International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

DETECTION OF MIMICRY ATTACKS AGAINST WIRELESS LINK SIGNATURE USING TIME-SYNCHED LINK SIGNATURE

B.Dhivya ,
Research Scholar,
Department Of Computer Science,
Theivanai Ammal College For Women,
Villupuram,Tamilnadu,India.

Dr.R.Suguna,
Assistant Professor,
Department Of Computer Science,
Theivanai Ammal College For Women,
Villupuram,Tamilnadu,India.

Abstract: Wireless link signature is a physical layer authentication mechanism, which uses the unique wireless channel characteristics between a transmitter and a receiver to provide authentication of wireless channels. A vulnerability of existing link signature schemes has been identified by introducing a new attack, called mimicry attack. To defend against the threat identified in this paper, we develop a new link signature scheme, which is called time-synched (i.e., time synchronized) link signature. Time-synched link signature integrates cryptographic protection as well as time factor into the wireless physical layer features, and provides an effective countermeasure against mimicry attacks. We also perform an extensive set of experimental evaluation of the mimicry attacks and the time-synched link signature scheme on the USRP2 platform running GNU Radio. Our experiments confirm that the mimicry attacks against the previous link signature schemes are a real threat and demonstrate that the newly proposed time-synched link signatures are effective in mitigating those attacks.

Keyword: Link signature, MIMO, time-synched.

I. INTRODUCTION

Wireless physical layer security is becoming increasingly important as wireless devices are more and more pervasive and adopted in critical applications. There have been multiple proposals in recent years to provide enhanced wireless security using physical layer characteristics, including fingerprinting wireless devices (e.g., [1]–[4]), authenticating and identifying wireless channels (e.g., [5], [6]), and deriving secret keys from wireless channel features only observable to the communicating parties (e.g., [7], [8]). 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 [5], [6], [9] have been proposed so far. Since its initial introduction, link signature has been recognized as a physical layer authentication mechanism for applications where wireless channel characteristics is unique for individual nodes.

In this paper, we identify the mimicry attack against these link signature schemes. Link signature based wireless security mechanisms exploit the radio channel characteristics between two wireless devices to provide security protection complementary to traditional cryptographic approaches. The success of these schemes relies crucially on the uniqueness of link signatures resulting from the assumed fast spatial decorrelation of wireless channels; in particular, it is widely accepted that half a wavelength separation is sufficient for security assurance. Built upon this optimistic assumption, various secret key extraction and signal authentication techniques have been developed based on link signatures (e.g., [1–8]). However, two critical questions remain unclear. First, does the common "half-wavelength decorrelation" assumption hold in all circumstances? As pointed out in [9–11], the spatial channel correlation is significantly influenced by the angular spread (AS) of the incoming signal. When two receivers are surrounded by rich scatterers, their corresponding AS is usually large and the half-wavelength decorrelation conclusion holds. But when a line-of-sight (LOS) component exists or the waveguide propagation effect dominates, the AS is small and will induce high spatial channel correlation. In fact, high spatial channel correlations have already been observed in realworld experiments [12]. Second, when the half-wavelength decorrelation assumption is violated, is the current link signature technique still able to provide security protection to wireless applications? This question attracts research interest very recently (e.g., [13, 14]). However, to the best of our knowledge, none of the existing literatures answers it in quantifiable measures based on a solid analysis.

The mimicry attack can apply to the following example scenarios when link signatures are used for authentication: (1) launching location spoofing attacks: an attacker can utilize a fake location to fool a target receiver by creating a fake wire-less link signaturer; (2) bypassing motion detection systems: an attacker could maintain its wireless signature unchanged while it is actually moving, thus from the perspective of the target receiver, who utilizes the wireless link signature to determine whether the transmitter moves or not, the attacker appears to remain stationary; (3) bypassing wireless trans-mitter authentication systems: an attacker can impersonate a legitimate transmitter by forging its wireless link signature. In fact, high spatial channel correlations have already been observed in realworld experiments [12]. Second, when the half-wavelength decorrelation assumption is violated, is the current link signature technique still able to provide security protection

to wireless applications? This question attracts research interest very recently (e.g., [13, 14]). However, to the best of our knowledge, none of the existing literatures answers it in quantifiable measures based on a solid analysis.

To provide physical layer authentication capability and defend against the threats identified in this paper, we develop a novel construction for link signature, which is called time-synched (i.e., time synchronized) link signature. Time-synched link signature integrates cryptographic protection as well as time factor into the wireless physical layer features, and provides an effective and practical solution for authenticating physical layer wireless signals. We also perform an extensive set of experimental evaluation of the mimicry attacks and the time-synched link signature scheme on the USRP2 platform running GNU Radio. Our experiments show that the mimicry attack can deteriorate the success rate of distinguishing between the legitimate transmitter and the attacker to 0.5935, which is close to a blind guess. First, we identify the mimicry attack against existing link signature schemes and extend the mimicry attack to MIMO systems. Second, we develop the time-synched link signature scheme to defend against various threats against existing link signature schemes, including the mimicry attacks presented in this paper. Finally, we perform extensive experiments to confirm the threats of the mimicry attack and demonstrate the effectiveness of the time-synched link signature for physical layer authentication.

II. RELATED WORK

A. Wireless Transmitter Authentication

Existing techniques using non-cryptographic approaches to authenticate wireless transmitters can be classified into three categories [2]: software fingerprinting (e.g., [28]–[30]), location distinction (e.g., [5], [6], [9]), and radiometric identification (e.g., [2], [31]). In software fingerprinting approaches, discrepancies in soft-ware configuration are used as fingerprints to distinguish between wireless nodes [2]. For example, Franklin et al. [28] proposed to use the implementation dependent differences among device drivers to identify 802.11 nodes. Kohno et al. [30] proposed to use clock skews in TCP and ICMP timestamps to fingerprint networked devices. In location distinction based authentication, a signal is authenticated by verifying whether it originates from the expected location of the transmitter. RSS (e.g., [32]) and link signatures have been used to enable such location dis-tinction [5]. The RSS based methods directly estimate the location of a signal origin using the RSS values. However, such methods can be defeated with an array antenna, which can fake arbitrary source locations [5]. The link signature based approaches authenticate the channel characteristics between the transmitter and the receiver [5], [6], [9]. In this paper, we showed that all these link signature scheme are vulnerable to mimicry attacks. Our newly proposed time-synched link signature is developed to fill this gap.

B. Attacks on Radiometric Identification

Recently, it was demonstrated in [33] and [34] that radio-metric identification techniques were vulnerable to imperson-ation attacks. The results in [33] revealed that both transient and modulation based techniques are vulnerable to imperson-ation attacks, though transient-based techniques are harder to reproduce. Edman and Yener [34] showed that an attacker can significantly reduce the accuracyof such techniques by simply using a commodity RF hardware platform. These works are complementary to ours in this paper.In our previous works [35] and [36], we only addressed the simple mimicry attack scenario, where both the receiver and the attacker have only one antenna. In this paper, we discussed the general case when both the receiver and the attacker have multiple antennas, and discovered that the mimicry attack is still feasible in MIMO systems, as long as the attacker can utilize at least the same number of antennas as the receiver. We also extended mimicry attacks to the multiple tone probing based link signature and showed that mimicry attacks can make all existing link signature schemes vulnerable. Furthermore, in [36], we only compared the link differences for the attacker and the transmitter in the normal, forgery and defense scenarios, respectively. In this paper, we further explored how to set an appropriate threshold that enables the proposed time-synched link signature scheme to achieve a high detection rate while keeping a low false alarm rate in the three scenarios.

III. PROPOSED METHODOLOGY

In this section, we develop a novel time-synched link signature to defend against the mimicry attack. A key feature of this new mechanism is the integration of cryptographic protection and time factor into wireless link signatures.

A. Assumptions and Threat Analysis Assumptions: We assume that there are a Transmitter and a Verifier, who share a secret key K that is only known to them. The Transmitter sends physical layer frames to the Verifier, who then verifies if these frames are directly transmitted by the Transmitter. We assume that the attacker can eavesdrop, overhear, and jam wireless communications. However, we assume that the attacker cannot compromise the Transmitter or the Verifier, and thus does not know their secret. Let us first understand what new challenges the mimicry attack brings given the existing network security tools. First of all, note that we can simply add digital signatures or Message Integrity Code (MIC) into each frame. As a result, the frames forged by the attacker can be easily detected through authentication of message content. Thus, the remaining threat is from the frames that are originally generated by the Transmitter but forwarded by the attacker. Note that the frame forwarded by the attacker is the same as the original frame generated by the Transmitter at the bit level, but different at the symbol level. Moreover, with replay attack detection mechanism such as sequence numbers, if the Verifier can receive the original frames sent by the Transmitter, it can easily identify frames forwarded by the attacker as duplicates and discard them. Thus, the unresolved threats are from the following two cases: (1) when the attacker can jam and replay the Transmitter's frames (jam-and-replay attack [5]), and (2) when the Transmitter and the Verifier are out of communication

range, but the jammer forwards frames from the Transmitter to the Verifier. In this paper, we focus on the unresolved threats, assuming existing mechanisms such as cryptographic authentication and sequence numbers can be used. In the following, we clarify the attacker's capabilities in forwarding frames. .

B. Design Strategy :

The fundamental reason for the mimicry attack is that the attacker can establish a set of equations based on (1) the knowledge of the training sequence and (2) the Transmitter's signal (i.e., physical layer symbols) at the Verifier's location. These allow the attacker to manipulate the transmitted physical layer symbols so that a forged frame has a valid link signature. Initial Idea: To defend against this attack, our strategy is to deprive the attacker at least one of these two pieces of information. It is in general very difficult to prevent a passive attacker from receiving signals (and then extracting valid link signatures). However, it is possible to prevent the attacker from knowing the training sequences. Thus, our initial idea is to use unpredictable, dynamic, and authenticated training sequences for extracting link signatures from wireless packets (frames). Detecting Frames Forwarded by Attackers: It is not hard to realize that simply using unpredictable, dynamic, and authenticated training sequences is still insufficient. **Detecting Frames Forwarded by Attackers:** It is not hard to realize that simply using unpredictable, dynamic, and authenticated training sequences is still insufficient. The attacker can receive and analyze the Transmitter's signal to learn the training sequence. If the Verifier cannot receive the original transmission (e.g., due to jam-and-replay attack), the attacker can still forge link signatures by manipulating and forwarding a frame received from the Transmitter.

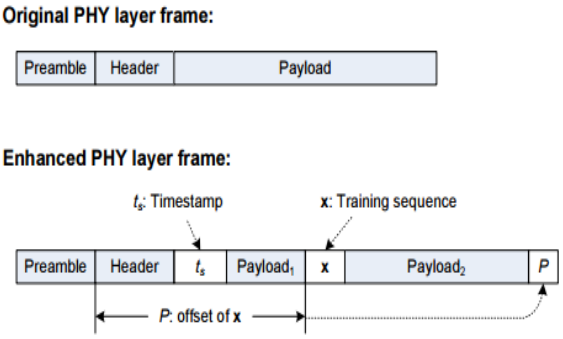

Fig.1. PHY layer frame: Dynamic training sequence with random offset

C. Training Phase

The training phase is intended for the Verifier to collect enough information from the Transmitter so that the Verifier can verify the link signatures of the future frames from the Transmitter. The Verifier should obtain the valid link signature from the Transmitter whenever the link signature may change. This can be accomplished by executing the training phase protocol periodically or whenever one of them moves. In the training phase, the Verifier needs to synchronize its clock with the Transmitter, and obtain the link signature for the current communication channel. Moreover, it needs to confirm that there is no successful attack during the training phase.

We use the classic time synchronization technique (e.g., [13]) to estimate the clock discrepancy between the Transmitter and the Verifier as well as the frame traverse time. We refer to the point in time when the anchor (e.g., the SFD field) in a frame is transmitted or received as the transmission time or the receiving time of this frame. Specifically, the Verifier sends a request frame to the Transmitter, and at the same time records the frame transmission time t1 in the Verifier's local clock. When the Transmitter receives the request frame, it records the receiving time t2 of this frame, and then sends a reply frame to the Verifier, in which t2 and the transmission time t3 of the reply frame (in the Transmitter's clock) are included. Finally, the Verifier receives the reply frame and records the receiving time t4 in its clock.

Figure 2 shows the training phase protocol between the Transmitter and the Verifier.

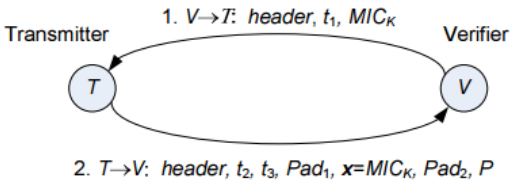

Fig. 2. Training phase protocol

Training Request: The Verifier sends the first training request frame to the Transmitter, which includes the frame header, the transmission time t1 of this frame, and the frame MIC that covers the entire frame (excluding the preambles). Upon receiving of the request frame, the Transmitter immediately records the receiving time t2 of the frame, and authenticates the request frame by verifying the MIC.

Training Reply: Upon verifying a training request frame, the Transmitter should send back a training reply frame. The Transmitter should include time t2 and the actual transmission time t3 of the reply frame in the frame. The Transmitter also pads the frame payload to at least the minimum frame length Lmin and randomly selects an offset P to place the training sequence as discussed earlier. The Transmitter then leaves a placeholder (e.g., all 0's) in place of the training sequence and computes the frame MIC using the shared key K. Finally, the Transmitter places the frame MIC as the training sequence x in the reply frame and sends it over the air. Once the Verifier receives the training reply frame, the Verifier computes the clock discrepancy δ and the one-way transmission time τ.

D. Operational Phase

Once the Verifier obtains the clock discrepancy and the valid link signature from the Transmitter, they can start the operational phase, during which the Verifier uses this link signature to verify frames that require physical layer authentication.

Transmitter: The Transmitter follows the design shown in Figure 1. Specifically, the Transmitter randomly selects an offset in the frame payload to include the field for the training sequence. places the offset P at the end of the frame, and computes the frame MIC using the shared secrete key K, with a placeholder (e.g., all 0's) for the training sequence. The Transmitter then uses the frame MIC as the training

sequence x, puts it in the frame, and sends the frame over the air.

Verifier: When the Verifier receives the frame, it immediately records the receiving time tr. The Verifier then retrieves the frame transmission time ts from the received frame and estimates the frame traverse time $\tau = ts - tr - \delta$, where δ is the clock discrepancy between the Verifier and the Transmitter learned in the training phase. If τ is greater than the threshold τ max, the maximum possible direct transmission time, the Verifier should consider the frame possibly forwarded by the attacker and discard it. Otherwise, the Verifier locates the frame MIC by using the offset P at the end of the frame, verifies the frame MIC using the shared key K, and then uses the frame MIC as the training sequence to extract the link signature. Finally, the Verifier compares this link signature with the one derived during the training phase. The frame is accepted if this link signature does not deviate from the valid one learned in the training phase. Otherwise, the frame is considered forged and discarded.

V. EXPERIMENTAL RESULT

We have implemented the link signature scheme in [5], the mimicry attack, and the newly proposed time-synched link signature. We have also implemented the frame repeater attack, which can be used along with the mimicry attack. Our prototype uses USRP2 [13], which are equipped with AD and DA converters as the RF front ends, and XCVR2400 daughter boards operating in the 2.4 GHZ range as transceivers. The software implementation is based on GNURadio [14]. USRP2s are capable of processing signals up to 100MHz wide. Such a high bandwidth enables the use of them for capturing multipath effects and measuring link signatures. However, GNURadio configuration requires to set the values of interpolation (decimation) rate at the transmitter (receiver) and the number of samples per symbol. If the values of those parameters are set too high, the actual bandwidth will be significantly reduced.

To guarantee the capture of multipath effect, we set those parameters the minimum values allowed by GNURadio (i.e., 5 for interpolation and decimation rate,and 2 for number of samples per symbol). We evaluate three scenarios: (1) normal scenario, (2) forgery scenario, and (3) defense scenario. In a normal scenario, the attacker simply sends original symbols to the receiver. In both the forgery and the defense scenarios, the receiver functions as the symbol sensor for the attacker. It estimates the link signatures for the attacker and provides this link signature and the received symbols from the transmitter to the attacker. Upon obtaining this information, the attacker launches the mimicry attack. However, the forgery scenario uses the previous link signature scheme in [5], while the defense scenario uses the newly proposed time-synched link signature.

VI. CONCLUSION

A mimicry attacker can forge a transmitter's link signature if she knows approximately the legitimate symbols at the receiver. To defend against the mimicry attack, we proposed the time-synched link signature scheme by integrating cryptographic protection and time factor into wireless features. Our experimental results demonstrated both the feasibility of mimicry attacks and the effectiveness of the proposed method.

VII.REFERENCES

[1] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," inProc. ACM Workshop Wireless Secur. (WiSec), 2006, pp. 43–52.

[2] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identifi-cation with radiometric signatures," inProc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 116–127.

[3] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identi-fication via analog signal fingerprinting: A matched filter approach," in Proc. 13th Annu. Symp. Netw. Distributted Syst. Secur. (NDSS), 2006, pp. 1–11.

[4] L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, "Identifying unique devices through wireless fingerprinting," inProc. 1st ACM Conf.Wireless Netw. Secur. (WiSec), 2008, pp. 46–55.

[5] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in Proc. 13th Annu. ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2007, pp. 111–122.

[6] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," inProc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 26–37.

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless chan-nel," inProc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 128–139.

[8] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," inProc. IEEE INFOCOM, Apr. 2013, pp. 3048–3056.

[9] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless sys-tems via lower layer enforcements," in Proc. ACM Workshop Wireless Secur. (WiSec), 2006, pp. 33–42.

[10] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signalsin cognitive radio networks via integrated cryptographic and wirelesslink signatures," in Proc. IEEE Symp. Secur. Privacy (S&P), May 2010,pp. 286–301.