A Real-time Two-way Authentication Method Based on Instantaneous Channel State Information for Wireless Communication Systems

Xiangyu Lu, Yuyan Zhang, Yuexing Peng, Hui Zhao, Wenbo Wang
Wireless Signal Processing & Network Lab
Key Lab of Universal Wireless Communications, Ministry of Education
Beijing University of Posts & Telecommunications, Beijing, China
Email:buptkingxiangyu@gmail.com, zhangyuyan007@163.com, {yxpeng,hzhao,wbwang}@bupt.edu.cn

***Abstract*—Traditional solutions handle security at the application layer, which causes huge signaling overhead and long delay if authentication is implemented for every signal to enhance the security of wireless communication systems. In this paper, a real-time and two-way authentication method is proposed, which is based on the characteristics of radio channel including randomness and privacy. For the proposed method, the unique instant channel state information (CSI) can be used to authenticate the transmitter. In frequency- and time-selective fading channels, the current estimated CSI is compared with the predicted CSI, which is implemented at the previous frame, in order to authenticate the validation of the received signal. Both the hypothesis testing and mutual information measure methods are used for authentication determination, and the Mont Carlo simulation results verify the efficiency of the proposed method.**

***Index Terms*—Physical-layer security; authentication; channel state information (CSI); channel estimation; channel prediction; hypothesis testing; mutual information measure.**

I. INTRODUCTION

Authentication is the process where claims of identity are verified. Most mechanisms of authentication of mainstream wireless communication systems, such as cellular mobile communication systems [1], wireless broadband access systems [2] and wireless sensor networks (WSN) [3][4], are based on traditional cryptography encryption and functioned at high layer. The authentication is set up by invoking the higher layer protocol stack at call establishing, location updating, and other value-added service.

In wireless communication system, especially the acentric networks like WSN and wireless ad hoc networks, the broadcast nature of the channels makes it easy for wiretapping and other attacks via air interface, and the existing security mechanism for wireless communication does not contain the appropriate design of real-time identity authentication [5][6]. Moreover, two-way authentication, which means the communication pair should authenticate each other, is required to avoid fake user (source) attacks and fake base station (sink) attacks [7][8]. Under this circumstance, a reliable two-way real-time authentication mechanism is urgently needed. However, if every message is authenticated in order to strengthen the real-time security, the current authentication process will call the upper layer authentication protocol, which will bring about huge signaling overhead and result in very long delay. Obviously the wireless communication system cannot endure such huge signaling overhead, and the authentication caused protocol processing delay makes the quality of service (QoS) unacceptable. Therefor more effective and real-time two-way authentication mechanism is urgently needed.

Recently channel-like fingerprint has been used to enhance the security in physical layer (PHY) [9]-[15]. Besides the broadcast feature, the radio channels feature randomness and privacy as well due to the multipath propagation effect of radio waveform [16]. That is to say, (1) randomness means the channel state information (CSI) varies rapidly and randomly. With the characteristics of randomness, the authentication is more reliable because the random and variable CSI makes the authentication code (namely, the CSI) change fast. (2) privacy means the CSI of the link between communication pair is unique due to the CSI decorrelates rapidly in space and time if the paths are separated by the order of an RF wavelength or more in scatter rich environments. Based on the randomness and privacy features of channel, Faria et.al firstly proposed a scheme in [9] to detect identity-based attacks by using the signal strength information, namely, the instantaneous signal-to-noise ratio (SNR). Xiao et al. proposed the authentication methods using the CSI information in [10]-[12], and then extended the PHY authentication methods to multiple-input multiple-output (MIMO) systems [13][14] and orthogonal frequency-division multiplexing (OFDM) systems [15].

In this paper, we propose a real-time two-way authentication method in physical layer based on instantaneous CSI. Our method differs with the existed methods on that we estimate and predict the CSI, and then compares the predicted CSI with the newly estimated CSI. When the predicted CSI and the estimated CSI is highly correlated, the identity of the authenticated user is said to be verified. Our method can be reliably used as PHY authentication is due to the observation that the CSI changes continuously in time- and frequency-domain, and results in the predicted CSI will be highly correlated with the previous estimated CSI of the same channel. Since the pilot-aided channel estimation and simple prediction methods are widely applied to obtain the CSI in all kinds

Manuscript received July 18, 2011; accepted August 3, 2011.

doi:10.4304/jcm.6.6.471-476

of wireless communication systems including single carrier (SC)/multiple carrier (MC) systems and single-input single-output (SISO)/MIMO systems in all sorts of selective fading channels, the proposed method needs no complicated channel modeling and parameters identification as done in [12], and can be easily applied without introduction of extra complexity, which is of importance for energy-constraint networks like WSN. Since the simplicity of our method, real-time per-message authentication is easily realized. Moreover, CSI is usually estimated at both sides of the communication pair, and then two-way authentication is achieved by implementing the proposed method at both ends.

The main contributions of the proposed authentication method are listed below.

1) CSI estimation and prediction based real-time authentication method is developed in PHY. This method facilitates application in wireless communication systems due to the widely used pilot-aided CSI estimation and simple CSI prediction method without induction of extra complexity or any changes to the exist systems.

2) Two-way authentication is achieved when the proposed method is implemented at both sides of the communication pair, and also no extra complexity is introduced due to the CSI estimation is widely applied to obtain CSI in current wireless communication networks.

3) Mutual information (MI) measure as well hypothesis testing is employed for the authentication determination.

The rest of the paper is organized as followed. System model is introduced in Section II, and the proposed method is presented in detail in Section III. In Section IV, numerical simulation is implemented to verify the performance of the proposed method, and we conclude the paper in Section V.

II. SYSTEM MODEL

A. Network topology

As shown in Figure 1, we use the same system model as that in [10]-[12], which we borrow from the conventional terminology of the security communication by setting three different parties: Alice, Bob and Eve. Alice broadcasts signals, and both Bob and Eve can receive the signals transmitted through wireless environment. However Bob is only would-be receiver while Eve is the eavesdropper.

Authentication is set up when call establishing, location updating, by invoking the higher layer protocol stack. However during the authentication process, if the active Eve cracks the random number which is used to compute security key, he can get the security key via A8 algorithm [1]. Then Eve can impersonate as Alice to communicate with Bob and intercept and capture what he wants. Since the authentication does not implement for each signal, Eve can act as Alice during the session.

In order to avoid the fake identity of Eve as Alice, we propose an active two-way authentication method which provides real-time and efficient authentication in PHY per message between Alice and Bob, in spite of the presence of Eve. Since Eve is within range of Alice and Bob, and capable of impersonating Alice to send her malicious signals to Bob, Bob must have the ability to differentiate between legitimate signals from Alice and illegitimate signals from active Eve.

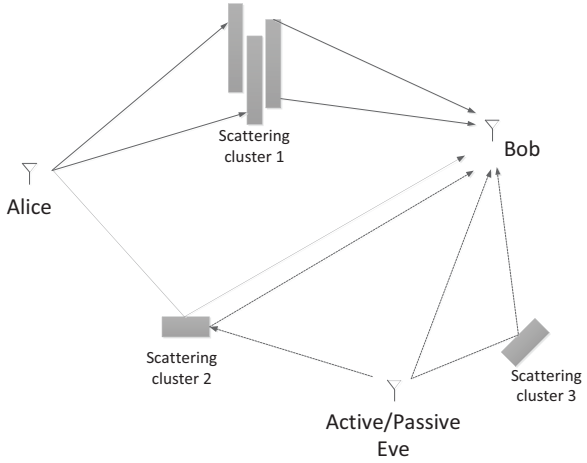


Fig. 1: The system model, where Alice sends messages to Bob over multipath channel with the eavesdropper Eve.

Consider a simple transmission in which Bob seeks to verify that Alice is the transmitter of the present message. Suppose that Alice transmits probes into the channel at a rate sufficient to assure temporal coherence between channel estimates and that, prior to Eve's arrival, Bob has estimated and saved the Alice-Bob channel. After a while, Eve wishes to convince Bob that he is Alice, Bob must verify that if the signals is still send by Alice at this time. The CSI of linked between Alice and Bob is a result of the multipath environment, as time goes on it has changed [16]; Bob may use the saved CSI of Alice-Bob link to predict present CSI [10]-[15]. Bob may also use the received signal to estimate the CSI and compare it with the predicted one for the Alice-Bob link. If these two CSI are highly correlated, then Bob will conclude that the source of the message is the same as the source of the previously sent message. If the channel estimates are not similar, then Bob should verdict that the transmitter is likely not Alice.

In the following sections, the notations we will use are listed as followed, where bold italic stands for vector.

$\boldsymbol{\hbar_{AB}}$,$\boldsymbol{\hbar_{BA}}$:CSI vectors from A to B and from B to A;

$\tilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}$,$\tilde{\boldsymbol{\hbar}}_{\boldsymbol{BA}}$,:Noisy CSI vectors from A to B and from B to A;

$\mathscr{H}_0$,$\mathscr{H}_1$:The null hypothesis and the alternative hypothesis;

α,β:Type I and Type II error;

χ^2:Chi-square distribution;

F_{χ^2}:Distribution function of chi-square distribution;

T_C,B_C:The channel's coherent time and bandwidth;

f_m:The Doppler shift;

$J_0(\bullet)$:The first kind zero-order modified Bessel function.

B. Channel Model

In wireless communication environment, rich scattering and the movement of the terminals cause multipath and dispersion in the time, frequency and angle domains. Without loss of generality, only the SISO channels are considered in this paper, and it is quite straight to extend to MIMO channels. In the case of SISO channel, parameters in time- and frequency-domain,

the multipath delay and the channel fading, can characterize the features of the channel.

Firstly the time/frequency coherence model of the channel is introduced by computing the coherence of signal's envelope [16]. Suppose the two envelopes are $r_1(t)$and $r_2(t)$, their frequency deviation is$\Delta f = |f_1 - f_2|$, and the correlation coefficient is

$$\begin{aligned}\rho_r(\Delta f,\tau) &= \frac{R_r(\Delta f,\tau)-\langle r_1\rangle\langle r_2\rangle}{\sqrt{[\langle r_1^2\rangle-\langle r_1\rangle^2][\langle r_2^2\rangle-\langle r_2\rangle^2]}} \\ &= \frac{\int_0^\infty r_1 r_2 p(r_1,r_2)dr_1dr_2-\langle r_1\rangle\langle r_2\rangle}{\sqrt{[\langle r_1^2\rangle-\langle r_1\rangle^2][\langle r_2^2\rangle-\langle r_2\rangle^2]}}\end{aligned} \quad (1)$$

where $p(\tau) = \frac{1}{T}e^{-\tau/T}$ is the power delay profile. The signal fading is assumed to obey the Rayleigh distribution, and we can get the approximate expression of the correlation coefficient

$$\rho_r(\Delta f,\tau) \approx \frac{J_0^2(2\pi f_m\tau)}{1+(2\pi\Delta f)^2\sigma_\tau^2} \quad (2)$$

where $J_0(\bullet)$ is the first kind zero-order modified Bessel function,f_m is the maximum Doppler shift.

The correlation coefficient is $\rho_r(\Delta f) \approx \frac{1}{1+(2\pi\Delta f)^2\sigma_\tau^2}$ when τi s zero, and the correlation coefficient is $\rho_r(0,T_C) \approx J_0^2(2\pi f_m T_C)$ when Δf is zero. When the coherence bandwidth is defined with the limitation of $\rho_r(\Delta f) = 0.5$, the coherence bandwidth is $B_C = \frac{1}{2\pi\sigma_\tau}$, and the coherence time is $T_C \approx \frac{9}{16\pi f_m}$ which is inversely proportional to the maximum Doppler shift. It is well known that the CSI remains invariant within the coherence time, otherwise the CSI varies independently.

As a result, we can predict the CSI accurately based on the previously estimated CSI when the time interval and frequency gap are within the channel's coherent time and coherent bandwidth. In this paper, we always assume that the message interval is within the channel's coherent time, and the frequency band used by the same user keeps the same within the same frame duration.

III. CSI PREDICTION-BASED AUTHENTICATION METHOD

A. Method Description

Three-step authentication method is proposed for Bob to identify Alice from Eve. Before the PHY authentication, it is assumed the traditional high layer authentication has successfully authenticated Alice, and Bob has gotten and saved the initial CSI estimate $\boldsymbol{\hbar_{AB}(t)}$ between Alice and Bob at the time t via channel probe method, such as pilot-aided channel estimation. Illegal Eve can make use of the vulnerabilities of existing authentication schemes to pretend to be Alice. At the time $t+\tau$, Bob receives another message, and Bob implements the proposed three-step PHY authentication to identify whether the sender is still Alice.

Step 1: Bob estimates the present CSI $\boldsymbol{\hbar(t+\tau)}$ without knowing the identity of the sender.

Step 2: Bob predicts the present legal channel response $\boldsymbol{\hbar_{AB}(t+\tau)}$ using the saved $\boldsymbol{\hbar_{AB}(t)}$ via prediction method [20][21].

Step 3: Bob decides that the sender is still Alice if $\boldsymbol{\hbar(t+\tau)}$ and $\boldsymbol{\hbar_{AB}(t+\tau)}$ are highly correlated, otherwise Bob declares an intrusion. If the sender is still Alice, Bob saves $\boldsymbol{\hbar(t+\tau)}$ for the following PHY layer authentication.

Implementing this three-step authentication at both Alice and Bob, two-way real-time authentication is achieved.

B. Authentication Determination

Bob can use a hypothesis testing to determine whether current and prior communication attempts are made by the same user via the CSI [17][10]. Due to the noise, estimation error and prediction error exist, and Bob stores a noisy version of vectors $\boldsymbol{\hbar(t+\tau)}$ and $\boldsymbol{\hbar_{AB}(t+\tau)}$,

$$\widetilde{\boldsymbol{\hbar}}\boldsymbol{(t+\tau)} = \boldsymbol{\hbar(t+\tau)} + \boldsymbol{N_1} \quad (3)$$

$$\widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}\boldsymbol{(t+\tau)} = \boldsymbol{\hbar_{AB}(t+\tau)} + \boldsymbol{N_2} \quad (4)$$

where $\boldsymbol{N_1}$ and $\boldsymbol{N_2}$ are independent and identically distributed(i.i.d) complex white Gaussian noise with the same covariance $N(0,\delta^2)$.

We set the null hypothesis

$$\mathscr{H}_0 : \widetilde{\boldsymbol{\hbar}}\boldsymbol{(t+\tau)} = \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}\boldsymbol{(t+\tau)} \quad (5)$$

$$\mathscr{H}_1 : \widetilde{\boldsymbol{\hbar}}\boldsymbol{(t+\tau)} \neq \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}\boldsymbol{(t+\tau)} \quad (6)$$

and test statistic

$$L = \frac{1}{\delta^2}\left\|\widetilde{\boldsymbol{\hbar}}\boldsymbol{(t+\tau)} - \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}\boldsymbol{(t+\tau)}\right\|_2 \quad (7)$$

If the claimant is Alice, $L \sim \chi^2_{2N,0}$, otherwise , $L \sim \chi^2_{2N,delat}$,and $delta = \frac{1}{\delta^2}\left\|\boldsymbol{h_{EB}(t+\tau) - h_{AB}(t+\tau)}\right\|_2$. We define k is the threshold and the rejection region for $\hbar_0$ as $L > k$. Thus, the Type I error is

$$\alpha = P_r\{L > k \mid \mathscr{H}_0\} = 1 - F_{\chi^2_{2N,0}}(k) \quad (8)$$

and the Type II error is

$$\beta = P_r\{L < k \mid \mathscr{H}_1\} = F_{\chi^2_{2N,\mu_L}}(k) \quad (9)$$

therefore the detection rate is $1-\beta$. Where $P_r\{\bullet\}$ is the probability density function.

Next, the mutual information (MI) of the predicted CSI and the estimated CSI can also be used as the measure parameter. MI, from another aspect, is a quantity that measures the mutual dependence of the two variables. So we can use MI to weigh the dependence between the estimated and predicted channel response.

The MI is defined as [17]

$$I(\widetilde{\boldsymbol{\hbar}}, \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}) = H(\widetilde{\boldsymbol{\hbar}}) + H(\widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}) - H(\widetilde{\boldsymbol{\hbar}}, \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}) \quad (10)$$

And we set normalization MI η as

$$\eta = \frac{I(\widetilde{\boldsymbol{\hbar}}, \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}})}{H(\widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}})} \quad (11)$$

If the sender is still Alice and in ideal conditions, we can get $\widetilde{\boldsymbol{\hbar}} = \widetilde{\boldsymbol{\hbar}}_{\boldsymbol{AB}}$, and $\eta = 1$. In practical conditions duo to the presence of noise, η is near to 1. Otherwise will be close to zero.

TABLE I: Parameters for the simulated OFDM system

Item	value	Item	value
Bandwidth: BW	10MHz	OFDM symbol: Ts	100 us
Carrier freq.: f_c	2GHz	Modulation	QPSK
Sampling freq.: f_s	10MHz	Vehicle speed	3, 60, 120 km/h
FFT size: N	1024	Doppler freq.: f_d	17, 333, 666 Hz
No. Tx antenna:	1	No. Rx antenna:	1
Channel estimation:	Least Square (LS)	Channel prediction:	Winner Filter [21]
Channel model:3GPP Veh. A [22]	Relative delay (ns): 0, 310, 710, 1090, 1730, 2510		
	Average power (dB): 0, -1, -9, -10, -15, -20		

IV. Numerical Simulations

A. Simulation system

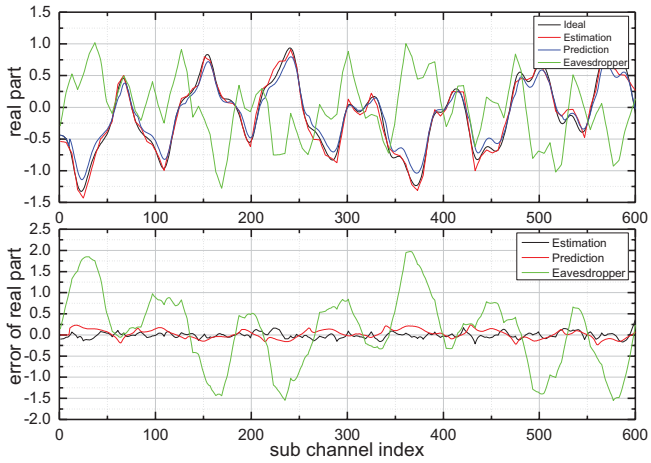
We use MATLAB to implement simulations. The topological structure of the simulated system is shown in Figure 1, and the simulated OFDM system is the third generation long term evolution (3G-LTE) system [18] whose main parameters are listed in Table 1. Vehicular Channel A model from ITU-R M.1225 [22] is adopted, and three types of moving speed are considered to simulate the terminal with low, medium, and high moving speed. Pilot-aided Least Square (LS) algorithm is used to estimate the CSI, and Winner Filter algorithm [21] is adopted to predict the CSI.

B. Simulation results

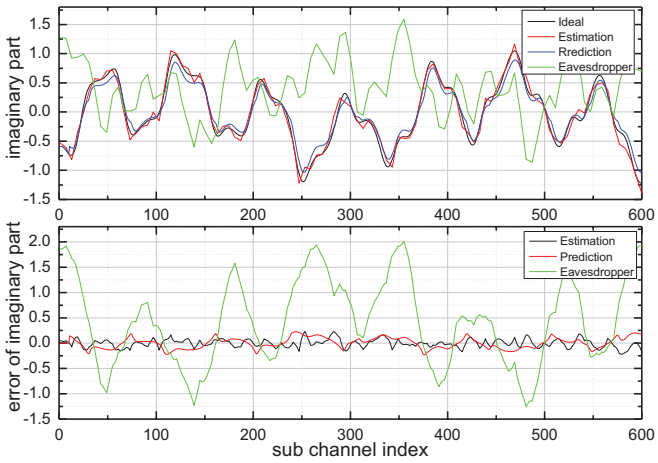
Firstly we testify the correlation of the CSI between the legitimate user and the eavesdropper. The simulation results are presented in Figure 2 and Figure 3. The signal-to-noise ratio (SRN) is 15dB, and the CSIs are compared in Figure 2. It is clear that the estimated and the predicted CSI of the legitimate user are highly correlated with the ideal CSI of the legitimate user, while the CSI of the eavesdropper is much different to the legitimate user's ideal CSI. In Figure 3, we present the correlation of different CSI with the legitimate user's ideal CSI, and we can see that the predicted CSI and estimated CSI of the legitimate user are highly correlated with the ideal CSI, while the eavesdropper's CSI is lowly correlated with the legitimate user's CSI. All these simulate results confirm the CSI can be used to authenticate the access user.

Next we testify the MI of different CSI, and the simulation results are shown in Figure 4. From the figures we can see that both the MI between the estimated CSI and the ideal CSI of the legitimate user and the MI between the predicted CSI and the estimated CSI of legitimate user are much larger than the MI between the predicted CSI and the estimated CSI of the eavesdropper. This observation verifies that the MI can be used to recognize the transmitter.

Last we evaluate the proposed method and compare it with the method proposed in [10][11]. In Figure 5 the detection rate performance is shown when hypothesis testing method is employed to identify the transmitter. From the simulation results it is clear that the proposed method outperforms the reference method in all kinds of scenarios. We also observe that the detection rate of both methods decreases with the increase of vehicle speed due to the channel estimation and prediction are more unreliable when Doppler spread becomes larger and larger, and the reference method degrades more than the proposed method due to the proposed method can track the CSI change and then decreases the error of authentication determination. The detection rate performances are presented in Figure 6 and Figure 7 when MI measure is employed to identify the transmitter in several scenarios. When the MI threshold is set 0.65, the changes of the detection rate performance of the authentication methods at different vehicle



(a) The real part of the channel response.



(b) The imaginary part of the channel response.

Fig. 2: The CSI comparison at SNR=15 dB.

speed are presented in Figure 6. The curves in Figure 6 show the same trend as that in Figure 5, that is the proposed method outperforms the reference method, and as the mobile speed increases the performance gap between the two simulated method becomes larger. In figure 7, we present the detection rate of two authentication methods at mobile speed of 60 km/h while the MI threshold varies from 0.6 to 0.7, and the simulation results show that at the low SNR the proposed method outperforms the reference better.

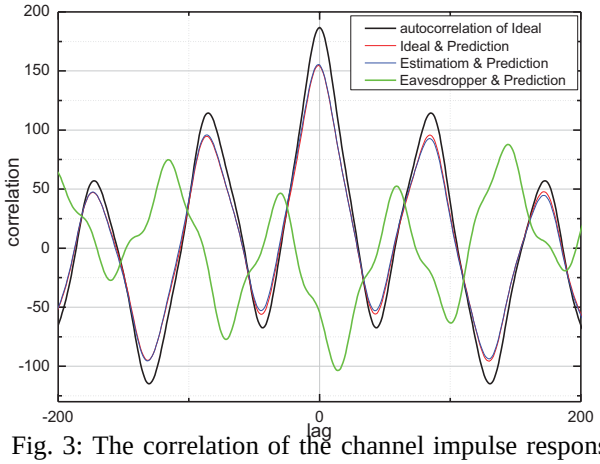


Fig. 3: The correlation of the channel impulse response at SNR=15dB.

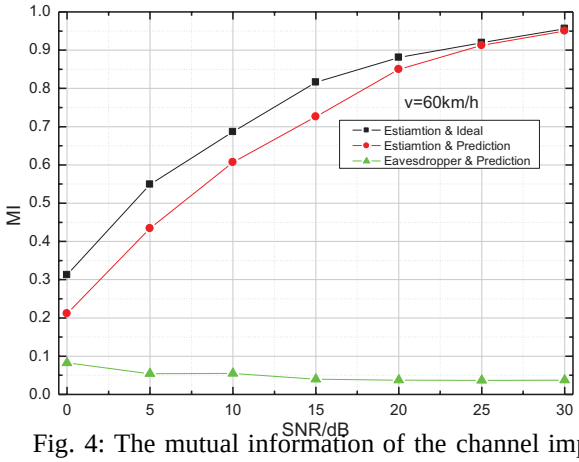


Fig. 4: The mutual information of the channel impulse response.

V. Conclusion

The random channel fading, which causes a big problem for reliable communication, is used to the physical layer security due to its features of randomness and privacy. In this paper, a CSI-based real-time two-way authentication method is proposed in the physical layer to enhance the security. Since the CSI varies continuously, the CSI is reliably predicted from the previous estimated CSI and then compared with the estimated CSI at the next frame after received the frame from the transmitter. By use of hypothesis testing and mutual information method, the reliable discrimination is achieved between a legitimate sender and an intruder or attacker.

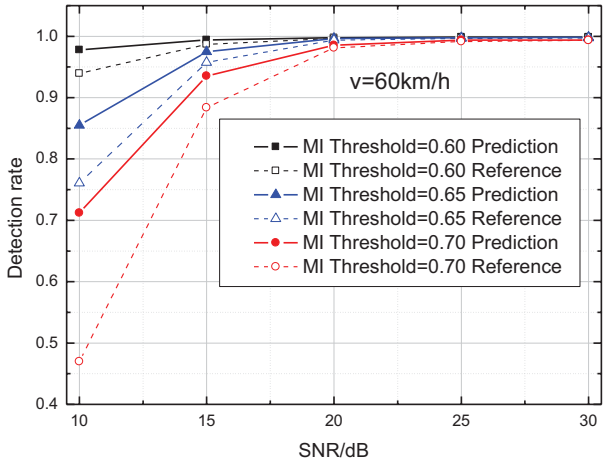


Fig. 5: The detection rate versus signal-to-noise ratio with different thresholds at vehicle speed of 60 km/h when MI measure is employed to authenticate transmitter.

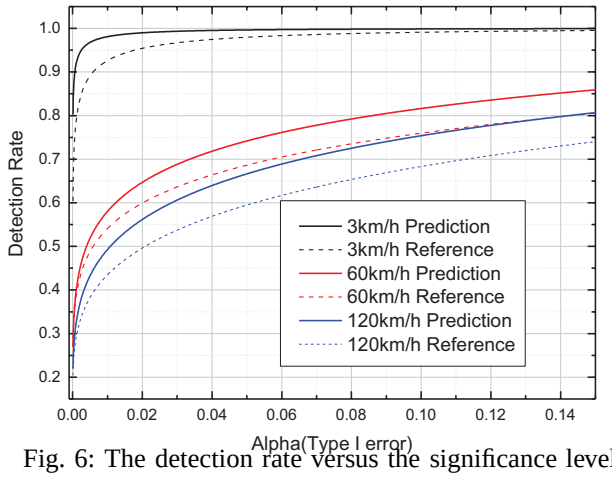


Fig. 6: The detection rate versus the significance level α when hypothesis testing method is employed to authenticate transmitter.

Acknowledgment

This work was supported by the National Key Technology R & D Program of China (Grant No. 2009ZX03005-003-02), the National Science Foundation for Post-doctoral Scientists of China (Grant No. 20110490329) and the Fundamental Research Funds for the Central Universities (2009RC0102).

References

[1] 3GPP, TS33.102 v5.1.0, *"Technical specification group services and system aspects; 3G security; Security architecture (Release 5),"* Dec., 2002.

[2] IEEE 802.16-2009, *"Air interface for broadband wireless access systems,"*May 29, 2009.

[3] IEEE 802.15.4, *"Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs),"* 2003.

[4] ZigBee specification v1.0, *"ZigBee Specification,"* 2005.

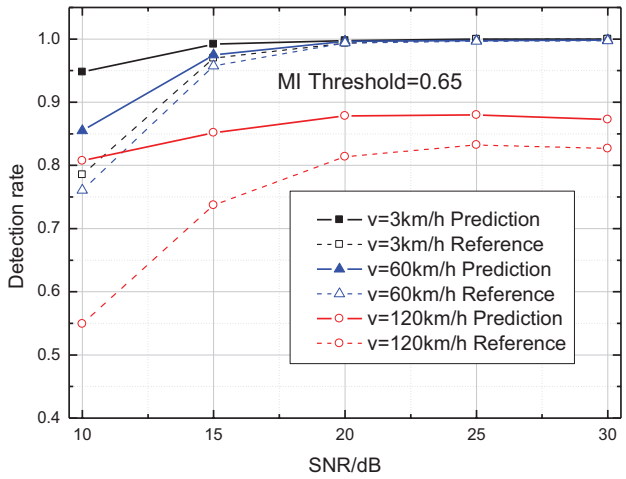


Fig. 7: The detection rate versus signal-to-noise ratio for MI threshold is 0.65 at different vehicle speed when MI measure is employed to authenticate transmitter.

[5] Y. Zhou, Y. Fang, and Y. Zhang, *"Securing wireless sensor networks: a survey,"* IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6-28, 2008.

[6] D. Martins and H. Guyennet, *"Wireless sensor network attacks and security mechanisms: a short survey,"* in Proc. Int. Conf. Network-based Inform. Systems (NBiS), Takayama, Japan, Sep. 14-16, pp. 313-320, 2010.

[7] U. Meyer and S. Wetzel, *"On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks,"* in Proc. Personal, Indoor and Mobile Radio Communications, Barcelona, Spain, Sep. 5-8, pp. 2876-2883, 2004.

[8] K. Bicakci, I. E. Bagci, and B. Tavli, *"Lifetime bounds of wireless sensor networks preserving perfect sink unobservability,"* IEEE Commun. Lett., vol.15, no.2, pp. 205-207, 2011.

[9] D. Faria and D. Cheriton, *"Detecting identity-based attacks in wireless networks using signalprints,"* in Proc. ACM Workshop on Wireless Security (ACM WiSe), Los Angeles, CA, Sept. 29, pp. 43-52, 2006.

[10] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, *"Fingerprints in the ether: Using the physical layer for wireless authentication,"* in Proc. IEEE Int. Conf. Commun. (ICC), Glasgow, Scotland. Jun. 24-28, 2007, pp. 4646-4651.

[11] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, *"Using the physical layer for wireless authentication in time-variant channels,"* IEEE Trans. on Commun, vol. 7, no.7, pp. 2571-2579, 2008.

[12] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, *"A physical-layer technique to enhance authentication for mobile terminals,"* in Proc. IEEE Int. Conf. Commun. (ICC) Beijing, China. May 19-23, 2008, pp. 1520-1524.

[13] Goergen, N., Lin, W.S., Liu, K.J.R., Clancy, T.C., *"Authenticating MIMO Transmissions Using Channel-Like Fingerprinting,"* In Proc. IEEE Global Commun. Conf. (GLOBECOM). Miami, Florida, USA. Dec. 6-10, 2010, pp. 1-6.

[14] Fangming He, Hong Man, Wei Wang, *"Physical layer assisted security for mobile OFDM networks,"* in Proc. Vehicular Networking Conference (VNC). Jersey City, New Jersey, USA, Dec. 13-15, 2010, pp. 346-353.

[15] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, *"Channel-Based Detection of Sybil Attacks in Wireless Networks,"* IEEE Trans. Commun., vol.4, no.3, pp. 492-503, 2007.

[16] A. Goldsmith, *"Wireless Communications,"* Cambridge Press, 2005.

[17] T M. Cover and J A. Thomas, *"Elements of information theory (second edition),"* John Wiley & Sons Publication, New York, USA, 2006.

[18] 3GPP TR 36.814 v1.4.1, "Physical layer aspects (Release 9)," Sept., 2009.

[19] Tugnait, J.K., Hyosung Kim, *"A Channel-Based Hypothesis Testing Approach to Enhance User Authentication in Wireless Networks,"* Communication Systems and Networks (COMSNETS), pp. 1-9, 2010.

[20] J. Li, F. Chen, *"Time-Frequency Joint Channel Prediction Algorithm of MIMO Channel,"* in Proc. ISECS'10,Guangzhou, China, July 29-31, pp. 351-353, 2010.

[21] S. Haykin, *"Adaptive Filter Theory Fourth Edition"*, Pearson Education, July 2002.

[22] ITU-R M.1225, Guidelines for evaluation of radio transmission technologies for IMT-2000, 1997

Xiangyu Lu received his B.S in information and communication engineering from Beijing University of Posts & Telecommunications (BUPT) in 2010, now he is pursuing his M.S. degree in BUPT. His research interest is the physical layer security for wireless communication systems.

Yuyan Zhang received her B.S., M.S, and Ph.D. from BUPT, Beijing, China, in 1986, 1993, and 2006, respectively. She is currently an associate professor at institute of education technology, BUPT, Beijing, China. Her research interests are the key technologies of mobile communications.

Yuexing Peng received his Ph.D degree in information and communication engineering from Southeast University, Nanjing, China, in 2004. From July 2004 to December 2005 he was with CDMA division, ZTE Cooperation as a senior engineer. From January 2006 to April 2008 he was a postdoctoral fellow at the school of information and communication engineering, BUPT. Since May 2008 he has been with the wireless signal processing and network lab, BUPT, Beijing, China. Now he is an associate professor, and his current research interests includes physical layer technologies including security, transmitting & receiving design, wireless sensor network.

Hui Zhao received her M.S in 2003 from Tianjin University and Ph.D. in 2006 from BUPT. Since 2006 she has been with the WSPN lab, and now is an associate professor in BUPT, China. She has published more than 20 papers as well as patent applications, and has taken part in a large number of research projects. Her current research interests include MIMO detection, space-time code design, and adaptive radio transmission techlogies in wireless communication systems.

Wenbo Wang received his B.S., M.S, and Ph.D. from BUPT, Beijing, China, in 1986, 1989, and 1992, respectively. He is currently a professor and the dean of the graduate school, BUPT. Prof. Wang directs the WSPN lab, and has made research on the key technologies of 3G, 3G-LTE, IMT-Advanced, WPAN/WLAN/WMAN, WSN, and wireless ad hoc networks. His research interests include signal processing, mobile communications, cognitive radio.