OPTIMAL ACTIVE EAVESDROPPING USING PSO

Arya Thampi*

Franklin George Jobin

Abstract- Eavesdropping is the act of secretly listening to the private conversation of others without their consent .In this paper explains how we can identify an active eavesdropper in the communication channel and how to drop it. We derive a new security attack from the pilot contamination phenomenon using PSO. Among the variety of threats and risks that wireless LANs are facing, session hijacking attacks are common and serious ones. Current techniques for detecting session hijacking attacks are mainly based on spoofable and predictable parameters such as sequence numbers, which can be guessed by the attackers. To enhance the reliability of intrusion detection systems, mechanisms that utilize the unspoofable PHY layer characteristics are needed. 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. A PSO based optimal filter is then designed for the purpose of detection. It's the fastest and high accuracy optimization technique. We show that using a Wavelet Transform (WT), the colored noise with complex Power Spectral Density (PSD) in our case can be approximately whitened. Since a larger Signal to Noise Ratio (SNR) increases the detection rate and decreases the false alarm rate, the SNR is maximized by analyzing the signal at specific frequency ranges. The detection mechanism is validated using both simulation results.

Keywords –BPSK Modulation,wavelet transform,CSI,PSO,Eavesdropping

* Department of Electronics and Communication Engineering, Lord Jegannath College Of Engineering, Ramanathichanputhur, Tamilnadu, India

1. INTRODUCTION

Recently, a significant effort has been made on physical layer security to prevent message eavesdropping by a malicious user. Many studies have taken an information-theoretic approach to compute the achievable rate with perfect secrecy. While various secure transmission schemes are under rapid development, increasingly powerful adversaries also bring in new security attacks. One important example is an active eavesdropper, which acts as either (both) a jammer or (and) a classical eavesdropper in a half-duplex (full-duplex) mode. The decision between jamming and eavesdropping for a half-duplex eavesdropper was studied. A quasi full-duplex case was considered where a multi-antenna eavesdropper partitioned its antenna array into eavesdropping and jamming sub-arrays. In this work, we look for new designs of an active eavesdropper from a practical viewpoint.

Among the variety of threats and risks that wireless LANs are facing, session hijacking attacks are common and serious ones. Current techniques for detecting session hijacking attacks are mainly based on spoofable and predictable parameters such as sequence numbers, which can be guessed by the attackers. To enhance the reliability of intrusion detection systems, mechanisms that utilize the unspoofable PHY layer characteristics are needed. 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. In this work, we show that this undesirable phenomenon can indeed be utilized by an active eavesdropper to improve its eavesdropping performance. A PSO based optimal filter is then designed for the purpose of detection. We show that using a Wavelet Transform (WT), the colored noise with complex Power Spectral Density (PSD) in our case can be approximately whitened. Since a larger Signal to Noise Ratio (SNR) increases the detection rate and decreases the false alarm rate, the SNR is maximized by analyzing the signal at specific frequency ranges. The detection mechanism is validated using both simulation results. For optimization we are choose particle swarm optimization, it’s the fastest and high accuracy optimization technique.

II. PROPOSED ALGORITHM

A.PSO Based Optimal Filter

In this case, Eve performs the pilot contamination attack during the reverse training phase and acts as a receiver during the data transmission phase. This is the special case of P_{Ed} =0or φ =1in previous subsections. To achieve a target minimum value of SNR $_E$ given by ρ, the minimum required pilot contamination power is found as

$$p_{Ep,min} = \frac{\rho\left(P_{B\beta_{BA}} + \sigma_A^2\right)(P_A\beta_{AE}\sigma^2_{W+\sigma_E^2})}{2P_{A\beta_{AE}}\beta_{EA}N_{A-\rho\beta_{EA\sigma_E^2}}}$$

The basic PSO algorithm can be described as follows: Each particle in the swarm represents a possible solution to the optimization problem existing. During PSO iteration, every particle accelerates independently in the direction of its own personal best solution found so far, as well as the direction of the global best solution discovered so far by any other particle. Therefore, if a particle finds a promising new solution, all other particles will move closer to it, exploring the solution space more thoroughly.

PSO is flexible, robust .Each i^{th} particle is described by the position vector $S_i = (S_{i1}, S_{i2}, \ldots\ldots, S_{iD})^T$ and the velocity as $V_I = (v_{i1}, v_{i2}, \ldots\ldots, v_{iD})^T$.The vectors of maximum and minimum velocities are V_{max}, V_{min} respectively.
$V_{max} = (v_{\max 1}, v_{\max 2}, \ldots., v_{\max D})^T$ and
$v_{min} = (v_{\min 1}, v_{\min 2}, \ldots., v_{\min D})^T$.The positive constants C_1, C_2 are related with accelerations and $rand_1, rand_2$ lie in the range [0, 1].

The training sequence is fixed and repeatedly used over time, it can be easily obtained by Eve. This creates an opportunity for an active eavesdropper to make a controlled impact on the channel estimation at Alice. Specifically, Eve transmits the pilots at the same time as Bob transmits during the reverse training phase. This makes Alice's estimate of her outgoing channel to Bob also align with her outgoing channel to Eve. The impact of the pilot contamination attack is twofold: it reduces the accuracy of Alice's estimate of her outgoing channel to Bob; and more importantly it helps the data detection at Eve by infecting the beam forming design at Alice. In order to synchronize with Bob, Eve needs to estimate the propagation delays between all the terminals using their location information and obtain any timing information by utilizing the signal exchange between Alice and Bob during the transmitter-receiver synchronization. From the viewpoint of the active eavesdropper design, it is desirable to optimally allocate the available energy budget in attacking the legitimate user's communication, so that the eavesdropper can enjoy a satisfactory detection performance while the legitimate receiver's detection is severely degraded. We assume that Eve has a total energy budget for each transmission block, given by $\varepsilon_{E,}$ which is allocated among pilot contamination (during the reverse training phase) and jamming (during the data transmission phase). In other words, we have $P_{EP} + P_{Ed}(L-1) = \varepsilon_E$

Note that the constraint of $SNR_E \geq \rho$ may not be satisfied if ρ is too large. The maximum feasible value of SNR_E is reached by setting φ =1, which should not be smaller than ρ. Hence, solving $SNR_E = \rho$ with φ =1gives the maximum feasible value of ρ as

$$\rho_{MAX} \quad = \frac{2P_A\beta_{AE}\beta_{EA}N_A\varepsilon_E}{(P_B\beta_{BA} + \sigma_A^2)(P_A\beta_{AE}\sigma_w^2 + \sigma_E^2) + \beta_{EA}\sigma_E^2\varepsilon_E}$$

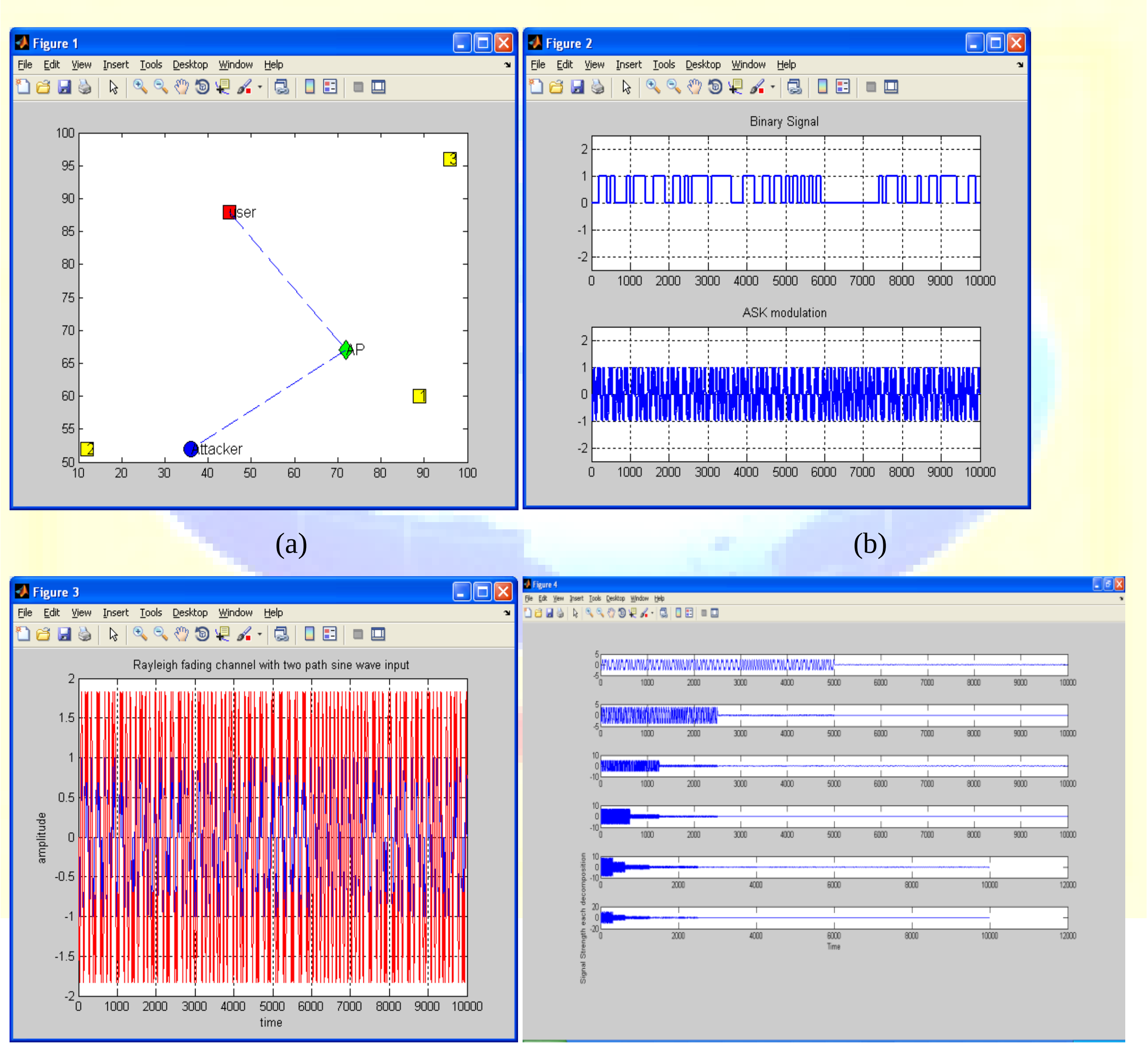
B.Extraction Algorithm-

In the exisisting system CSI based optimal filter is used for the purpose of detection. it will give the current status of the channel. In wireless communication, channel state information (CSI) refers to known channel properties of a communication link. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for example, scattering, fading, and power decay with distance. The CSI makes it possible to adapt transmissions to current channel conditions, which is crucial for achieving reliable communication with high data rates in multiantenna systems.PSO based optimal filter is used for the purpose of detection. It is highly accurate and fastest technique compared with CSI.By using the PSO optimum threshold value is to be find out. ie is, If Threshold value > 1 , it shows the presence of Hijackers. If Threshold value <1, it indicate the presence of noise. Thus we can identify the eavesdropper and drop that particular channel and continue the safe communication.

III. Experiment and Result

Now, we present numerical results to illustrate the benefits obtained by Eve from the pilot contamination attack. The average post-processing SNRs at Bob and Eve, i.e., SNR_B and SNR_E during data transmission. The full-duplex mode is considered in which Eve uses different power levels for pilot contamination and jamming. The primary goal of Eve is to meet a minimum SNR_E of 10 dB. Results are shown for Eve's average power budget ε_E /L ranging from 5 dB to 15 dB.We see that Eve is able to simultaneously achieve the required SNR for herself and make

Bob suffer from a relatively low SNR. The values of SNR $_B$ and SNR $_E$ strongly depend on the energy allocation parameter φ. We include the SNR results for the case of minimum pilot contamination energy allocation, i.e ., φ_{min}, and the case of optimal energy allocation, i.e ., φ∗ that the optimal energy allocation not only reduces SNR $_B$ but also achieves a better SNR_E compared to the case of using minimum energy for pilot contamination.

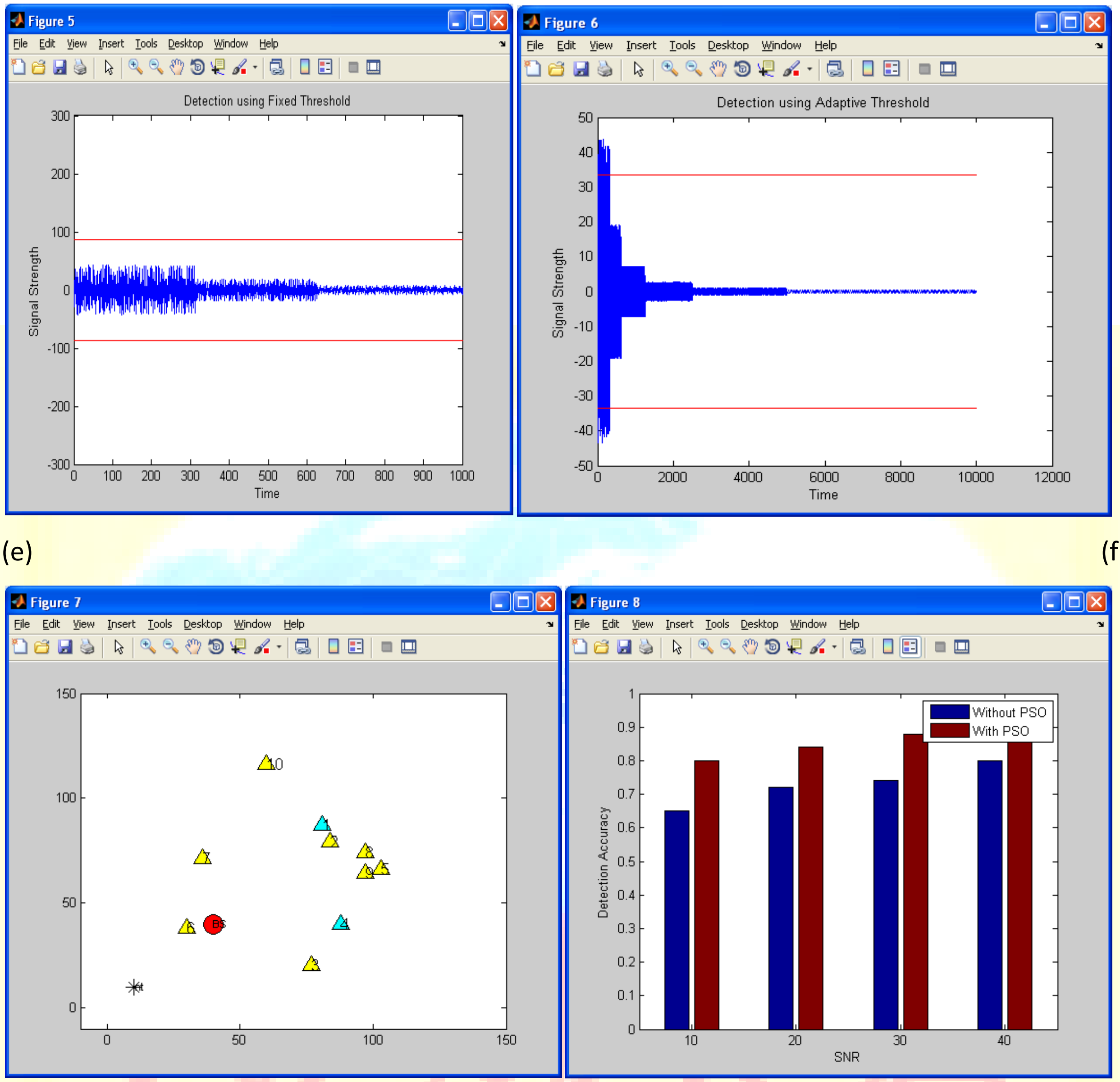


(a)

(b)

(c)

(d)



(e) (f)

(g) (h)

FIG 1. (A) DEMO FOR TRANSMITTING DATA, (B) BPSK MODULATION,(C) RAYLEIGH FAIDING,(D) ANALYSIS OF SIGNAL ,(E) FIXED THRESHOLD MEASUREMENT ,(F) OPTIMUM THRESHOLD MEASUREMENT ,(G) DEMO FOR EAVESDROP DETECTION AND DROPPING,(H) COMPARISON

IV.CONCLUSION

In this work, we showed the detrimental effect of the pilot contamination attack on the secrecy performance. It is therefore important for the legitimate user to detect such an attack and design countermeasures. The detection of the pilot contamination attack may be achieved by transmitting a sufficiently long pilot sequence in the reverse training phase and analyzing the variance of the received signal at Alice after normalizing it by the pilot sequence. If the variance is close to that of the receiver noise, it indicates that the pilot contamination attack may have been used by Eve. In order to make this attack ineffective, blind channel estimation can be used by Alice based on the data transmission from Bob, assuming two-way communications.

V. REFERENCE

[1] Z. Li, W. Trappe, and R. Yates, "Secret communication via multiantenna transmission," in *Proc. 2007 Conf. on Inform. Sciences and Syst.*, pp. 905–910.

[2] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificialnoise- aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[3] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast fading channels: a block-Markov Wyner secrecy encoding scheme," submitted to *IEEE Trans. Inf. Theory*. Available: http://arxiv.org/abs/1002.1313.

[4] ——, "A full-duplex active eavesdropper in MIMO wiretap channels: construction and countermeasures," in *Proc. 2011 Asilomar Conf. on Signals, Syst., and Computers*.

[5] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Tech.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[6] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2640–2651, Aug. 2011.