Wavelet Based Detection of Session Hijacking Attacks in Wireless Networks

Xiaobo Long and Biplab Sikdar
Electrical, Computer and System Engineering
Rensselaer Polytechnic Institute, 110 8th Street, Troy NY 12180

Abstract— **This paper develops a mechanism for detecting session hijacking attacks in wireless networks. The proposed scheme is based on detecting abrupt changes in the strength of the received signal. We first develop a mathematical model to describe the signal strength during a session hijacking: a step function signal, which represents the abrupt jump in the signal strength, imbedded in colored noise, which is caused by fading wireless channels. An optimal filter is 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 larger Signal to Noise Ratio (SNR) increases the detection rate and decreases the false alarm rate, we maximize the SNR by analyzing the signal at specific ranges of frequency. We validate the detection mechanism by simulation and experimental results.**

I. Introduction

Among various risks wireless LANs are facing, session hijacking attacks are common and serious ones. In a session hijacking attack, an attacker forces a normal user to terminate its connection to an AP by first masquerading the AP's MAC address. The attacker then associates with the AP by masquerading the user's MAC and takes over its session. 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 also. To enhance the confidence of intrusion detection systems, mechanisms that utilize the unspoofable PHY layer characteristics are needed.

The authors of [1] propose a session hijacking attack detection mechanism by periodically monitoring the received signal strength values for a particular MAC address at a monitor. If an attacker B spoofs the MAC address of a normal user A the monitor will observe a sudden change in signal strength profile of A's MAC address and raise an alarm. In [1], any abrupt change in the nodes' signal strength dynamic profile can possibly be flagged as suspicious activity. However, the received signal strength suffers from multipath fading and shadow fading also, both of which may lead to abrupt changes in both "normal" or "abnormal" network conditions. Multipath fading can cause abrupt deep power loss in the received signal strength even when the wireless user is stationary. Shadow fading can cause at least 6db power loss for 10% of time when the user suddenly enters a shadow region [2]. How to robustly detect the abrupt changes in fading signal strength traces caused by session hijacking requires further investigation.

In our work we first develop a mathematical model of the signal strength time series under the hypothesis that there exists a session hijacking attack. The abrupt change in the signal strength caused by session hijacking is considered as "signal" and the sum of multipath fading, shadow fading plus path loss components is regarded as "noise". Since the "noise" is not white noise but has a complex Power Spectral Density (PSD), the design and implementation of optimal matched filter in traditional Fourier frequency domain is challenging. We show that Wavelet Transform (WT) efficiently solves the problem by presenting the signal at different time and frequency (scale) resolutions. Working in the wavelet domain, the optimal matched filter is designed by maximizing the SNR at certain frequency ranges.

The rest of paper is organized as follows: Section II presents the related work. Section III describes the proposed methodology. Section IV validates the method through experiments and simulations. Section V gives the concluding remarks.

II. Related Work

Multi-resolution wavelet signal analysis is an efficient tool for detection of change-points. A change point detection method is proposed in [3] based on the cumulative sum of squared wavelet coefficients. Authors in [4] combine wavelet based methods and extreme value theory to test the presence of an arbitrary number of discontinuities in an unknown function observed with noise, by checking the absolute peak value of wavelet coefficients against a threshold. A wavelet based signal processing method to extract a signal obscured by noise in order to detect the pipeline leakages is proposed in [5]. In our work, a thresholding mechanism using wavelet coefficients is also employed. Our work focuses on the design of the optimal wavelet and observation scale.

The authors in [6] propose a Continuous Wavelet Transform (CWT) based method for detection of additive and multiplicative abrupt jumps. With the assumption of white noise, an optimal wavelet is given. In our work, we address the problem of detection of abrupt jumps embedded in additive colored noise, using Discrete Wavelet Transform (DWT) which is computationally efficient to implement.

III. Methodology

A. Mathematical Model

In our work, we use the commonly used ITU recommended channel model [7]. The ratio of the received and transmitted powers, P_r and P_u respectively, in dBm is given by

$$L = \frac{P_r}{P_u}(\text{dBm}) = K + \gamma \log_{10} d + \varphi_{\text{dBm}} + \phi_{\text{dBm}} \qquad (1)$$

where $\gamma \log_{10} d$ models the path loss as a function of the distance d between the transmitter and receiver. Also, γ is the path loss exponent and K is a unitless constant. The attenuation from shadowing, φ_{dBm}, is normally distributed with zero mean and variance σ_φ^2. The values of parameters γ, K, σ_φ^2 depend on the propagation environment. Finally, ϕ_{dBm} represents the variation caused by multipath fading and can be modeled as a Raleigh or Rician distribution with appropriate parameters which depends on the propagation environment as well as the moving speed of the wireless users.

Next we develop a mathematical model for the event of session hijacking. For convenience of analysis, continuous time signal models are used. Although our final detection algorithms are implemented using discrete signal models, the discretization process has no effect on achieving the optimal performance of the detector. We assume that both the wireless user and attacker can be mobile or static. We denote the distance from wireless user and the AP by $d_0(t)$ and the distance from the attacker to the AP by $d_1(t)$. d_0 and d_1 are continuous functions of time t. Unless the attacker has a movement pattern that is symmetrically exact with the movement pattern of the wireless user, $d_1(t) \neq d_0(t)$. Suppose a session hijacking attack occurs at time t_0. Let $d_1(t_0) = d_0(t_0) + \Delta d$. We assume that the user and attacker are in environments with propagation parameters $[K_i, \gamma_i, \varphi_i, \phi_i]$ where $i = 0$ for the user and $i = 1$ for the attacker, respectively. Then the monitored signal strength $x(t)$ is given by

$$\begin{aligned} x(t) &= N(t) + f(t) \\ &= N(t) + \Delta m \cdot u(t - t_0) \end{aligned} \qquad (2)$$

where $f(t)$ represents the signal and $N(t)$ is the noise. $u(t)$ is the unit step located at unknown time instance t_0. The jump amplitude of $f(t)$ at time t_0 is $\Delta m = K_1 - K_0 + \gamma_1 \log_{10} d_1(t_0) - \gamma_0 \log_{10} d_0(t_0)$, and

$$N(t) = \begin{cases} N_1(t), & t < t_0; \\ N_2(t), & t \geq t_0. \end{cases} \qquad (3)$$

where $N_1(t) = K_0 + \gamma_0 \log_{10} d_0(t) + \varphi_0 + \phi_0$ and $N_2(t) = K_0 + \gamma_0 \log_{10} d_0(t_0) + \gamma_1 \log_{10} \frac{d_1(t)}{d_1(t_0)} + \varphi_1 + \phi_1$.

The ITU-R model describes five types of propagation environments [7]: indoor office, outdoor to indoor pedestrian test environments PED_A and PED_B, and vehicular test environments VEH_A and VEH_B. In our work, we don't limit the user and attacker to be in the same environment. For example, the user can be in indoor office and the attacker can walk outside the building. In our work, we assume that carrier frequency $w_c = 2.4 \times 10^9$ Hz that is typically in IEEE 802.11 based WLANs. Velocity of both mobile wireless user and the attacker is less than pedestrian speed $v = 3$ km/hour. The corresponding maximum doppler frequency $w_m = 0.67$ Hz. When both the user or the attacker are static, $v = 0$ and $w_m = 0$. Although only walking speed is assumed in our work, our detection mechanism can be extended to the environments where either the wireless user or the attacker is moving at vehicular speed. For the indoor test environment, 12 dB variance is assumed for fading signal strength in the ITU-R model. For outdoor test environment, the variance is 10 dB. If both the normal user and attacker are indoor, the fading signal strength $N(t)$ have the same statistical distribution before and after the intrusion attack. If one of them is outdoor, the variance of $N(t)$ is smaller, which in turn makes the detection of $f(t)$ easier. In the following analysis, we assume that both the wireless user and the attacker are in indoor environment since it is the worst case for the session hijacking attack to be detected. We then test the detection algorithms in the indoor, PED_A and PED_B environments to validate the mechanism.

B. Matched Filter

Our aim is to develop a robust detection algorithm for the step signal $f(t) = \Delta m \cdot u(t - t_0)$ embedded in noise $N(t)$. The detection consists of determining the jump instance t_0. The hypothesis test is given as follows:

- $\mathcal{H}_0$[null]: $x(t) = N(t)$
- $\mathcal{H}_1$[alternate]: $x(t) = f(t) + N(t)$

where $x(t)$ is our observed signal strength. $\mathcal{H}_0$ corresponds to the "normal" network condition where no session hijacking attack occurs. $\mathcal{H}_1$ corresponds to the "abnormal" network condition when there exists an attack. Note that $f(t)$ is a deterministic signal for a given Δm and t_0, while $N(t)$ is a stochastic signal. For the purpose of detection, we pass $x(t)$ through a Linear Time Invariant (LTI) system $H(w)$. $H(w)$ is chosen to maximize the output SNR at time t_0 under $\mathcal{H}_1$. The output SNR γ_0 is given by,

$$\begin{aligned} \gamma_0 &= \frac{|\frac{1}{2\pi}\int_{-\infty}^{+\infty} F(w)H(w)e^{jwt_0}dw|^2}{\frac{1}{2\pi}\int_{-\infty}^{+\infty} S_N(w)|H(w)|^2 dw} \\ &\leq \frac{\frac{1}{2\pi}\int_{-\infty}^{+\infty} |F(w)|^2 dw \int_{-\infty}^{+\infty} |H(w)|^2 dw}{\frac{1}{2\pi}\int_{-\infty}^{+\infty} S_N(w)|H(w)|^2 dw} \end{aligned} \qquad (4)$$

where $F(w)$ and $H(w)$ are the Fourier transforms of $f(t)$ and LTI system impulse response $h(t)$ respectively. $S_N(w)$ is the PSD function of noise $N(t)$. In the simple case, i.e., if $S_N(w) = \frac{N_0}{2}$ where N_0 is a constant over range of w, Equation (4) can be simplified as,

$$\gamma_0 \leq \frac{\int_{-\infty}^{+\infty} |F(w)|^2 dw}{N_0/2} \qquad (5)$$

and the optimal $h(t)$ that maximizes γ_0 is then the matched filter given by Equation (6), where A is a constant.

$$h_{opt}(t) = Af(t_0 - t) \qquad (6)$$

In our work, $N(t)$ is the sum of multipath fading, shadow fading and path loss, and $S_N(w)$ has much more complex PSD than white noise. We analyze $S_N(w)$ at different frequency ranges in order to simplify γ_0 in Equation (4) and find the optimal $h(t)$. Note that multipath fading causes variation in the received signal strength within the order of one wavelength and is therefore a high frequency component. Shadow fading causes variation in the order of tens of wavelength. Path loss is caused by spatial movements in the order of hundreds of wavelengths and corresponds to the low frequency component. This motivates us to divide the whole frequency domain of $N(t)$ into three frequency subsets as $w = w_1 \cup w_2 \cup w_3$, where w_1, w_2 and w_3 are the frequency ranges of multipath fading component $N_1(t)$, shadow fading component $N_2(t)$ and path loss component $N_3(t)$, respectively. Since $N(t) = N_1(t) + N_2(t) + N_3(t)$ and $N_1(t), N_2(t), N_3(t)$ are mutually independent, $S_N(w) = S_{N_1}(w) + S_{N_2}(w) + S_{N_3}(w)$. We will show later that $S_N(w)$ can be assumed constant for specific ranges of frequency. Then we can claim that $h_{opt}(t)$ given in Equation (6) is the matched filter for the detection of jump step signal $f(t)$, working on a certain frequency range. This motivates us to work in the wavelet domain.

C. Optimal Wavelet

Wavelet transform is an efficient tool for signal detection since it provides a way to represent a signal at different time and frequency (scale) resolutions. A larger scale j corresponds to lower observation frequency. In our strategy, we use the wavelet transform defined as $d_x(j,k) =< x, \psi_{j,k} >$ where $d_x(j,k)$ is the wavelet detail coefficient of $x(t)$ at scale j at time k and can be interpreted as detail of $x(t)$ at the scale j, and $< x_1, x_2 >$ represents the inner product of $x_1(t), x_2(t)$. $\psi_{j,k}(t) = 2^{-\frac{j}{2}}\psi(2^{-j}t - k)$ is the wavelet function transformed from the mother wavelet function $\psi(t)$.

To detect a step function embedded in the noise in our case, the Haar wavelet $\psi(t)$ given in Equation (7) is the matched filter and is therefore the optimal wavelet [6],

$$\psi(t) = \begin{cases} 1, & \text{if } 0 \le t < \frac{1}{2}; \\ -1, & \text{if } \frac{1}{2} \le t < 1; \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Owing to the wavelet transform linearity, the wavelet transform of $x(t) = N(t) + f(t)$ can be expressed by,

$$d_x(j,k) = d_N(j,k) + d_f(j,k) \tag{8}$$

where $d_f(j,k)$ are the wavelet detail coefficients of the step function $f(t) = \Delta m \cdot u(t - t_0)$. Let $I_\psi(t) = \int_{-\infty}^{t} \psi(u)du$. We then have

$$d_f(j,k) = -\Delta m \cdot 2^{\frac{j}{2}} I_\psi(t_0 2^{-j} - k) \tag{9}$$

Note that $d_f(j,k)$ are deterministic. $d_N(j,k)$ are the wavelet coefficients of stochastic process $N(t)$ and are thus stochastic.

The signal to noise ratio SNR at time t_0 observed at scale j in wavelet domain is then given by [6],

$$\begin{aligned} \gamma(j) &= \frac{|d_f(j,k)|^2}{\text{var}(d_N(j,k))} \\ &= \frac{\Delta m^2 2^j |I_\psi(t_0 2^{-j} - k)|^2}{\text{var}(d_N(j,k))} \\ &= \frac{\Delta m^2 2^j |I_\psi(0)|^2}{\text{var}(d_N(j,k))} \end{aligned} \tag{10}$$

where $t_0 = 2^j k$ and var$(\cdot)$ represents the variance of a stochastic signal.

Our aim is to maximize the SNR. We can see from Equation (10) that SNR of our detector is proportional to Δm^2. Note that $\Delta m = K_1 - K_0 + \gamma_1 \log_{10} d_1(t_0) - \gamma_0 \log_{10} d_0(t_0)$. For any given environment, $K_1, K_0, \gamma_1, \gamma_0$ is given. We can conclude that farther the attacker is from the normal user, usually the easier it can be detected. Compared to the SNR in Equation (4) which is for the whole frequency domain, Equation (10) is a function of observation scale j. In our work, we further investigate how to robustly detect $f(t)$, by maximizing the SNR as a function of j. Since the numerator in Equation (10) is proportional to 2^j, this motivates us to work on the high scales, which corresponds to large j, in the time-scale plane. We will show later that the denominator in Equation (10) can be assumed a constant for j large enough.

D. Optimal Scale

In this section, we calculate var$(d_N(j,k))$ and derive it as a function of octave j. Since $N(t_0) = N_1(t_0) + N_2(t_0) + N_3(t_0)$ is the sum of three mutually independent components: multipath fading, shadow fading and path loss, we have the following,

$$\begin{aligned} \text{var}(d_N(j,k)) &= \text{var}(d_{N_1}(j,k)) + \text{var}(d_{N_2}(j,k)) \\ &+ \text{var}(d_{N_3}(j,k)) \end{aligned} \tag{11}$$

where $d_{N_1}(j,k)$, $d_{N_2}(j,k)$, $d_{N_3}(j,k)$ represents the detail coefficients of $N_1(t), N_2(t), N_3(t)$ at scale j, respectively. The wavelet coefficients $d_{N_i}(j,k)$, $i = 1,2,3$ can be assumed to be zero mean stationary process. At a given time t_0 and scale j, var$(d_{N_i}(j,k))$ represents the energy of noise $N_i(t)$ around frequency $2^{-j}w_0$, where w_0 is the maximum frequency of $N(t)$, and is given by,

$$\text{var}(d_{N_i}(j,k)) = \int S_{N_i}(w) 2^j |\Psi(2^j w)|^2 dw \tag{12}$$

where $\Psi(w)$ is the Fourier transform of mother wavelet $\psi(t)$. Scale $j = 1, \cdots, J$ and $S_{N_i}(w)$ is the PSD of N_i at time t_0 for $i = 1,2,3$.

1) Energy of Noise Caused by Multipath Fading: According to the ITU-R model [7], for outdoor environments, the Doppler Spectrum of narrow band multipath fading channels can be modeled as follows, given by Clark and Jake,

$$S_{N_1}(w) = \frac{1}{\pi w_m \sqrt{1 - (\frac{w_c - w}{w_m})^2}} \tag{13}$$

where $w_c - w_m < w < w_c + w_m$, w_c is the carrier frequency of the propagated waveform, and w_m is the maximum doppler frequency shift. The U-shaped PSD $S_{N_1}(w)$ approaches the constant $\frac{1}{\pi w_m}$ where w approaches w_c.

For indoor channels, the Doppler spectrum is nearly flat,

$$S_{N_1}(w) = \frac{1}{\pi w_m} \tag{14}$$

where $w_c - w_m < w < w_c + w_m$. In both cases, we can assume that $S_{N_1}(w) \cong C_1$ for $w \in w_1$. $C_1 = \frac{1}{\pi w_m}$ is a constant and

$w_1 = [w_c - \Delta w, w_c + \Delta w]$, where $0 < \Delta w < w_m$. var$(d_j^{N_1})$ is then given by,

$$\text{var}(d_{N_1}(j,k)) = C_1 \int |2^j \Psi(2^j w)|^2 dw \tag{15}$$

where w is around frequency $2^{-j}w_0$ and w_0 equals the maximum frequency $w_c + w_m$. Since multipath fading belongs to high frequency noise in signal strength $x(t)$, $w \in w_1$ therefore corresponds to small scales in the wavelet domain. var$(d_{N_1}(j,k)) \neq 0$ is valid only for those j where $2^{-j}w_0 \in [w_c - \Delta w, w_c + \Delta w]$. i.e. $\frac{w_c+w_m}{2^j} > w_c - \Delta w > w_c - w_m$. The noise energy caused by multipath fading can be assumed zero for scales $j > \log_2(\frac{w_c+w_m}{w_c-w_m})$. When $w_c = 2.4 \times 10^9$ and $w_m = 0.67$, var$(d_{N_1}(j,k)) \neq 0$ only for $j = 0$ and var$(d_{N_1}(j,k)) \cong 0$ for $j \geq 1$.

2) Energy of Noise Caused by Shadow Fading: Shadow fading $N_2(t)$ can be modeled as a correlated log-normal distributed noise, according to the ITU-R model, with normalized correlation function given by,

$$R(\Delta x) = e^{-\frac{\Delta x}{d_{cor}} ln2} \tag{16}$$

where d_{cor} is the de-correlation length [7]. For both indoor, PED_A and PED_B test environments, $d_{cor} = 5$ meters. The PSD of $N_2(t)$ is then given by,

$$S_{N_2}(w) = \sigma^2 \frac{2\alpha}{\alpha^2 + w^2} \tag{17}$$

where σ^2 is the variation of log-normal shadow fading, and $\alpha = \frac{ln2}{d_{cor}}$. For scale j large enough, w is small enough such that $\alpha \gg w$, and $S_{N_2}(w) \cong \frac{2}{\alpha}$ is approximately a constant function. By solving $2^{-j}w_0 \ll \alpha$, we can obtain that $j \geq 4$. Therefore, for scales $j \geq 4$, var$(d_{N_2}(j,k))$ is given by,

$$\text{var}(d_{N_2}(j,k)) = C_2 \int |2^j \Psi(2^j w)|^2 dw \tag{18}$$

where $C_2 = \frac{2\sigma^2}{\alpha} = \frac{2\sigma^2 d_{cor}}{ln2}$.

3) Energy of Noise Caused by Path Loss: At time t, path loss $N_3(t)$ is determined by the distance from the wireless user to the AP. At time t_0, $N_3(t_0)$ is a deterministic function and $d_{N_3}(j,k)$ is a deterministic process. Therefore, var$(d_{N_3}(j,k)) = 0$ for all j. So far we can rewrite var(d_j^N) as follows,

$$\text{var}(d_N(j,k)) = C_2 \int |2^j \Psi(2^j w)|^2 dw \tag{19}$$

From Equation (4) we have $\gamma(j)$ for $j \geq 4$ given by,

$$\begin{aligned} \gamma(j) &\leq \frac{\frac{1}{2\pi}\int |F(w)|^2 dw \int |2^j \Psi(2^j w)|^2 dw}{\frac{1}{2\pi}\int C_2 |2^j \Psi(2^j w)|^2 dw} \\ &= \frac{\int |F(w)|^2 dw}{C_2} \\ &= \frac{\Delta m^2 2^j |I_\psi(0)|^2 ln2}{2\sigma^2 d_{cor}} \end{aligned} \tag{20}$$

The optimal scale j to maximize $\gamma(j)$ is thus $j \to \infty$. To implement our mechanism, $x(t)$ are sampled into discrete time series $x[n]$, due to the discrete sampling in the signal strength measurements. A sliding window of size M is defined that consists of the last M signal strength measurements, $x = [x_1, \cdots, x_M]$. The scale j is a discrete value and is limited by $0 \leq j \leq J_{MAX}$, where $J_{MAX} = \lfloor \log_2(M) \rfloor$ is the maximum decomposition scale and is determined by the length, M, of the time series. The optimal scale to maximize the SNR is thus $j = J_{MAX} = \lfloor \log_2(M) \rfloor$.

E. Bayesian Hypothesis Test

Our detection problem in wavelet domain can be summarized as follows. Let the observed wavelet detail coefficient y transformed from $x(t)$ at time $k = t_0 2^j$ and scale $j (\geq 4)$ have the form $y = s + n$, where $s = \Delta m 2^{\frac{j}{2}} |I_\psi(0)|$ and $n \sim \eta(0, \Sigma)$, with $\Sigma = C_2$. The noise n has Gaussian distribution because it has approximately constant power lever C_2 when $j \geq 4$. Our aim is to detect signal s from Gaussian noise n. The hypotheses to be tested are:

- $\mathcal{H}_0$[null] : $Y \sim \eta_0(0, \Sigma)$
- $\mathcal{H}_1$[alternative] : $Y \sim \eta_1(s, \Sigma)$

We assume that there exists an a priori probability associated with the hypothesis: $P(H_0) = \pi$ and $P(H_1) = 1 - \pi$. For simplicity, we assume that the risk of hypotheses test has uniform cost. The likelihood ratio test between $\mathcal{H}_0$ and $\mathcal{H}_1$ is $L(y) = \frac{p_1(y)}{p_0(y)}$. Thus the corresponding Bayesian decision rule is:

$$\delta_B(y) = \begin{cases} 1, & \text{if } L(y) \geq \tau \\ 0, & \text{if } L(y) < \tau \end{cases} \tag{21}$$

The rule above can be proved to have a form as follows,

$$\delta_B(y) = \begin{cases} 1, & \text{if } y \geq \frac{s}{2} \\ 0, & \text{if } y < \frac{s}{2} \end{cases} \tag{22}$$

Given a signal strength trace $x[n] = [x_1, \cdots, x_M]$, our detection algorithm is described as the following steps,

1) step1: Use Discrete Wavelet Transform (DWT) to obtain detail coefficients $d(k,j)$ at maximum scale $J \leq \lfloor \log_2(M) \rfloor$, where $k = 1, \cdots, \frac{M}{2}$
2) step2: Compare $d(k,j)$ with threshold $Thr_j = \frac{s}{2}$
3) step3: Generate alarm if $d(j,k) > Thr_j$ for some k.

The threshold $Thr_j = \frac{s}{2} = \min \Delta m 2^{\frac{j}{2}-1} |I_\psi(0)|$ for scale j where $|I_\psi(0)| = 0.5$. The value of $\min \Delta m$ is obtained empirically for each environment and is given in Table I.

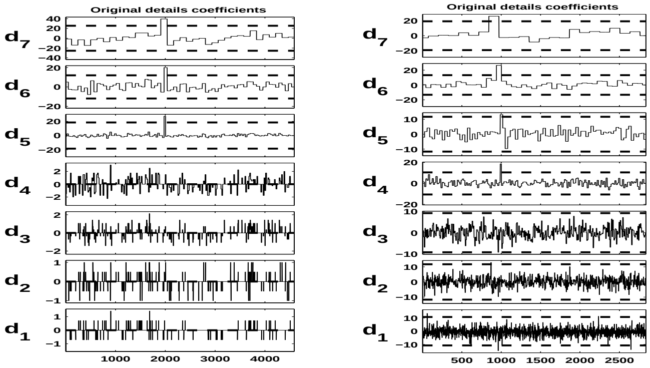
IV. Simulation and Experimental Results

We first validate the detection mechanism for indoor environment. The signal strength measurements were conducted in the building of Johnsson Engineering Center of RPI which primarily consists of rooms for faculty and space for laboratories, using a LINKSYS Wireless-G Broadband Router as the access point (AP) and IBM T42 laptop, with built in PH12127-E IBM 802.11a/b/g Wireless LAN Mini PCI adapter as receiver. To simulate a session hijacking attack where both the wireless user and attacker are moving at pedestrian speed on the aisles of Johnsson Engineering Center, we first collected the signal strength measurements $N[n]$ for wireless user that was moving with a random pattern. At time n_0, a session hijacking attack occurred. Signal strength trace $N[n]$, where $n = [n_0, \cdots, M]$ was obtained by the signal strength measurements for the attacker that was moving with some other pattern. Several traces of $N[n]$ were collected to validate the detection mechanism.

In our work, DWT is employed to decompose $x[n]$ into its approximation at any scale J where $1 \leq J \leq J_{MAX}$ where $J_{MAX} \leq \log_2(M)$ is the maximum decomposition scale, plus all the details at lower scales $j, 1 \leq j \leq J$. Figure 1 shows the detail coefficients d_j of $x[n]$ at scales $j = 1, 2 \cdots, 7$, when $J_{MAX} = 7$. We detect signal $f[n] = \Delta u[n - n_0]$ by thresholding the wavelet coefficients d_j. If $d_j(k) > Thr_j$, an alarm is generated. For one of our measured signal strength trace, its wavelet detail coefficients and corresponding detection threshold Thr_j are shown in Figure 1 (a). The session hijacking attack occurred at $n_0 = 2000$. For scales $j = 5, 6, 7$, the peak value of d_j located at time n_0 exceeds Thr_j and the corresponding session hijacking attack event is detected. The session hijacking intrusion attack can be accurately detected at all scales $j = 5, 6, 7$ with a false alarm rate of zero. However, the detected intrusion time k will be more ambiguous as j increases, which lead to a larger delay of detection time. Therefore, $j = 5$ is chosen for the purpose of accurately locating the attack time for the indoor environment. Similar results were obtained for all the traces that we collected.

To further validate our detection mechanism in diverse propagation environments, we generate multipath fading signal strength traces $N_1[n]$ and shadow fading signal strength traces $N_2[n]$, $n = 1, 2, \cdots M$, by simulation using the ITU-R model. Three different sets of $N_1[n], N_2[n]$ are generated for three different environments: indoor office environment, PED_A, PED_B [7]. To simulate path loss of signal strength $N_3[n]$, we observe the patterns of random movements of the wireless users in both indoor and outdoor environments. At any time instance n, since we know the distance between user and AP, path loss $N_3[n]$ can be estimated according to ITU-R models. The signal strength traces are then obtained by $N[n] = N_1[n] + N_2[n] + N_3[n]$. For one of our simulated signal strength trace, where the wireless user is in indoor office environment and the attacker is in PED_A environment, the wavelet detail coefficients and corresponding detection threshold Thr_j are shown in Figure 1(b). The simulated session hijacking attack occurred at $n_0 = 1000$. For scales $j = 4, 5, 6, 7$, the peak value of d_j located at time n_0 exceeds Thr_j and the corresponding session hijacking attack event is detected. No other alarm is generated besides at time n_0. $j = 4$ is chosen for the purpose of accurately locating the attack time for the scenario where the wireless user is indoors and the attacker is in PED_A environment.

The detection results for the experimental and simulated signal strength traces are summarized in Table I. For each test environment, several traces are obtained where the time instances of session hijacking attacks are randomly located. For some signal strength traces, the jump amplitude Δm is so small that it is totally embedded in noise, which lead to false alarms (false positive) and missed detections (false negative). The minimum value of Δm (dB) is obtained and the number of missed detections is recorded for each test environment. In our test, the false alarm rate is approximately the same as miss detection rate. Therefore, only miss detection rate is given in the tables. Detection delay is obtained by comparing the time of attack with the time when alarm is raised.



(a) Experimental Results

(b) Simulation Results

Fig. 1. Detection Results

TABLE I

DETECTION RESULTS

Experiments				
user	**attacker**	**detection rate**	**min Δm**	**delay (seconds)**
indoor	**indoor**	0.88	4	0.32
Simulation				
indoor	**indoor**	0.83	4	0.32
indoor	**PED_A**	0.90	3	0.16
indoor	**PED_B**	0.88	3	0.16
PED_A	**PED_B**	0.91	2	0.16

V. CONCLUSIONS

In this paper, we develop a robust algorithm to detect session hijacking in wireless networks using received signal strength. We show that a session hijacking attack event can be represented as a step signal embedded in colored noise. A wavelet based optimal filter is designed to detect the signal. The detection mechanism is validated through experimental and simulation results.

REFERENCES

[1] R. Gill, J. Smith and J. A. Clark, "Detecting Session Hijacking Attacks in IEEE 802.11 Networks," *Proceedings of Fourth Australasian Information Security Workshop,* pp. 221-230, vol.54, January 2006.

[2] M. Flament and M. Unbehaun, "Impact of shadow fading in a mm-wave band wireless network," *The 3rd Symposium on Wireless Personal Multimedia Communications IEEE,* Bangkok, Thailand, November 2000.

[3] T. Odgen and O. Parzen, "Change-Point Approach to Data Aalytic Thresholding," *Transanctions of Statistics and Computing,* pp. 93-99, vol. 6, no. 2, November 2004.

[4] M. Raimondo and N. Tajvidi, "A Peaks Over Threshold Model For Change-Point Detection By Wavelets," *Statistica Sinica,* pp. 395C412, vol. 14, part. 2, 2004.

[5] X. Lu, Y. Sang, J. Zhang, Y. Fa, "A Pipeline Leakage Detection Technology Based on Wavelet Transform Theory," *Proceedings of IEEE Information Acquisition,* pp. 1432-1437, vol.20, August 2006.

[6] M. Chabert, J.-Y.Tourneret, F. Castanie, "Additive and Multiplicative Abrupt Jump Detection Using The Continuous Wavelet Transform," *Proceedings of IEEE Acoustics, Speech, and Signal Processing,* pp. 3002-3005, vol.5, May 1996.

[7] Recommendation ITU-R M.1225, " Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000".