POSTER: Mimicry Attacks against Wireless Link Signature

Yao Liu
Department of Computer Science
North Carolina State University, Raleigh, NC
yliu20@ncsu.edu

Peng Ning
Department of Computer Science
North Carolina State University, Raleigh, NC
pning@ncsu.edu

ABSTRACT

Wireless link signature is a physical layer authentication mechanism, which uses the multi-path effect between a transmitter and a receiver to provide authentication of wireless signals. We identify a new attack, called *mimicry attack*, against the wireless link signature scheme in [7]. It is assumed in the past that an attacker cannot "spoof" an arbitrary link signature and that the attacker will not have the same link signature at the receiver unless it is at exactly the same location as the legitimate transmitter. However, we show that an attacker *can* forge an *arbitrary* link signature as long as it knows the legitimate signal at the receiver's location, and the attacker does not have to be at exactly the same location as the legitimate transmitter in order to forge its link signature.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Algorithms, Design, Security

Keywords

Wireless security, Link signature, Attacks

1. INTRODUCTION

Wireless physical layer security is becoming increasingly important as wireless devices are more and more pervasive and adopted in critical applications. For example, implantable medical devices (IMD) such as pacemaker may grant access to an external control device only when it is close enough [8], thus making it critical to verify the physical proximity of the control device.

There have been multiple proposals recently to provide enhanced wireless security using physical layer characteristics, including fingerprinting wireless devices (e.g., [2]), authenticating and identifying wireless channels (e.g., [7,11]), and deriving secret keys from wireless channel features only observable to the communicating parties (e.g., [6]).

Among the recent advances in wireless physical layer security is (wireless) link signature. Link signature uses the unique wireless channel characteristics (e.g., the multi-path effect) between a transmitter and a receiver to provide authentication of the wireless channel. Three link signature schemes [4,7,11] have been proposed so far. Since its introduction, link signature has been recognized as a wireless channel authentication mechanism for applications where wireless channel characteristics are unique (e.g., [2,6]).

We identify a new attack, which is called the *mimicry attack*, against existing link signature schemes [4,7,11]. We start our investigation with the link signature scheme in [7]. It is assumed in [7] that an attacker "cannot 'spoof' an arbitrary link signature" and that the attacker "will not have the same link signature at the receiver unless it is at exactly the same location as the legitimate transmitter." However, we show that an attacker *can* forge an *arbitrary* link signature as long as it knows the legitimate signal at the receiver's location, and the attacker does not have to be at exactly the same location as the legitimate transmitter in order to forge its link signature.

We also extend the mimicry attack to the link signature scheme in [4]. Since the last link signature scheme in [11] is essentially an integration of the techniques in [7,11], all existing link signature schemes are vulnerable to the mimicry attack. This attack thus allows an attacker to forge link signatures and impersonate wireless nodes when link signatures are used for authentication and/or identification.

2. PRELIMINARIES

2.1 Multi-path Effect and Link Signature

Wireless signal usually propagates in the air along multiple paths due to reflection, diffraction, and scattering [7]. As a result, a receiver may receive multiple copies of the transmitted signal from different paths, each of which may have a different delay due to the path it traversed on. The received signal is indeed the sum of these time delayed signal copies. Each path imposes a *response* (e.g., distortion and attenuation) on the signal traveling along it [7], and the superposition of all responses between two nodes is referred to as a *channel impulse response* [3].

The multi-path effects between different pairs of nodes are usually different, and so are the channel impulse responses [7]. Due to this reason, a channel impulse response between two nodes is also called a *link signature*, and has been proposed to provide robust location distinction and location-based authentication [7,11].

CCS'11, October 17–21, 2011, Chicago, Illinois, USA.
ACM 978-1-4503-0948-6/11/10.

Specifically, when a transmitter and attackers are in different locations, to determine whether a received signal is from the transmitter, the receiver can estimate the link signature of the received signal and compare it with the known value from the transmitter. The received signal is accepted only if the estimated link signature is similar to the known value.

2.2 Estimating Channel Impulse Responses

With the knowledge of channel impulse responses, wireless systems can achieve high quality communication with low bit error rate. A popular method for estimating channel impulse responses is the *training sequence based estimation* [9]. In this method, the transmitter sends a training sequence (i.e., a sequence of bits) over the wireless channel. The receiver then uses the same training sequence and the corresponding received signal samples to estimate channel impulse responses, where the value of the training sequence can be pre-shared [9].

Mathematical Formulation: To estimate channel impulse responses, the receiver exploits the known transmitted data content and the corresponding received samples. As discussed earlier, the sender and the receiver share a *training sequence*. For example, a training sequence can be $[0, 1, 0, 1]$.

To transmit the training sequence, the transmitter converts it into M physical layer symbols (i.e., complex numbers that are transmission units at the physical layer [3]). This process is called modulation [3]. The transmitter then sends the M symbols to the wireless channel.

Let $\mathbf{x} = [x_1, x_2, ..., x_M]$ denote the transmitted symbols in the training sequence. Assume that there exist L paths. Thus, the receiver can receive L copies of $\mathbf{x}$, each traveling on one path and undergoing a response (i.e., distortion and attenuation) caused by the corresponding path.

The vector $\mathbf{y}$ of received symbols is the convolution sum of the L copies of $\mathbf{x}$. Let $\mathbf{h} = [h_1, h_2, ..., h_L]^T$ be the channel impulse response, where h_i is the response of the i-th path. Assuming an additive white Gaussian noise (AWGN) channel, the received symbols $\mathbf{y}$ can be represented by [9]

$$\mathbf{y} = \mathbf{h} * \mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{n}$ is the white Gaussian channel noise and $*$ is the convolution operator. The matrix form of Equation (1) is

$$\mathbf{y} = \begin{bmatrix} x_1 & 0 & \cdot & 0 \\ x_2 & x_1 & \cdot & \cdot \\ \cdot & x_2 & \cdot & 0 \\ \cdot & \cdot & \cdot & x_1 \\ x_M & \cdot & \cdot & x_2 \\ 0 & x_M & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ 0 & 0 & \cdot & x_M \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ \cdot \\ \cdot \\ h_L \end{bmatrix} + \mathbf{n} \tag{2}$$

Rewriting Equation (2) in a compact matrix form gives us

$$\mathbf{y} = \mathbf{X}\mathbf{h} + \mathbf{n}, \tag{3}$$

where $\mathbf{X}$ is a $(L + M - 1) \times L$ Toeplitz matrix, containing L delayed versions of the transmitted symbols $\mathbf{x}$, and $\mathbf{y}$ is a vector consisting of $(L + M - 1)$ received symbols.

Least-square estimator and Linear minimum mean squared error estimator are are generally used to estimate $\mathbf{h}$ from Equation (3). Details of both estimators can be found in [10].

3. MIMICRY ATTACK

3.1 Overview

The root cause of mimicry attack is the linear relationship between the transmitted symbols $\mathbf{x}$, the received symbols $\mathbf{y}$, and the link signature $\mathbf{h}$, as indicated in Equation (3).

Let $\mathbf{y}_t$ and $\mathbf{y}_a$ denote the received symbols that are from the transmitter and the attacker, respectively. The attacker's goal in mimicry attack is to make $\mathbf{y}_a$ approximately the same as $\mathbf{y}_t$. When the receiver attempts to extract the link signature from the attacker's symbols $\mathbf{y}_a$, it will get a link signature that is very similar to the one estimated from $\mathbf{y}_t$. As a result, the attacker can impersonate the transmitter to bypass link signature based authentication.

The attacker needs to meet two requirements to launch a mimicry attack: First, the attacker needs to know the transmitter's symbols (i.e., $\mathbf{y}_t$) at the receiver's location. Second, the attacker needs to manipulate its own symbols to be transmitted such that when they arrive at the receiver they are similar to those from the transmitter (i.e., $\mathbf{y}_a \approx \mathbf{y}_t$).

3.2 Obtaining Transmitter's Symbols

There are multiple ways for the attacker to obtain the transmitter's symbols at the receiver's location. For example, the attacker may learn $\mathbf{y}_t$ by placing a sensing device in the proximity of the receiver. For the sake of presentation, we call this device the *symbol sensor*. It records the symbols received from the transmitter and reports them to the attacker through any available communication channel. Since the symbol sensor is geographically close to the receiver, the symbols it receives are roughly the same as those received by the receiver, and can be used as $\mathbf{y}_t$.

The attacker can also use the mathematical model $\mathbf{y}_t = \mathbf{h}_t * \mathbf{x} + \mathbf{n}$ to derive $\mathbf{y}_t$, where $\mathbf{h}_t$ is the link signature between the transmitter and the receiver. Specifically, the symbol sensor can receive symbols from the transmitter, estimate the link signature from these symbols, and report the link signature to the attacker. The attacker can use the reported link signature as an approximation of $\mathbf{h}_t$ to calculate $\mathbf{y}_t$. In this case, the symbol sensor only needs to report the derived link signatures from time to time, and the attacker can calculate $\mathbf{y}_t$ directly by using the estimated link signature $\mathbf{h}_t$ rather than wait for the sensor to report $\mathbf{y}_t$.

3.3 Manipulating Transmitted Symbols

The symbols $\mathbf{y}_a$ received from the attacker can be represented as $\mathbf{y}_a = \mathbf{h}_a * \mathbf{x}_a + \mathbf{n}_a$, where $\mathbf{x}_a$, $\mathbf{h}_a$, and $\mathbf{n}_a$ are the symbols transmitted by the attacker, the link signature of the attacker, and the channel noise, respectively. To make $\mathbf{y}_a$ equal to $\mathbf{y}_t$, the attacker can treat $\mathbf{x}_a$ as a unknown variable, and solve it from the following equation

$$\mathbf{h}_a * \mathbf{x}_a + \mathbf{n}_a = \mathbf{y}_t, \tag{4}$$

where link signature $\mathbf{h}_a$ of the attacker can be obtained from the symbol sensor as well. The solution to this equation enables $\mathbf{y}_a$ to be similar to or the same as the transmitter's symbols $\mathbf{y}_t$. As a result, the link signatures that are estimated from $\mathbf{y}_a$ will also be close to those estimated from $\mathbf{y}_t$. In Theorem 1, we give a way to solve Equation (4) and calculate $\mathbf{x}_a$ from $\mathbf{y}_t$.

THEOREM 1. *Let $\mathbf{y}_t$ and $\mathbf{y}_a$ denote the received symbols that are sent by the transmitter and the attacker, respec-*

tively. Further let $\mathbf{H}_a$ *be the Toeplitz matrix of the attacker's link signature. If* $\mathbf{x}_a = (\mathbf{H}_a^H \mathbf{H}_a)^{-1} \mathbf{H}_a^H \mathbf{y}_t$*, then* $\mathbf{y}_a = \mathbf{y}_t$*.*

Proof. Let $\mathbf{x}_a = [x_{a1}, x_{a2}, ..., x_{aM}]^T$ denote the symbols transmitted by the attacker, and $\mathbf{h}_a = [h_{a1}, h_{a2}, ..., h_{aL}]^T$ denote the link signature of the attacker. We have

$$\begin{aligned}
\mathbf{y}_t &= \mathbf{h}_a * \mathbf{x}_a + \mathbf{n}_a = \mathbf{X}_a \mathbf{h}_a + \mathbf{n}_a \\
&= \begin{bmatrix} h_{a1} & 0 & \cdot & 0 \\ h_{a2} & h_{a1} & \cdot & \cdot \\ \cdot & h_{a2} & \cdot & 0 \\ \cdot & \cdot & \cdot & h_{a1} \\ h_{aL} & \cdot & \cdot & h_{a2} \\ 0 & h_{aL} & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ 0 & 0 & \cdot & h_{aL} \end{bmatrix} \begin{bmatrix} x_{a1} \\ x_{a2} \\ \cdot \\ \cdot \\ x_{aM} \end{bmatrix} + \mathbf{n}_a \\
&= \mathbf{H}_a \mathbf{x}_a + \mathbf{n}_a.
\end{aligned}$$

Therefore, $\mathbf{y}_t = \mathbf{h}_a * \mathbf{x}_a + \mathbf{n}_a \Leftrightarrow \mathbf{y}_t = \mathbf{H}_a \mathbf{x}_a + \mathbf{n}_a$. We can solve $\mathbf{x}_a$ from $\mathbf{y}_t = \mathbf{H}_a \mathbf{x}_a + \mathbf{n}_a$. Since $\mathbf{n}_a$ is unknown, we use the standard least square approach [10] to solve $\mathbf{x}_a$. Specifically, we minimizes $||\mathbf{y}_t - \mathbf{H_a \hat{x}_a}||^2$, where $\hat{\mathbf{x}}_a$ is the approximate solution of $\mathbf{x}_a$. The minimization yields $\hat{\mathbf{x}}_a = (\mathbf{H}_a^H \mathbf{H}_a)^{-1} \mathbf{H}_a^H \mathbf{y}_t$ □

Elements in $\mathbf{x}_a$ are already physical layer symbols, and thus they can be transmitted directly. The attacker does not need to modulate them again for transmission.

4. INITIAL EVALUATION RESULTS

We have implemented the link signature scheme in [7] and the basic mimicry attack on USRP2 platform [5]. The software toolkit is GNURadio [1]. In our evaluation, we consider two scenarios: (1) *normal scenario* and (2) *forgery scenario*. In a normal scenario, the attacker simply sends original symbols to the receiver. In the forgery scenario, the attacker launches the mimicry attack, during which it transmits manipulated symbols to the receiver.

Intuitively, the attacker wants to reduce the difference between its own link signature and the transmitter's link signature, whereas the defense method aims to increase this difference to alert the receiver. Thus, the link difference between both the attacker's and the transmitter's link signatures can visually reveal the impact of mimicry attacks, and we use link difference as our evaluation metric. The way to calculate the link difference is shown in [7].

In each evaluation scenario, the receiver first measures a set $\mathcal{H}$ of $N = 50$ link signatures of the transmitter in the training phase. It then collects 450 link signatures of the attacker and calculates the link difference $d_{a,\mathcal{H}}$ for each. Moreover, the receiver collects another 450 link signatures of the transmitter, and calculates the link difference $d_{t,\mathcal{H}}$ for each of them. Figures 1 and 2 show the link differences for the attacker $d_{a,\mathcal{H}}$ and the transmitter $d_{t,\mathcal{H}}$ in the normal and forgery scenarios, respectively.

In the normal scenario, as shown in Figure 1, $d_{a,\mathcal{H}}$ is generally larger than $d_{t,\mathcal{H}}$. Most of the transmitter's link difference is less than 0.15, whereas most of the attacker's link difference is larger than 0.15. Thus, based on the link difference, the receiver can achieve a high accuracy in distinguishing between the transmitter and the attacker.

In the forgery scenario, the attacker launches mimicry attacks to make its own link signatures similar to the transmitter's link signatures. Figure 2 shows that $d_{a,\mathcal{H}}$ decreases to the same level as $d_{t,\mathcal{H}}$, and $d_{a,\mathcal{H}}$ and $d_{t,\mathcal{H}}$ substantially overlap with each other. The mimicry attack reduces the link difference between the attacker and the transmitter, leading to high decision error rate at the receiver.

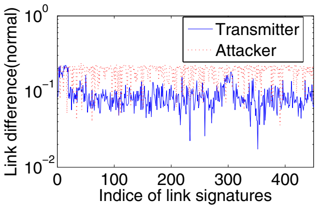

Figure 1: Normal

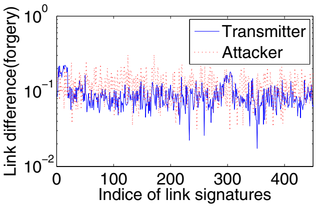

Figure 2: Forgery

5. REFERENCES

[1] GNU Radio - The GNU Software Radio. http://www.gnu.org/software/gnuradio/.

[2] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom '08)*, pages 116–127, 2008.

[3] A. Goldsmith. *Wireless Communications*. Cambridge University Press, New York, NY, USA, 2005.

[4] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *In Proceedings of ACM Workshop on Wireless Security (WiSe'06)*, 2006.

[5] E. R. LLC. The USRP product family products and daughter boards. http://www.ettus.com/products. Accessed in April 2011.

[6] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom '08)*, pages 128–139, 2008.

[7] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 111–122, New York, NY, USA, 2007. ACM.

[8] K. Rasmussen, C. Castelluccia, T. Heydt-Benjamin, and S. Čapkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, 2009.

[9] R. Safaya. A multipath channel estimation algorithm using a kalman filter. http://www.ittc.ku.edu/research/thesis/documents/rupul_safaya_thesis.pdf.

[10] K. S. Shanmugan and A. M. Breipohl. *Random signals: detection, estimation, and data analysis*. Wiley, May 1988.

[11] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera. Advancing wireless link signatures for location distinction. In *MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking*, New York, NY, USA, 2008. ACM.