Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

MIMICRY ATTACKS AGAINST WIRELESS LINK SIGNATURE AND NEW DEFENSE USING TIME-SYNCHED LINK SIGNATURE

Ms.R.Keerthika,
Assistant Professor,
Department of Computer Science,
Vel Tech Ranga Sanku Arts College,Avadi, Chennai-62.

Abstract

Wireless link signature is becoming increasingly important as wireless devices between a transmitter and a receiver to provide authentication of wireless signals. This paper identifies a new attack, called mimicry attack, against the existing wireless link signature schemes. It is assumed in 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". To defend against the mimicry attack, this paper proposes a novel construction for wireless link signature, called time-synched link signature, by integrating cryptographic protection and time factor into wireless physical layer features. This link signature is effective in physical layer authentication.

Introduction

There have been multiple proposals in recent years to provide enhanced wireless security using physical layer characteristics, including fingerprinting wireless devices, authenticating and identifying wireless channels, and deriving secret keys from wireless channel features only observable to the communicating parties. We also extend the mimicry attack to the link signature scheme. Since the last link signature scheme is essentially an integration of the techniques, all existing link signature schemes are vulnerable to the mimicry attack. Furthermore, we find that if the receiver has two antennas to cooperatively authenticate the transmitter, the attacker with only one antenna cannot successfully launch the mimicry attack. However, we discover that the

Copyright © 2019 Authors

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

mimic attack is still feasible if the attacker also has two antennas. Then we explore the feasibility of the mimicry attack into MIMO systems. If the number of the receiver's receive antennas is larger than that of the attacker's transmit antennas, the receiver can detect the mimicry attack, otherwise, the receiver can be fooled that the attacker's link signatures are the same with the ones of the authenticated transmitter's. 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 wireless link signature; (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 transmitter authentication systems: an attacker can impersonate a legitimate transmitter by forging its wireless link signature.

Hypothesis

Existing techniques using non-cryptographic approaches to authenticate wireless transmitters can be classified into three categories: software fingerprinting, location distinction, and radiometric identification. 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. The link signature based approaches authenticate the channel characteristics between the transmitter and the receiver. In radiometric identification approaches, the distinctive physical layer characteristics exhibited by wireless devices are utilized to distinguish between them.

Disadvantages

- will not have the same link signature at the receiver
- the attacker with only one antenna cannot successfully launch the mimicry attack

Proposed hypothesis

Copyright © 2019 Authors

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

We identify the mimicry attack against these link signature schemes. Then we explore the feasibility of the mimicry attack into MIMO systems. If the number of the receiver's receive antennas is larger than that of the attacker's transmit antennas, the receiver can detect the mimicry attack, otherwise, the receiver can be fooled that the attacker's link signatures are the same with the ones of the authenticated transmitter's. 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. 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.

Methodology

Link Signature

Link signature uses the unique wireless channel characteristics between a transmitter and a receiver to provide authentication of the wireless channel. We start our investigation with the link signature scheme. It is assumed 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 in this paper 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.

Training sequence

The transmitter first sends a sequence of bits over the wireless channel. The receiver then uses the training sequence and the received corresponding packets to estimate channel impulse responses, where the data value of the training sequence can be pre-shared. To transmit the

Copyright © 2019 Authors

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

training sequence, the transmitter converts files into packets. The transmitter then sends the M symbols to the wireless channel.

Multiple signatures

In our previous works and 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

Detecting packets

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. To handle this threat, we propose to bring "time" into the scheme. We assume the Transmitter and the Verifier have synchronized clocks. (As we will show in the proposed scheme, in the training phase the Transmitter and the Verifier will synchronize their clocks to meet this assumption.) The Transmitter may include a timestamp in the transmitted frame, which indicates the time when a particular bit or byte (e.g., the Start of Frame Delimiter (SFD) field in an IEEE 802.11 or 802.15.4 frame [24]) is transmitted over the

Copyright © 2019 Authors

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) sponsored by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

air. We assume that the Transmitter can use authenticated time stamping techniques to ensure that the timestamp precisely represents the point in time when the SFD field is transmitted in air. As a result, upon receiving a frame, the Verifier can use the timestamp included in the frame and the time when it receives the frame, which should also be obtained through Medium Access Control (MAC) layer time stamping to estimate the traveling time of the frame. An overly long time indicates that the frame has been forwarded by an intermediate attacker. Also, an attacker may revise the timestamp to conceive the Verifier that the calculated delay is small. To avoid such attacks, the Transmitter will send the MIC of the entire frame along with the frame to the Verifier. Thus any revision of the timestamp by an attacker will be detected by the Verifier.

CONCLUSION

In this paper, we identified the mimicry attack against the existing wireless link signature schemes. We then extended the mimicry attack in MIMO systems and concluded that the attacker utilizing at least the same number of antennas as the receiver's antennas can successfully launch the mimicry attack. To defend against the mimicry attack, we proposed the novel time-synched link signature construction by integrating cryptographic protection and time factor into wireless physical layer features. We also performed an extensive set of experiments to demonstrate both the feasibility of mimicry attacks and the effectiveness of time-synched link signature.

REFERENCES

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

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

Copyright © 2019 Authors

[3] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identification 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," in Proc. 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," in Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 26–37

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. 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," in Proc. IEEE INFOCOM, Apr. 2013, pp. 3048–3056.

[9] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proc. ACM Workshop Wireless Secur. (WiSec), 2006, pp. 33–42. FANG et al.: mimicry attacks against wireless link signature and new defense 1527

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

Copyright © 2019 Authors

[11] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," IEEE Wireless Commun., vol. 17, no. 5, pp. 56–62, Oct. 2010.

[12] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: Cooperative proximity-based authentication," in Proc. 8th Int. Conf. Mobile Syst., Appl., Services (MobiSys), 2010, pp. 331–344.

Copyright © 2019 Authors