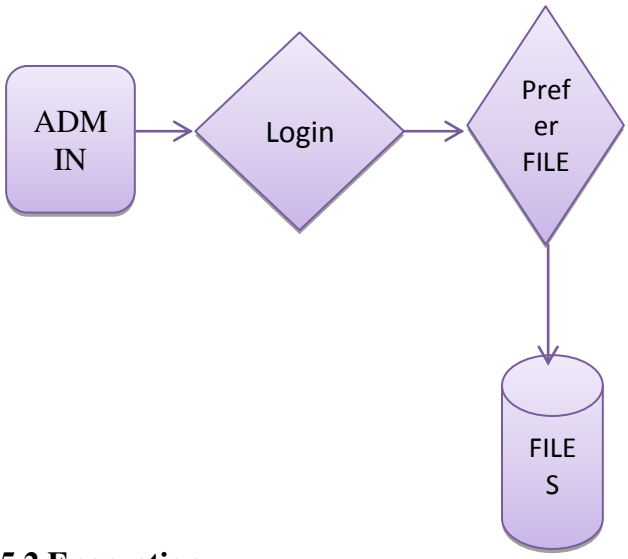
5.1. Authentication

The user need to enter exact username and password which is given to the Admin, if login success means it will take up to main page else it will remain in the login page itself.



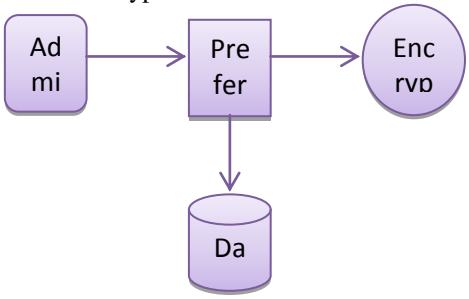
Prefer file

Admin will select the Resource Manager from the list of Resource Managers .Also will choose the files from the list of files stored in the system.



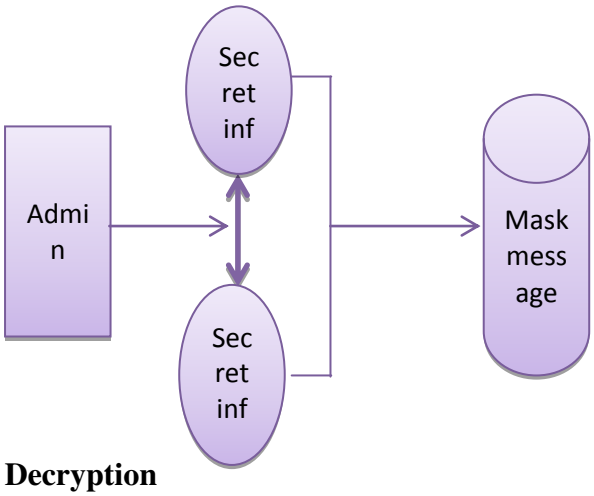
5.2 Encryption

Admin after registration and login would prefer a file from the database. The preferred file would be encrypted, so that the attackers are not able to attack the file. The encrypted file would become unstructured.



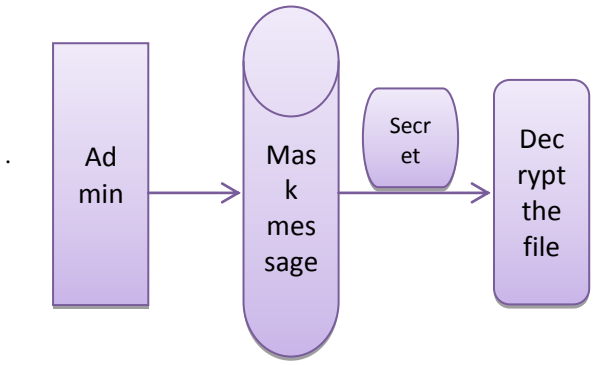
5.3 Public information

Admin after choosing and encrypting the file would generate some public information and combine with encrypted secret information. The combined information would be send to the destination.



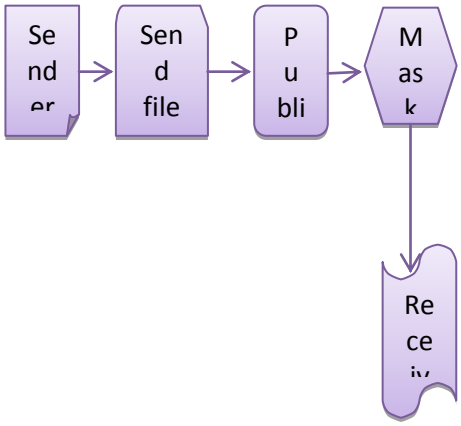
Decryption

Receiver would collect the secret information from the mask message .receiver will decrypt the received encrypted message by using the decryption key.



6 Future enhancements

In future we would use Revacator.Revactor is an application framework for which monitors the Actor's work. These simplify the creation of high-performance network services.



7. 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 beam forming 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.

8. References

[1] 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.

[2] 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.

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

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

[5] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentica-tion using inherent properties of channel impulse response," in *Proc. MILCOM*, Nov. 2011, pp. 538–542.

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

[7] D. J. Tylavsky and G. R. L. Sohie, "Generalization of the matrix inversion lemma," *Proc. IEEE*, vol. 74, no. 7, pp. 1050–1052.

[8] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214.