ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

Detection and Localization of Pilot Spoofing Attacks in Wireless Communication Systems

T C Deepthi[1], Jenelin S S[2]

Assistant Professor, Dept. of ECE, Sivaji College of Engineering and Technology, Manivila, Tamilnadu, India [1]

PG Student, Dept. of ECE, Sivaji College of Engineering and Technology, Manivila, Tamilnadu, India[2]

ABSTRACT: The Pilot spoofing attack is a kind of eavesdropping conducted by malicious users while transmission takes place between a legitimate transmitter and a legitimate receiver. Here the eavesdropper spoofs the legitimate transmitter on the estimation of Channel State Information (CSI) by sending the identical pilot signal as the legitimate receiver, in order to obtain larger information rate in the data transmission phase. The pilot spoofing attack would reduce the strength of the received signal at the legitimate receiver when the eavesdropper utilizes large enough power.So, an Energy Ratio Detector(ERD) is proposed to help the legitimate users to detect and locate such attacks. This Energy Ratio Detector detects the existence of pilot spoofing attack by exploring the asymmetry of received signal power levels at the legitimate transmitter and thelegitimate receiver when there exists a pilot spoofing attack. Also this detector does not require to change the design of current pilot signal and redesign the process of current channel estimation process. The proposed ERD could protect the legitimate users from the pilot spoofing attack efficiently.

KEYWORDS: Pilot spoofing attack, eavesdropping, legitimate receiver, energy ratio detector.

I.INTRODUCTION

Protecting transmissions from being eavesdropped is an important research topic in modern wireless communications. Encryption methods have been used to achieve such protection by implementing secrecy keys in the transmissions. With the advances of computational capability of digital devices, however, the encryption methods face more and more challenges in secrecy key design and management. In recent years, the physical layer security (also known as information theoretical security) has drawn much attention. Furthermore, the development of multiple-antenna technologies helps to provide the achievable rate with perfect secrecy to the legitimate system. For example, beam forming design at the transmitter could either strengthen the signal reception at the legitimate receiver or weaken the signal power received at the eavesdropper resulting in a larger achievable secrecy rate. However, the information theoretical security has great dependence on complex encoding-decoding schemes and accurate channel state information (CSI), which may not be always possible to obtain. Different from passive eavesdropping, another security threat is active attack, including, e.g., identity-based attack (spoofing attack). The original idea of the spoofing attack is that the adversary pretends to be the legitimate transmitter and sends the fake information to the receiver.

In a practical multiple-antenna communication system, a training phase is implemented before the actual data transmission. For example, in a time-division-duplex (TDD) system, the legitimate receiver will send the assigned pilot signal (training signal) to the transmitter through uplink channel. According to the reciprocity of the uplink and downlink channels, the transmitter could estimate the channel based on the received pilot signal. These pilot signals are repeatedly used by the system and are usually publicly known. If the eavesdropper can successfully synchronize its transmission with that of the legal receiver, the transmitter would be spoofed and utilize the estimation of legitimate channel, which is actually the combination of the legitimate channel and illegitimate channel, to design the beam former in the data transmission phase, e.g., maximum-ratio transmission (MRT). Then such a pilot spoofing attack could lead to the information leakage to the active eavesdrop-per and also decrease the legitimate channel rate considerably. By increasing the power of the pilot signal, the eavesdropper could even diminish the legitimate receiver's rate approaching zero. The pilot spoofing attack is noticed rather than other active attacks such as jamming attack, because jamming attack intends to degrade the legitimate transmission instead of eaves dropping the confidential information due to the half-duplex implementation.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

II.SYSTEM MODEL AND ASSUMPTIONS

In the system model three-component system model is considered: one transmitter (Alice), one legitimate receiver (Bob) and one active eavesdropper (Eve). Alice is equipped with antennas and both Bob and Eve are single-antenna users. All the antennas are assumed to be omni-directional and working in half-duplex mode.
The detection method mainly includes two phases: first, the legitimate receiver (Bob) sends the assigned pilot signal to the transmitter (Alice) via uplink channel, and Alice estimates the channel based on the samples of the signal; second, Alice calculates the received signal power, modulates that as a data signal and broadcasts it via downlink channel. Bob demodulates the data and calculates the power of his received signal. Bob then decides whether the system is under pilot spoofing attack or not by comparing the two power levels. Note that Alice utilizes the same power to broadcast the data as that of Bob used for sending the pilot signal.

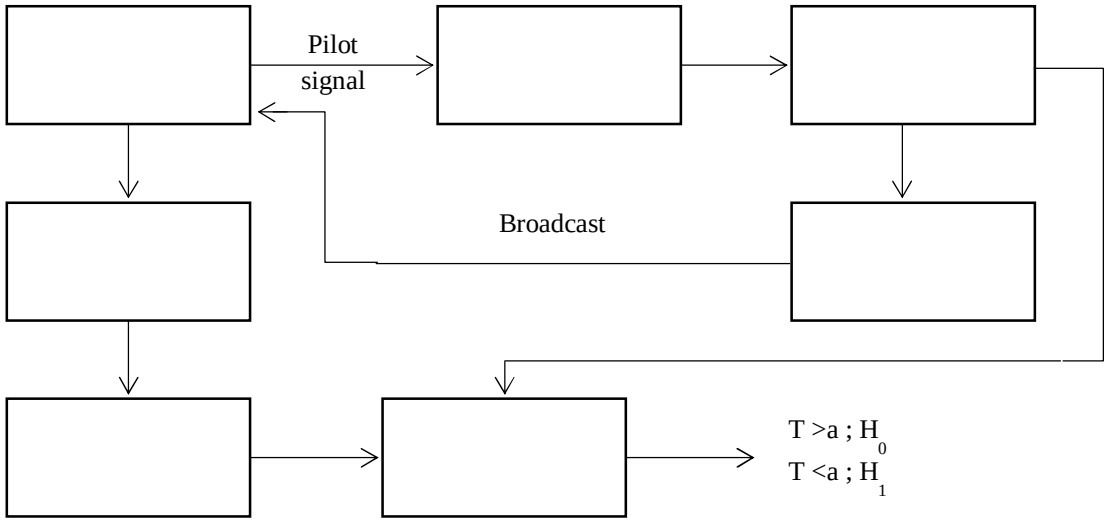

Figure 3.1 Schematic representation of proposed system

The main contributions of this method are summarized as follows:Unlike the other methods the ERD does not require drastic changes on either the design of pilot signals or the channel estimation phase structure. .Large power utilization by Eve could increase the gain to the eavesdropper but also considerably increase the risk of Eve being detected by the legitimate system. Therefore, the trade-off brought by the power consumption of Eve is studied. The result shows that ERD could efficiently reduce the ergodic information leakage, which is the largest information rate that Eve could possibly obtain by choosing the optimal power budget, to a trivial level.

III.ENERGY RATIO DETECTOR

The pilot spoofing attack could cause certain decrease a SNR at Bob. This phenomenon motivates the idea of exploring the power difference between Alice and Bob to detect the existence of pilot spoofing attack.Firstly, define two events, H0 and H1, i.e., H0: there exists no active eavesdropper who conducts the pilot spoofing attack; and H1: the active eavesdropper conducts the pilot spoofing attack trying to steal the information from the transmitter. In the uplink phase of a given time slot, Bob transmits the assigned pilot signal to Alice and the smart eavesdropper broadcasts the same pilot signal to spoof Alice as well.
Then the received signal at Alice is given as follows

$$H_0 : y(n) = \sqrt{P_B h_B} x_p(n) + u(n),$$
$$H_1 : y(n) = \left(\sqrt{P_B h_B} + \sqrt{P_E h_E}\right) x_p(n) + u(n) \quad (3.1)$$

Based on y(n), the channel estimation result is derived as

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

$$H_0 : \widehat{h_B} = \sqrt{P_B h_B} + \tilde{e},$$
$$H_1 : \widehat{h_B} = \sqrt{P_B h_B} + \sqrt{P_E h_E} + \tilde{e} \quad (3.2)$$

Alice then applies the maximum-ratio combining (MRC) to process the received signal, which yields

$$H_0 : y_a(n) = \frac{\hat{h}_B^H}{\|\hat{h}_B\|}[\sqrt{P_B h_B} x_p(n) + u(n)],$$
$$H_1 : y_a(n) = \frac{\hat{h}_B^H}{\|\hat{h}_B\|}[\left(\sqrt{P_B h_B} + \sqrt{P_E h_E}\right) x_p(n) + u(n)], \quad (3.3)$$

Based on $y_a(n)$, we can obtain the average power of received signal in the uplink phase at Alice, which is denoted as Q1

$$Q_1 = \frac{1}{N_1} \sum_{n=1}^{N_1} |y_a(n)|^2 \quad (3.4)$$

We apply the MRT to the downlink transmission and the received signal at Bob is

$$y_b(n) = \frac{h_B^H \hat{h}_B}{\|\hat{h}_B\|} \sqrt{P_A} x_q(n) + v(n), \quad (3.5)$$

Then we derive the average energy of the received signal at Bob as

$$Q_2 = \frac{1}{N_2} \sum_{n=1}^{N_2} |y_b(n)|^2 \quad (3.6)$$

According to this observation, we design the detecting mechanism at Bob and let Bob explore the difference between Q1 andQ2 by setting the test statistic as T=Q2/Q1.

IV.PERFORMANCE ANALYSIS

The possibility that the eavesdropper might be aware of theQ1transmission and send the jamming signal to Bob to interfere the reception of Q1.Topreventsuch jamming attack, one possible countermeasure is that Alice transmits a variable length of non-confidential message to Bob beforeQ1 data and the confidential message are transmitted. By doing so, Eve then cannot determine the position ofQ1 data transmission so it cannot conduct the jamming attack specifically to Q1 without jeopardizing the possible reception of the confidential information. Otherwise, Eve will become a pure jammer which is against its objective to conduct the pilot spoofing attack, which is to eavesdrop the confidential information between Alice and Bob. Indeed, further study on how to detect a super intelligent eavesdropper who could conduct both the pilot spoofing attack and the jamming attack is an interesting topic for future research direction. Apply the MRT to the downlink transmission and the received signal at Bob is

$$y_b(n) = \frac{h_B^H \hat{h}_B}{\|\hat{h}_B\|} \sqrt{P_A} x_q(n) + v(n), \quad (3.7)$$

where n=1,..., N2 and N2 is the number of received signal samples at Bob. v(n)is white complex Gaussian noise. Based on the CLT, if N2 is sufficiently large, Q2 can be approximated by a Gaussian distribution with meanμ2and variance σ^2_2.

$$\mu_2 = \left|\frac{h_B^H \hat{h}_B}{\|\hat{h}_B\|}\right| P_a + \sigma^2$$
$$\sigma_2^2 = \frac{1}{N_2} \mu_2^2 \quad (3.8)$$

Clearly, the performance of the ERD is relying on the channel realizations. In some special occasion, e.g., $h_E = \alpha h_E$ ($\alpha \geq 0$), it is difficult for the ERD to detect the existence of the pilot spoofing attack. However, given the condition that two channels are independent, the possibility of the two channels are in the same direction is quite low. When the eavesdropper spends only small power in sending the pilot signal, it is observed that the ERD also face more difficulty to successfully detect the attack. However, if P_E becomes small, the impact of the pilot spoofing attack will be much weaker as well.The actual probability of false alarm $P_{fa}$is tested when the theoretical value is utilized. The actual P_{fa} levels are all smaller than the required values, which satisfies the demand of the system.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

N1,N2	1000	1000	100	100
Required P_{fa}	0.10	0.01	0.10	0.01
Actual P_{fa}	0.0999	0.0096	0.0988	0.0087

Table 3.1 Comparison of required P_{fa} and actual P_{fa}

V. RESULT AND DISCUSSION

The system model is initiated by choosing the number of test antennas and number of nodes to be tested. Here the three component model (Alice, Bob and Eve model) is generated in which Alice is equipped with multiple antennas and Bob as well as Eve is equipped with a single antenna. The above simulation result shows that there are about nine nodes along with the legitimate and illegitimate nodes.

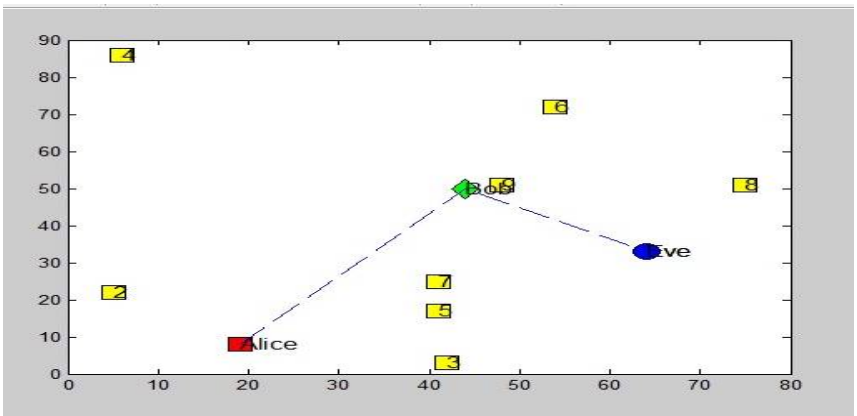

Figure 5.1 System Model

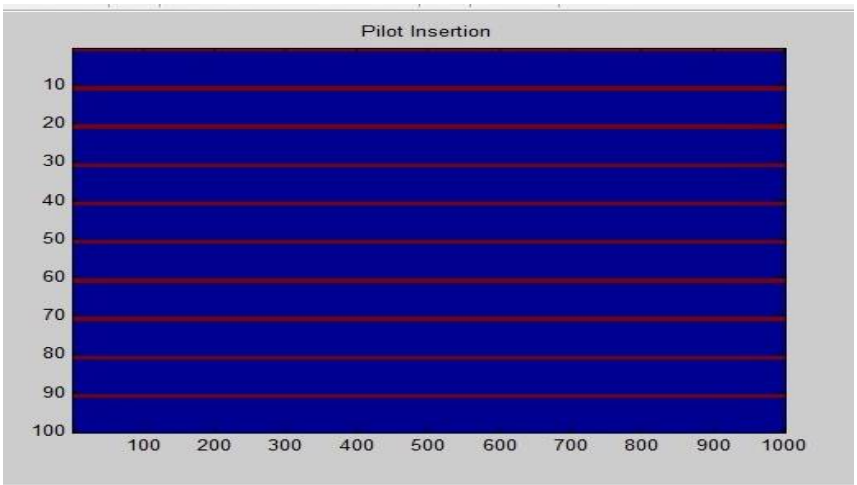

Figure 5.2 Pilot Insertion

At the receiver, the pilot signal is removed, it is demodulated and received. Alice will receive this signal. At the same time it is noted that Alice not only receives the signal from Bob. It will receive signal from other nodes including

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

illegitimate users. Now Alice will estimate the channel SNR and power. The histogram of the power of all the signals received by Alice is shown in Figure 5.2.

Alice then generate a data with some predefined specifications, insert the pilot signal and then broadcast it via uplink transmission. Alice utilize the same power as that of Bob to broadcast the signal.

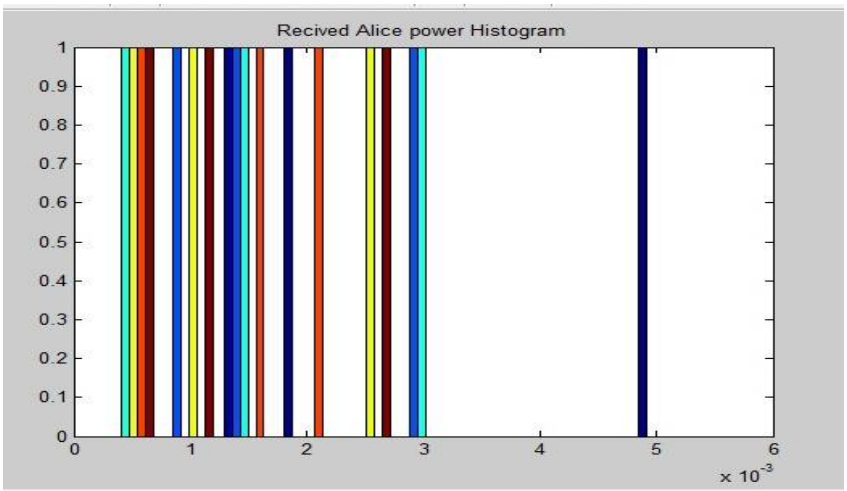

Figure 5.3 Alice's received power histogram

Bob receives the signal from and it is noted that Bob not only receives signal from Alice but also from other users. So the histogram of power of all the received signal by Bob is shown

Now, the power ratio is taken and it is compared with the threshold value. Here the threshold value is assumed to be 5 and if the ratio is graeter than the threshold then it is concluded that there is a spoofing attack else there is no spoofing. The Figure 5.4. shows the attacker as well as non-attacker nodes.

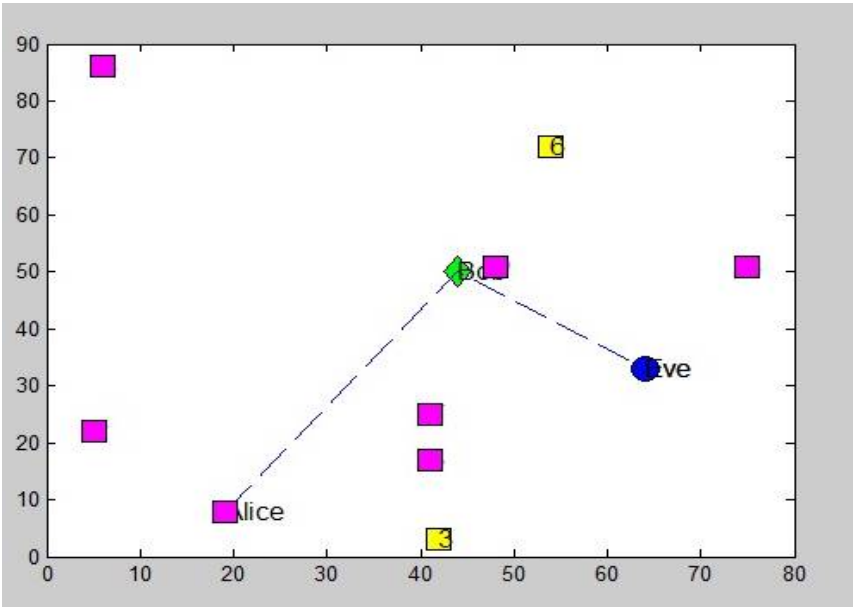

Figure 5.4 Detection of Spoofing attacks

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

The detection performance of proposed ERD is shown under different requirements of P_{fa} and different power budget at Eve.Inorder to make the ergodic secrecy rate to zero,the eavesdropper needs to spend atleast equal power as that of BobBased on probability of false alarm, the large power at Eve leads to higher probability of detection and it is shown in Figure 5.5.

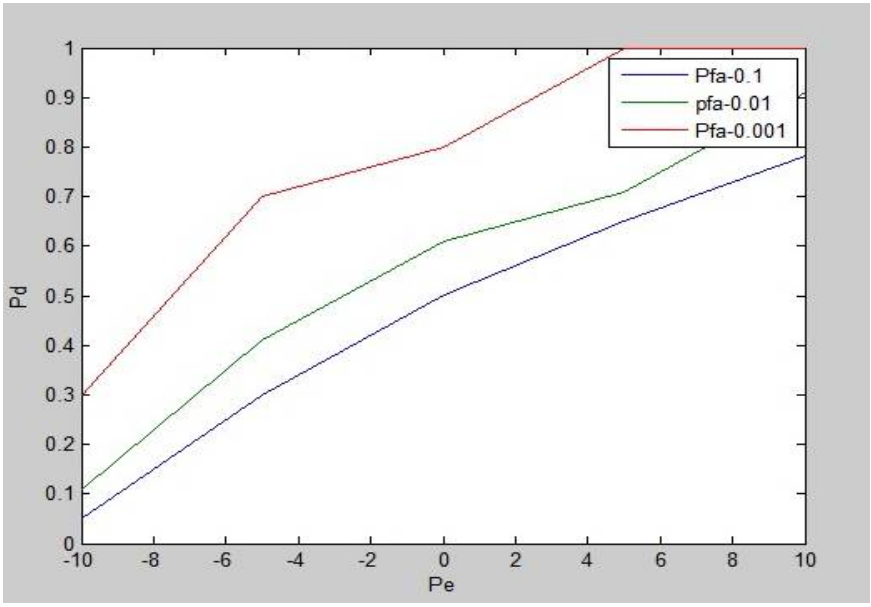

Figure 5.5. Probability of detection Vs different Probability of false alarm

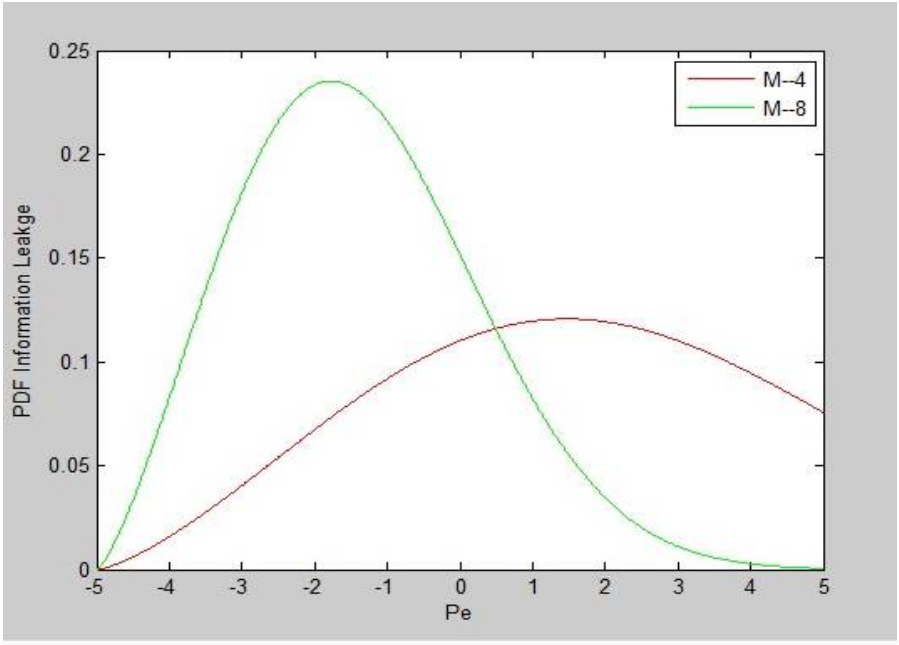

Figure 5.6.Ergodic information leakage Vs different power at Eve

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 5, Special Issue 2, March 2016*

National Conference on Future Technologies in Power, Control and Communication Systems (NFTPCOS-16)

on 10, 11 and 12th March 2016

Organised by

Dept. of EEE, College of Engineering Perumon, Kollam, Kerala – 691601, India

The ergodic information leakage to Eve is given under different power budget and number of antennas from the above figure it is concluded that, as the number of antennas at Alice increases the information leakage will be more.

VI.CONCLUSION

In this paper, an active eavesdropping problem, i.e., pilot spoofing attack is studied. The smart eavesdropper sent the identical pilot signal as that of the legitimate receiver to spoof the transmitter, which gained higher data rates in return. Since this attack could cause a lot of damages, the energy ratio detector is proposed to help the legitimate users to detect and locate such attacks. The ERD is working based on exploring the asymmetry of received signals power levels at Alice and Eve if there exists the pilot spoofing attack. This detector does not require changing the design of current pilot signal and drastically redesign the process of current channel estimation process. Finally, numerical results validated the accuracy of theoretical analysis on the ERD and also proved that the ERD could protect the legitimate users from the pilot spoofing attack efficiently.

REFERENCES

[1].Csiszár I. and Körner J. (1978), 'Broadcast channels with confidential messages', IEEE Trans. Inf. Theory, Vol. 24, No. 3, pp. 339–348.
[2].Garnaev A. and Trappe W. (2013) , 'The eavesdropping and jammingdilemma in multi-channel communications', in Proc. ICC, pp. 2160–2164.
[3]. Goel S. and Negi R.(2008), 'Guaranteeing secrecy using artificial noise',IEEE Trans. Wireless Commun., Vol. 7, No. 6, pp. 2180–2189.
[4]. Kapetanovi D., Zheng G., Wong K K. and Ottersten B. (2013) , 'Detection of pilot contamination attack using random training and massive MIMO', in Proc. PIMRC, pp. 13–18.
[5].Khisti A. and Wornell G. W. (2010), 'Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel', IEEE Trans. Inf. Theory, Vol. 56, No. 11, pp. 5515–5532.
[6]. Li J. and Petropulu A.P.(2011), 'Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading', IEEE Trans. Inf. Forensics Security, Vol. 6, No. 3, pp. 861–867.
[7]. Li Q. and Trappe W. (2007), 'Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships', IEEE Trans. Inf.Forensics Security, Vol. 2, No. 4, pp. 793–808.