Physical Layer Technique to Assist Authentication Based on PKI for Vehicular Communication Networks

Hong Wen[1, 2] and Pin-Han Ho[2]
[1] National Key Lab of Communication of UESTC, Chengdu 610054, China
[e-mail: sunlike@uestc.edu.cn]
[2] Department of Electrical Computer Engineering, University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
[e-mail: p4ho@uwaterloo.ca]
*Corresponding author: Hong Wen

Received December 21, 2010; accepted February 6, 2011;
published February 28, 2011

Abstract

In this paper, we introduce a novel Public Key Infrastructure (PKI) based message authentication scheme that takes advantage of temporal and spatial uniqueness in physical layer channel responses for each transmission pair in vehicular communication networks. The proposed scheme aims at achieving fast authentication and minimizing the packet transmission overhead without compromising the security requirements, in which most messages can be authenticated through an extreme fast physical-layer authentication mechanism. We will demonstrate that the proposed secure authentication scheme can achieve very short message delay and reduced communication overhead through extensive analysis and simulation.

Keywords: Physical layer, security, authentication, PKI, channel estimation

The work is partially supported by NSERC Discovery Grant and NSERC SPG when the first author worked at the Dept. of Electrical Computer Engineering, University of Waterloo. The first author also wants to thank the NSFC (Project No. 61032003 and 61071100), NCET (Project No. NCET-09-0266) and NISFPC (No. 2011ZX03002-005-03) for their support for this research.

DOI: 10.3837/tiis.2011.02.012

1. Introduction

AVehicular Ad hoc Networks (VANETs) is a type of mobile ad hoc networks where each vehicle serves as a node interconnected by wireless links. One of the most important features in VANETs is that each vehicle can only move in a predictable manner while at much higher speeds compared with the traditional Mobile Ad-hoc Networks (MANETs). The Dedicated Short Range Communication (DSRC) standard [1], which is currently under extensively development by the IEEE 802.11p [2] standardization committee, defines two types of communication in VANETs: vehicle- to-vehicle (V2V) and vehicle-to-infrastructure (V2I). DSRC is committed to support a suite of safety applications such as collision warning, up-to-date traffic information, and active navigation and infotainment. With DSRC, each vehicle on the road is broadcasting routine traffic related messages with the information of position, current time instance, driving direction, speed, acceleration/deceleration, and possible traffic conditions. In addition to the safety messages, emergency messages are defined and sent when any abnormal situation and driving condition of the car is identified, such as emergent braking, flat tire warning, and the detection of sleeping status of the driver. By frequently broadcasting and receiving routine traffic related messages, drivers can get better awareness of their driving environment. Early actions can be taken to respond to an abnormal situation to avoid any possible damage or to follow a better route by circumventing a traffic bottleneck [8]. Certainly, VANETs can also be used to collect the city traffic information and report to the traffic management center, which serves as an active role in an Intelligent Transportation System (ITS).

The creation of VANETs is obviously a great plus to the traffic management and road driving safety. However, any malicious behavior of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to the other users, and should be identified and rejected from the networks [4]. One of the main challenges of securing VANETs is source authentication that enables receivers to verify the identity of the sender of the received data. A well-recognized solution is to deploy Public Key Infrastructure (PKI) [3] such that every vehicle is equipped with one or a number of public-private key pairs. However, due to the intermittent communication memory storage constraints in VANETs, classic PKI-based security schemes are subject to further elaboration in order to satisfy the extremely dynamic network environment and the design requirements specific in the vehicular communication scenario. To provide an effective certificate service for VANETs, it is required for each the On-Board Unit (OBU) to efficiently update its certificate anytime and anywhere in a timely manner.

Recently, many researchers have turned to using physical layer information to enhance wireless security [10][11][12], and channel responses between communication peers have been explored as a form of fingerprint in the scenario of wireless security [13][14][15]. In these studies, physical layer authentication is performed by comparing a measured (test) channel response with a prior channel response to discriminate between transmitters at different locations. In [13][14], the authors introduced a physical layer algorithm that integrates a suite channel probing mechanisms with hypothesis testing to determine whether the current and prior communication attempts are made by the same user. Their studies were based on a generalized channel response with both spatial and temporal variability, and consider correlations in the time, frequency and spatial domains.

With physical layer authentication, a channel response is extracted and used to estimate the channel information before the signals received. It has been envisioned that the physical layer security mechanisms are promising to achieve fast authentication and low overhead in the future communication networks, particularly in a highly dynamic networking environment like VANETs. Therefore in this paper, we explore the potential possibility of using physical-layer channel responses as authenticators between each communication pair, and propose a novel message authentication scheme call Physical layer Assisted Authentication (PAA) in a PKI environment for VANETs, in order to cope with the stringent requirements on message authentication delay and communication overhead. We take advantage of the spatial and temporal uniqueness of Physical layer (PHY) channel responses of each communication pair, and demonstrate that a receiver can take its PHY measurement to discriminate one transmitter from the others for a train of messages. We will show that such a PHY-assisted authentication mechanism can be taken for achieving fast and efficiency message authentication. The proposed PAA approach has each vehicle pre-loaded with public keys of other vehicles to access the communication networks. Additionally, each vehicle extracts and stores the channel responses of all its surrounding vehicles. Thus, after receiving the first message that requires to be authenticated via the conventional process, the subsequent messages can be authenticated by mapping the stored channel and the estimated channel responses. Specifically to 802.11p based VANETs, we use the preamble of each Orthogonal Frequency-Division Multiplexing (OFDM) packet for channel estimation, where no extra bandwidth or transmission power will be consumed.

The rest of the paper is organized as follows. Section 2 gives a brief view about the related work. Section 3 presents a previously reported physical layer authentication mechanism and our extended mechanism that serve as a building block of the study. Section 4 describes in detail the proposal PAA protocol. Section 5 demonstrates our methodology for simulation and the resultant simulation results that verify the proposed protocol and methods. Section 6 concludes the paper.

2. Related Work

The authentication and certificate services for VANETs have been extensively studied in the past. In [3], Hubaux et al. identified the specific issues of security and privacy challenges in VANETs, and claimed that PKI should be deployed to authenticate each received message and to mutually authenticate among network entities. Raya et al. [4] proposed a PKI-based security and privacy protocol, where each vehicle is pre-loaded a pool of anonymous public/private keys in order to achieve user location privacy. To allow the trust authority to trace the sender identity of each launched message, the trusted authority has to store all the certificates of each vehicle, which incurs inefficiency for certificate management. In [5], an approach to implement privacy in VANETs was presented by using geo-bounded pseudonyms and a trusted-third party.

Another PKI based architecture for authentication and authorization was proposed using the Kerberos model by Moustafa et al. [6]. Based on batch verification signatures, C. Zhang et al. [7] introduced an efficient batch signature verification scheme for communications between vehicles and Roadside Units (RSUs). Nonetheless, the authors did not investigate the scenario where any illegitimate signature is in the batch such that all the other legitimate signatures have to be re-examined. The same authors as [7] introduced a fast signature authentication scheme, called RAISE [9], where Message Authentication Code (MAC) can be

used for inter-vehicle authentication under the aid of an RSUs. This is considered as a solid solution for solving the scalability issues of signature authentication for VANETs.

Lin et al. [8] proposed a Timed efficient and Secure Vehicular Communication (TSVC) scheme by using the one-way hash chain. With TSVC, each receiver only needs to go through the conventional authentication process when verifying the first message, while the subsequent messages can be verified through a hash function. Thus, extremely short delay and little communication overhead can be achieved as if a symmetric key communication is taking place. However, the biggest problem of TSVC is that the group of vehicles has to be highly synchronized, which is not feasible in a dynamic ad hoc networking environment like VANETs. Furthermore, how to group the vehicles and how to define the boundary of each group become other challenging issues that could hinder the practical implementation of the scheme. Obviously, it is still an open question on how to perform message authentication under PKI in a scalable and efficient way for VANETs.

3. Physical Layer Authentication

3.1 System Model

We consider the scenario illustrated in Fig. 1 by taking the conventional terminology widely used in the security community for three different parties in a secure multicast scenario: a sender, multiple receivers, and Eavesdroppers (Eves). These three entities could also be taken as a wireless transmitter and a number of receivers that are potentially located in spatially separated positions. In our paper, the sender serves as the transmitter that initiates communication with the receivers, while Eve is an active opponent who injects undesirable signals into the medium in the hopes of spoofing the sender. Our security objective is to provide authentication between the sender and the legal receivers, in which the legal receivers have to differentiate a signal launched by the sender from that by Eve. To achieve this, each information-carrying transmission is accompanied with the channel response at the sender, which serves as an authenticator signal for the receivers to verify the legitimacy of the transmission. With the authenticator signal, each receiver authenticates the transmission by comparing the authenticator signal with the estimated channel response. If the two channel estimates are "close" to each other, the receiver 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 the receiver will reject the message.

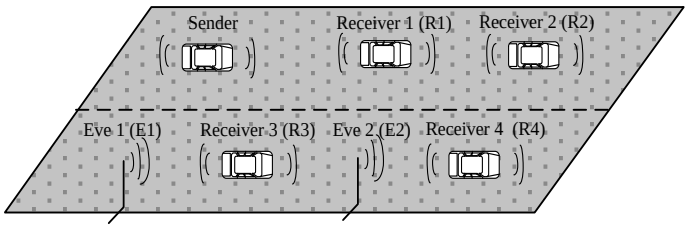

Fig. 1. Scenario with sender, receivers and Eves.

Suppose the source sends a signal to the receivers with the frame structure shown in **Fig. 2**, where we consider a cyclic prefix (CP) Orthogonal Frequency-Division Multiplexing (OFDM) system with M subcarriers and total transmit bandwidth B. The duration of one

OFDM symbol is *T*. A packet consists of frames N_x, which consist of N_d OFDM data symbols and one pilot in each subcarrier. The corresponding system model is then given by

$$Y_k(n,m) = H_k(n,m)X_k(n,m) + Z_k(n,m) \tag{1}$$

where $k \in \{1,2,\cdots N_x\}$, $n \in \{1,2,\cdots N_d\}$ and $m \in \{1,2,\cdots M\}$ are the frame index, the symbol index and subcarrier index, respectively; furthermore, $Y_k(n,m)$ and $X_k(n,m)$ are the receive and transmit symbols, respectively, $H_k(n,m)$ denotes the channel coefficients, and $Z_k(n,m)$ is additive white Gaussian noise with variance σ_Z^2. We consider time-varying Rayleigh fading channel. The channel time-frequency domain coefficient $H_k(n,m)$ are related to the delay-Doppler spreading function $S_k(n,m)$ of the channel via a 2-D Fourier transform [17],

$$H_k(n,m) = \frac{1}{\sqrt{MN_d}} \sum_{\tau=0}^{M_\tau - 1} \sum_{l=-\frac{M_v}{2}}^{\frac{M_v}{2}} S_k(n,m) e^{-j2\pi\left(\frac{m\tau}{M} - \frac{nl}{N_d}\right)} \tag{2}$$

where τ, l denote discrete delay and discrete Doppler, respectively. M_τ dentotes the channel's maximum delay spread and M_v characterizes the maximum Doppler spread. Since in practice $M_\tau \ll M$ and $M_v \ll N_d$, $H_k(n,m)$ is a 2-D lowpass function.

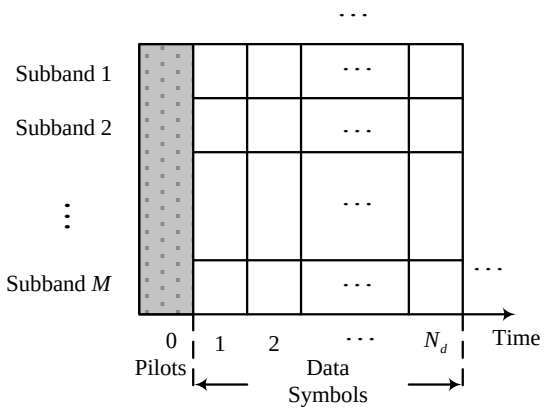

Fig. 2. Frame structure of the transmission from the sender to the receivers.

3.2 Physical Layer Authentication Based on Likelihood Ratio Test

In this section, we briefly review some facts about the Physical Layer Authentication (PLA) scheme introduced by L. Xiao *et al*. [13][14][15]. The receivers use the pilots for channel estimation, which can come up with the test vectors as follows

$$\hat{\underline{H}}_k(n) = \left[H_k(n,1), H_k(n,2), \cdots, H_k(n,M) \right]^T \tag{3}$$

where *k* is the frame index, *M* is the number of subcarriers and *n* is OFDM symbol index. For convenience, the index *n* is omitted. Then Eq. (3) could be rewritten as:

$$\hat{\underline{H}}_k = \left[H_k(1), H_k(2), \cdots, H_k(M) \right]^T \tag{4}$$

The receiver uses channel estimates in two consecutive frames, $\hat{\underline{H}}_{k-1}$ and $\hat{\underline{H}}_k$, to determine

whether they are from the same transmitter (sender) or not. The receiver is assumed to obtain the sender-receiver channel gain in the previous frame, $\hat{\underline{H}}_{k-1}$, and can compare it with the current channel gain, $\hat{\underline{H}}_k$, to determine whether the current received frame is from a common transmitter that has launched the previous one. $\hat{\underline{H}}_{k-1}$ and $\hat{\underline{H}}_k$ can be estimated by Iterative Least Square (ILS) channel estimation [22] and Minimum Mean-Square Error (MMSE) [20] channel estimation methods. In the null hypothesis, H_0, the claimant is the original send. Otherwise, in the alternative hypothesis, H_1, the claimant terminal is someone else. The notation $\sim$ is used to denote accurate values without measurement error, and thus have:

$$\begin{aligned} H_0: &\quad \tilde{\underline{H}}_k \to \tilde{\underline{H}}_{k-1} \\ H_1: &\quad \tilde{\underline{H}}_k \mapsto \tilde{\underline{H}}_{k-1} \end{aligned} \tag{5}$$

We normalize the likelihood ratio test (LRT) statistic as:

$$\Lambda_0 = \frac{K_{co}\left\|\hat{\underline{\tilde{H}}}_k(i) - \underline{H}_{k-1}(i)e^{j\varphi}\right\|^2}{\left\|\hat{\underline{H}}_{k-1}(i)\right\|^2} \begin{matrix} >H_1 \\ <H_0 \end{matrix} \eta \tag{6}$$

where $\hat{\underline{H}}_k$ represents the channel response with measurement errors; K_{co} is the normalization factor and let $\eta \in [0,1]$.

As mentioned in reference [13], the authentication scheme depends on the richly scattered multipath environment. Because the received signal rapidly decorrelates over a distance of roughly half a wavelengths and the spatial separation of one to two wavelengths is sufficient for assuming independent fading paths, the time interval of two continuous authentication procedures should be less than the channel's coherence time τ.

3.3 Physical Layer Authentication Based on Sequential Probability Ratio Test

In this section, we developed the PAA scheme by the sequential probability ratio test (SPRT), which was initially introduced by Abraham Wald [23] as a hypothesis test for sequential analysis. The SPRT considers sequential sample units as a statistical test. LRT only compares the estimation in the *k*-th frame ($\hat{\underline{H}}_k$) with that in the (*k*-1)-th frame ($\hat{\underline{H}}_{k-1}$). A sequential probablility ratio test can compare ($\hat{\underline{H}}_k$) with all past records ($\hat{\underline{H}}_i$) where $i < k$ in some way which may yield a better detection rate. So it is possible that SPRT is better than the simple LRT. Let ith statistical test the log-likelihood ratio as:

$$\Lambda_i = \frac{K_{co}\left\|\hat{\underline{\tilde{H}}}_{k-i+1}(i) - \underline{H}_{k-i}(i)e^{j\varphi}\right\|^2}{\left\|\hat{\underline{H}}_{k-i}(i)\right\|^2}, \quad i = 1,2,\cdots,S \tag{7}$$

where $S \geq 1$. Then we calculate the cumulative sum of the log-likelihood ratio Λ as:

$$\Lambda = K_{co\_S}\sum_{i=1}^{S}\Lambda_i \begin{matrix} >H_1 \\ <H_0 \end{matrix} \delta \tag{8}$$

where K_{co_S} is the normalization factor to let the threshold $\delta \in [0,1]$. Because the channel response may change with time due to change in the environment, it is necessary to guarantee the time intervals of the continuous authentication procedure less than the channel's coherence time τ. The number of the statistical test cumulative sum *S* in Eq. (7) and Eq. (8) has to be set as $t_k - t_{k-s} < \tau$, *i.e.* *S* time intervals is less than the channel's coherence time τ.

4. PHY-Assisted Authentication Scheme Based on PKI

In this section, the proposed PHY-Assisted Authentication (PAA) scheme for VANETs based on DSRC and IEEE802.11p [2] is presented as follows. We will first describe how the proposed scheme takes advantage of the 802.11p standard, followed by the protocol stack in the MAC layer of each vehicle.

4.1 IEEE 802.11p Support

The IEEE 802.11p has constructed an OFDM-based PHY layer to operate in the 5.85-5.925 GHz unlicensed national information infrastructure band with 10 MHz bandwidth. Fig.3 shows the block diagram of IEEE 802.11p system model, where a 64-subcarrier OFDM system is employed. Among the 64 subcarriers, 52 are used for data transmission, which is further composed of 48 data subcarriers and 4 pilot subcarriers. The pilot signals are used for tracing the frequency offset and phase noise. Fig. 4 shows the frame format which consists of the OFDM Physical Layer Convergence Protocol (PLCP) preamble, PLCP header, PLCP Service Data Unit (PSDU), tail bits, and pad bits. In the PLCP preamble field shown in Fig. 5, the preamble consists of 10 identical short training symbols and 2 identical long training symbols. The short training symbols and long training symbols, which are located in the preamble at the beginning of every PHY data packet, are used for signal detection, coarse frequency offset estimation, time synchronization, and channel estimation. A guard time GI, is attached to each data OFDM symbol in order to eliminate the Inter Symbol Interference introduced by the multi-path propagation. The proposed PAA scheme utilizes the two long training symbols pilot signal for channel estimation.

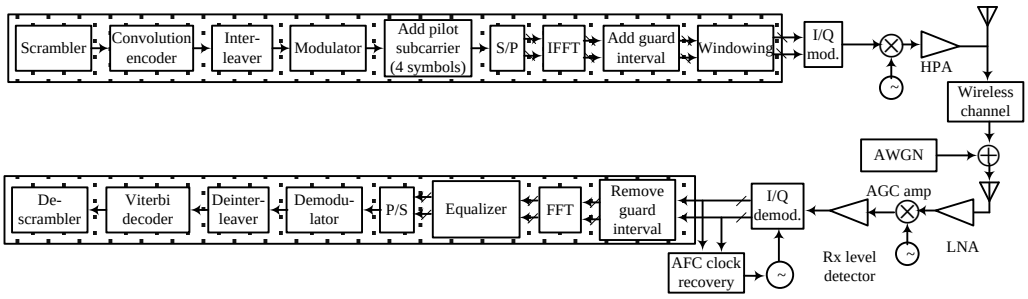

Fig. 3. System model of IEEE802.11p physical layer.

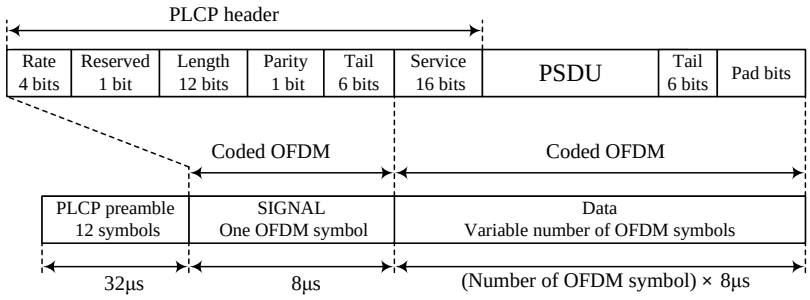

Fig. 4. The frame format of IEEE 802.11p(Transmission packet details).

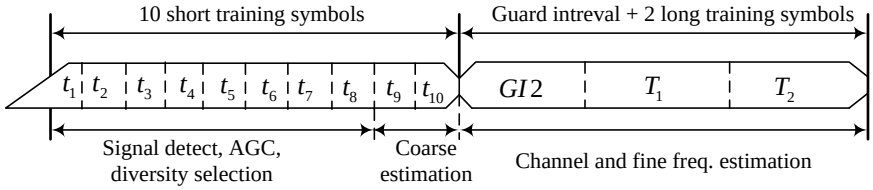

Fig. 5. Preamble structure of IEEE802.11p.

4.2 Scheme Descriptions

Let all the vehicles be installed with a list of anonymous public/private key pairs $\langle PK_i, SK_i \rangle$ in the vehicle registration phase or annual check-up, where the corresponding anonymous certificates are $Cert_i$ with pseudo identities $PVID_i$ as its certificate identities [4]. For the purpose of traceability, vehicle registration authority keeps records of those anonymous certificates and their corresponding real identities. Each pair of keys has a short life time, e.g., a few minutes. A sender sends the first massage to the receivers. A signature is produced for the first message with the conventional public key signature technique. Then the receiver estimates the channel response $\hat{\underline{H}}_1$ by packet pilot [2] which originally was designed to serve as the channel estimation and save it. For the following messages, the receiver estimates the channel response $\hat{\underline{H}}_i$ by packet pilot and compare with $\hat{\underline{H}}_{i-1}$ according to Eq. (6) or Eq. (8). If the message verifies successfully, the receiver saves $\hat{\underline{H}}_i$ instead of $\hat{\underline{H}}_{i-1}$ for the next packet authentication. If the message do not verify successfully, the receiver drops the message and picks up another public/private key pairs and initiates new PAA scheme again.

Let the routine messages sent by a vehicle be denoted as $X_1, X_2, \cdots, X_N$, and X_i is transmitting packet. The proposed security scheme is shown in **Fig. 6**. For an arbitrary sender *V*, before it sends the first message, it signs the hashed message with its private key SK_V and includes the certification authority's certificate $Cert_V$ as follows:

$$P_1 = \langle PVID,\ X_1,\ Sig_{SK_V}[X_1 | T_1],\ Cert_V \rangle \tag{9}$$

where *PV ID* is the pseudo *ID* of the sender *V*, which is kept in accordance with the *ID* that is being used in the current public key certificate $Cert_V$ that is the currently used anonymous public key certificate; *j* is the concatenation operator, and T_1 is the time when the sender sends

the packet, which is used to defeat replay attack. When the sender sends the following messages, he directly picks up the packet X_1 without any authentication tag.

The receivers of the first message have to extract the public key of *V* using the certificate, and then verify *V*'s signature using its certified public key. The first message will go through a complete authentication process via the conventional PKI mechanism. With the first message fully authenticated, the receivers perform channel estimation, extract and save the channel responses with the sender $\hat{\underline{H}}_1$. For each of the subsequent messages, the receivers perform channel estimation $\hat{\underline{H}}_i$ according the currently received message, and compare it with the channel response $\hat{\underline{H}}_{i-1}, \underline{H}_{i-2}, \cdots, \underline{H}_{i-S}$ of the previously received *S* frame messages, where the physical layer authentication is performed according to Eq. (8). The physical layer authentication will be performed according to Eq. (6) if *S* equals to 1. In case the verification fails, the packet is dropped. Otherwise, the receiver updates the entry $\left(packet\#, \hat{\underline{H}}_i, lifetime\right)$ in its local cache table corresponding to the sender *V*, which maintains the packet index, channel response, and lifetime which serves as a timer controlling how long the entry is active. If the timer hits 0, another freshness process in Eq. (9) has to be done again. As mentioned earlier, when the time interval of two continuous authentication procedures is larger than the channel's coherence time, the received signals decorrelates each other. So the receiver needs to check whether the time interval $t_i - t_{i-1}$ between two slots is larger than the channel's coherence time τ after the verification successfully, if the test statistic Eq. (6) is used. If we use Eq. (8) as the test statistic, the receiver needs to check whether the *S* larger than 1 after the verification successfully. When $t_i - t_{i-1} < \tau$ or $S \geq 1$ hold, the authentication procedure continues. Otherwise, the send has to refresh the process in Eq. (9) and initiates new PAA scheme again. The proposed PAA authentication scheme is shown in **Fig. 6**.

To summarize, the proposed PAA scheme builds a trust connection between the sender and receiver by comparing the channel response of the currently received message with the channel estimation of the previously received message. It is possible that a receiver loses the trust connection with the sender due to false positive. Similar to TSVC or any other TESLA-based approach, in such a circumstance the receiver has to wait for the next message that can be fully authenticated from the sender in order to restore the trust connection. The analysis and optimization on the period of broadcasting the fully authenticated message is considered out of scope of the current study, and will be focused in our future research.

5. Simulation Results

Simulation is conducted to verify the proposed PAA approach by collecting the PHY layer channel response from the two long training symbols in the pilot signal of each 802.11 frame. We set the simulation parameters as follows. There are *M*=52 sub-carriers which consists of $N_d = 60$ OFDM symbols, bandwidth *B*=10MHz, and carrier frequency f_c=5.9GHz. The maximum delay spread is 200ns corresponding to $M_\tau = 4$. The discrete Doppler spread M_v is determined as:

$$M_v = 2\left\lceil \frac{\omega_d}{B} \times M \times N_d \right\rceil \tag{10}$$

where ω_d is the maximum Doppler frequency in Hertz given by $\omega_d = f_c v_{\max} / c_0$, with $v_{\max}$ denoting the maximum terminal velocity, f_c being the carrier frequency, and c_0 denoting the speed of light. To estimate $\hat{\underline{H}}_k$ in Eq. (6) and Eq. (7), both Iterative Least Square (ILS) channel estimation method [22] and Minimum Mean-Square Error (MMSE) [20] channel estimation method are examined. Typically, four iterations were performed in the ILS estimation method. In Eq. (6) and Eq. (8), because the threshold η and δ have no closed-form expression, it has to be determined by simulations according to the false alarm α and the detection rate β, which are given by

$$\begin{aligned} \alpha(\eta) &= P\left[\Lambda_0 > \eta \middle| H_0\right] \quad or \quad \alpha(\delta) = P\left[\Lambda_0 > \delta \middle| H_0\right] \\ \beta(\eta) &= P\left[\Lambda_0 < \eta \middle| H_0\right] \quad or \quad \beta(\delta) = P\left[\Lambda_0 < \delta \middle| H_0\right] \end{aligned} \tag{11}$$

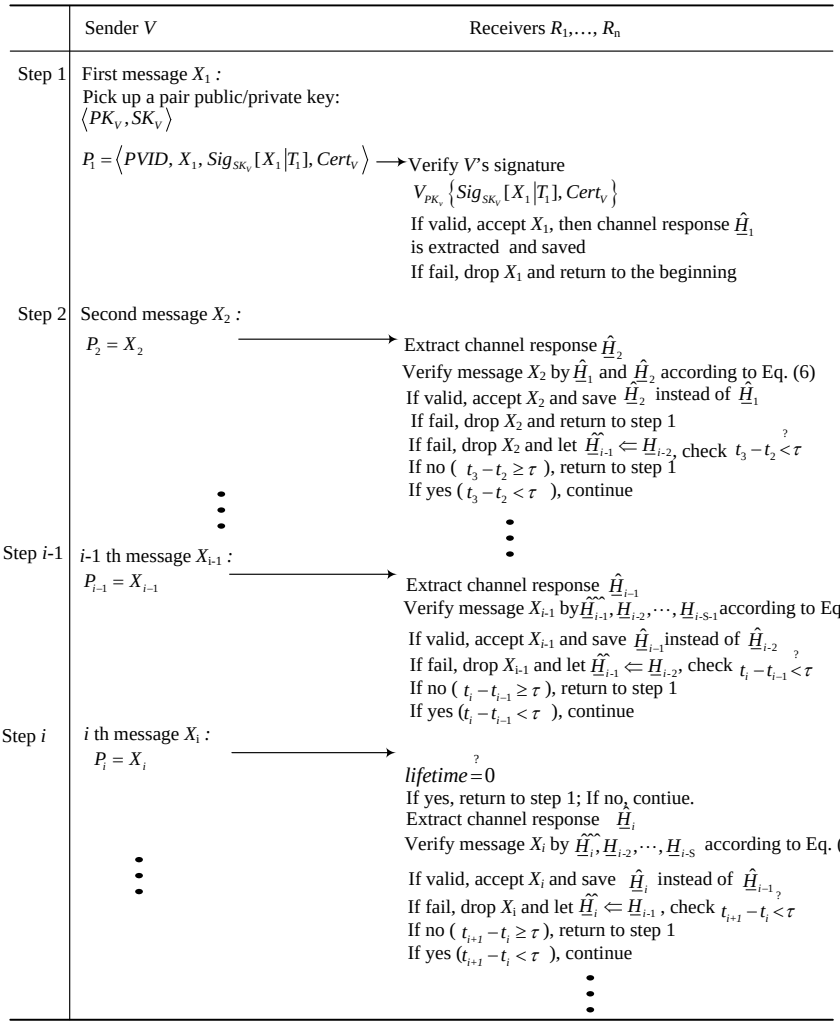

Fig. 6. The proposed security scheme.

In an urban road environment, we let false alarm rate $\alpha < 0.05$, the threshold $\eta = 0.05$ and $\delta = 0.05$, and the distance between vehicles are 25 meters. **Fig. 7** shows the receiver operation characteristic curves by using the two different estimation methods and two different test statistic in Eq. (6) and Eq. (8). From the simulation results, we can conclude that the detection rate of the MMSE estimation method and SPRT test statistic are a little bit higher than that by the ILS estimation method and LRT test statistic. With a higher vehicle moving speed, the detection rate decreases accordingly. The detection rate and false alarm rate of a receiver under different moving speeds of the vehicles and different estimation methods are illustrated in **Fig. 8**. Further, simulation is conducted to investigate the relationship between the threshold $\eta(\delta)$ and the moving speed of vehicles under a given detection rate $\beta \geq 0.98$. **Fig. 9** illustrates the results of threshold $\eta(\delta)$) as a function of the vehicles moving speed.

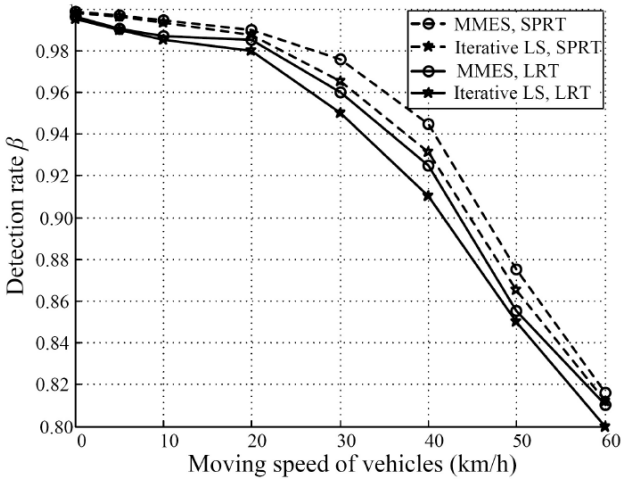

Fig. 7. The receiver operation characteristic curves.

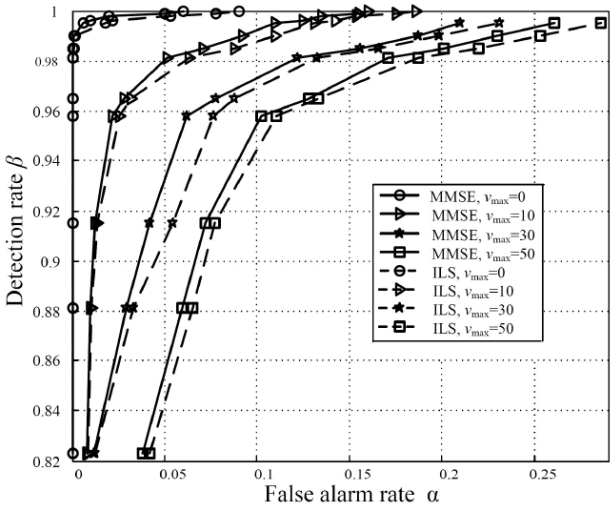

Fig. 8. The detection rate and false alarm rate of the receiver under different moving speed of the vehicles and different estimation methods.

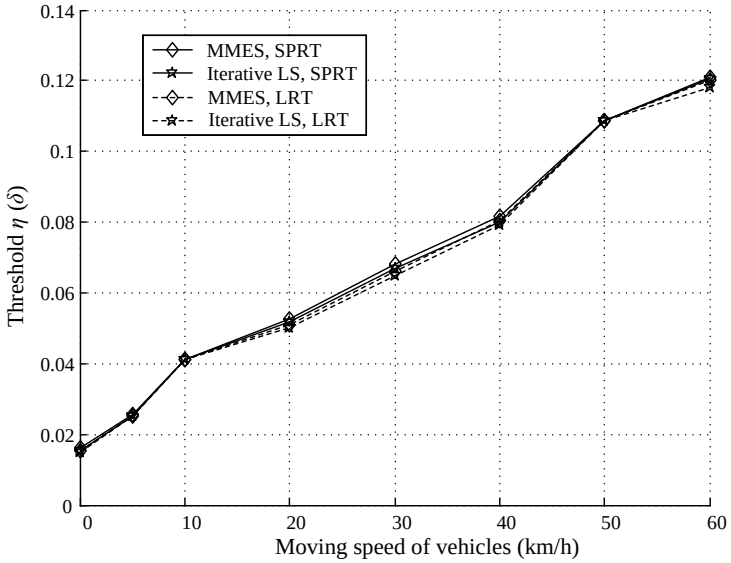

Fig. 9. The threshold as a function of the vehicles moving speed.

To research whether the proposed scheme can work well when the route of the transmitter changes, we give two different scenarios in **Fig. 10** and **11**, in which the senders change the lines or direction. The correspondence parameters are illustrated in **Table 1** and **Table 2**. We assume that the road environment is urban road and let the false alarm rate $\alpha < 0.05$, the threshold $\eta = 0.05$ and $\delta = 0.05$. The MMSE channel estimation method are used. The detection rate of the receivers under different moving speeds of the vehicles and different test statistic methods are illustrated in **Fig. 12** and **Fig. 13**. From the simulation results, we can conclude that the detection rate of the receivers drops with moving speed increasing and the receivers yields the lower detection rate in scenario II than in scenario I.

Table 1. Parameters for **Fig. 10**.

	$l_1(m)$	λ_1	λ_2
Model1_1	30	100^{o}	100^{o}
Model1_2	60	120^{o}	120^{o}
Model1_3	150	150^{o}	150^{o}

Table 2. Parameters for **Fig. 11**.

	$L_1(m)$	$L_2(m)$
Model2_1	50	100
Model2_2	100	200
Model2_3	150	300

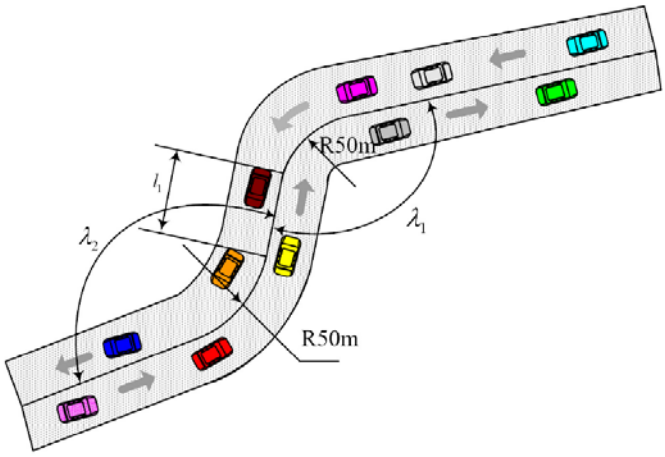

Fig. 10. The sender changes the route----scenario I.

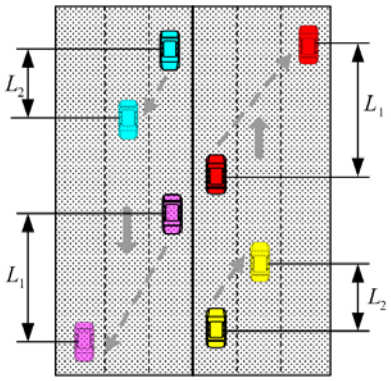

Fig. 11. The sender changes the route----scenario II.

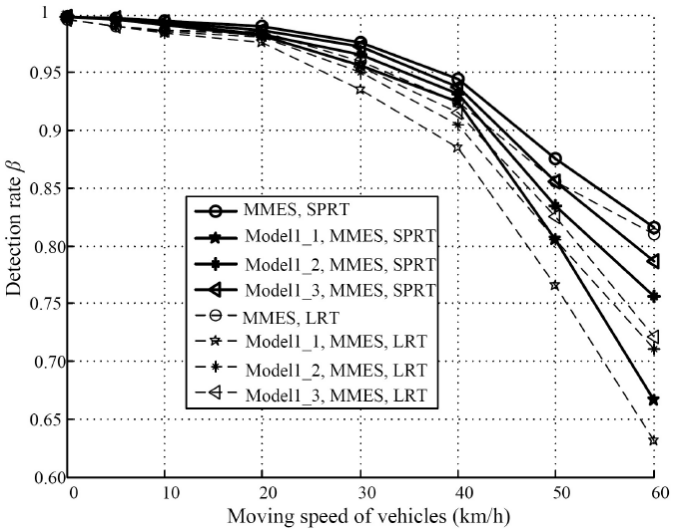

Fig. 12. The detection rate of the receivers under different moving speed of the vehicles and different test statistic methods when the sender changes route----scenario I.

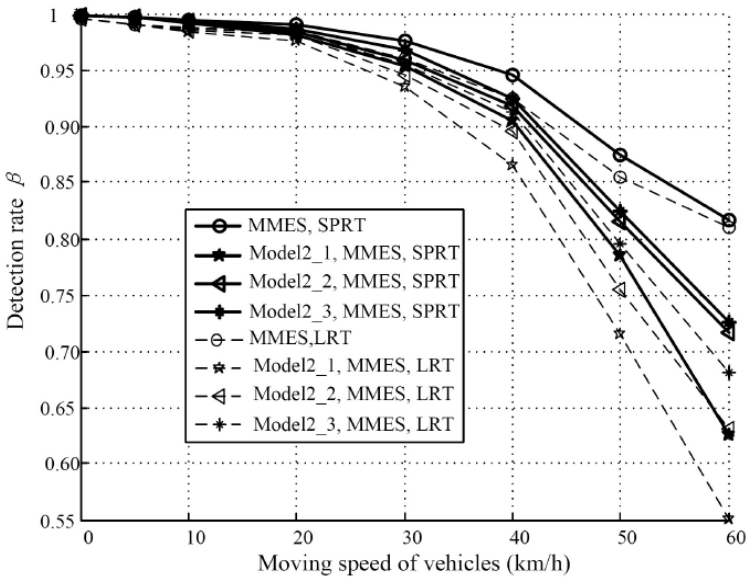

Fig. 13. The detection rate of the receivers under different moving speed of the vehicles and different test statistic methods when the sender changes route----scenario II.

The current DSRC protocol is working at the 5.9 GHz in which the wavelength is 0.05 metres. Because of the spatial uniqueness of Physical layer (PHY) channel responses, the channel response will change if the distance between two sender is larger than 0.05 metres. **Fig 14** illustrated the attacking results with different distance between Eve and the sender (in **Fig 1**).

The comparison of several authentication schemes is shown in **Fig. 15**, which shows that the proposed PAA scheme yields the lowest time delay for authenticating each message. Note that the simulation result was derived by jointly considering the false positive and detection mismatch due to unexpected channel fluctuation.

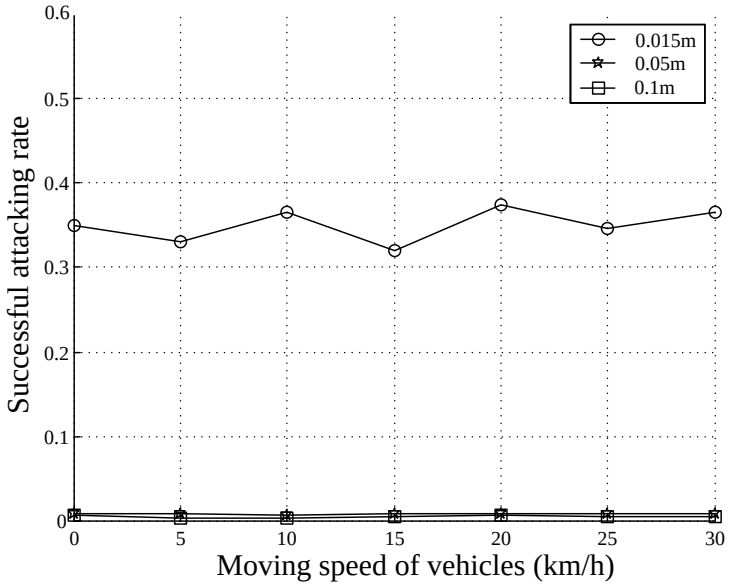

Fig. 14. The attacking rate with ifferent distance between Eve and the sender.

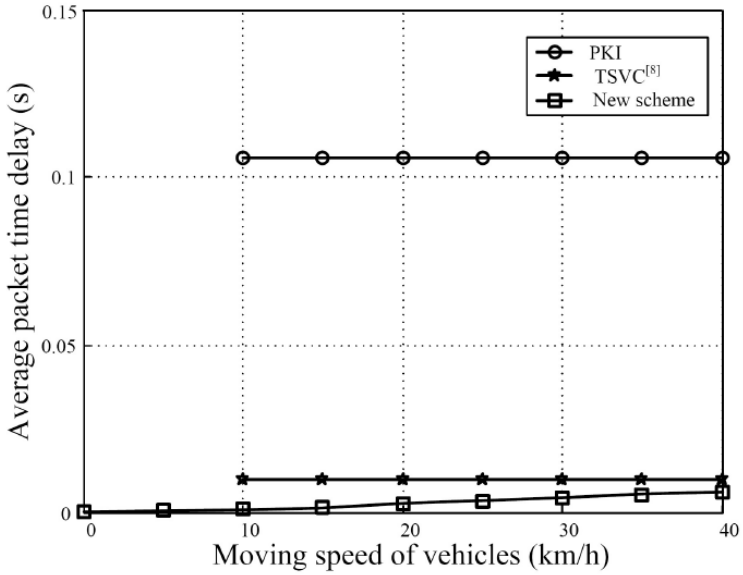

Fig. 15. The comparison of three authentication schemes.

6. Conclusions

In this paper, a novel Physical layer Assisted Authentication (PAA) security scheme has been introduced for vehicular communications under PKI, which aims to achieve high efficiency in terms of packet overhead incurred in the message authentication scheme and computation latency. We claim that the proposed PAA scheme serves as a framework for message authentication in a highly dynamic network, and can overcome a number of legacy problems in the conventional TESLA-based message authentication approaches. The proposed PAA protocol can achieve the fast and light-weight message authentication process and does not need synchronization among a group of vehicles as that required by the TSVC scheme or any other Timed Efficient Stream Loss-tolerant Authentication (TESLA) based schemes. Further, the proposed PAA approach does not involve the concept of vehicle grouping, where a newly joined vehicle or any vehicle that lost the trust connection will wait for the next arriving authentication message.

We verified the proposed PAA scheme in typical urban road environments, where the pilot signals of IEEE 802.11p frames are employed for channel response acquisition and estimation. The results demonstrated the merits of the PAA scheme by comparing with a number of existing messages authentication methods. Our future research will be on the analytical modeling on the performance of the proposed PAA as well as the optimization for the period of sending a fully authenticated message.

References

[1] Cseh C., "Architecture of the dedicated short-range communications (DSRC) protocol," in *Proc. of Vehicular Technology Conference, VTC 98. 48th IEEE*, vol. 3, pp. 2095 – 2099, 2007. Article (CrossRef Link)

[2] Task Group p, "IEEE P802.11p: Draft Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific

requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," *IEEE Computer Society*, Jun. 2009. Article (CrossRef Link)
[3] J.P. Hubaux, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 2, pp. 49-55, 2004. Article (CrossRef Link)
[4] M. Raya and J.P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007. Article (CrossRef Link)
[5] F. Dotzer, "Privacy issues in vehicular ad hoc networks," in *Proc. of ACM Workshop on Vehicular Ad Hoc Networks*, September 2006. Article (CrossRef Link)
[6] H. Moustafa, G. Bourdon and Y. Gourhant, "AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture," in *Proc. of ACM workshop on Vehicular ad hoc networks*, pp. 79-80, 2005. Article (CrossRef Link)
[7] C. Zhang, R. Lu, X. Lin, Pin-Han Ho and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," in *Proc. of IEEE INFOCOM*, pp. 246 - 250, 2008. Article (CrossRef Link)
[8] X. Lin, X. Sun, X. Wang, C. Zhang, Pin-Han Ho and X. Shen, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving," *IEEE Trans. on Wireless Communications*, vol. 7, no. 12, pp.4987-4998, 2009. Article (CrossRef Link)
[9] C. Zhang, X. Lin, R. Lu and P. H. Ho, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks," in *Proc. of ICC'08*, pp.1451-1457, May 19-23, 2008. Article (CrossRef Link)
[10] A.O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235 - 3249, Dec. 2003. Article (CrossRef Link)
[11] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24-32, May 2007. Article (CrossRef Link)
[12] M. Nloch, J. Barros and M. R. D. Rodrigues, "Wireless information theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515-2534, June, 2008. Article (CrossRef Link)
[13] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. on Wireless Communications*, vol. 7, no. 7, pp. 2571 - 2579, July 2008. Article (CrossRef Link)
[14] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," in Proc. of *IEEE International Conference on Communications*, pp. 4646 - 4651, June 2007. Article (CrossRef Link)
[15] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals," in *Proc. of IEEE International Conference on Communications*, pp. 1520 - 1524, May 2008. Article (CrossRef Link)
[16] P. L. Yu, J. S. Baras and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. on Information Forensics and Security*, vol. 3, no. 1, pp.38-51, March 2008. Article (CrossRef Link)
[17] P. A. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. Comm. Syst.*, vol. 11, pp. 360-393, 1963. Article (CrossRef Link)
[18] O. Edfors, M. Sandell, J. J. van de Beek, S. K. Wilson and P. O. Borjesson, "OFDM channel estimation by singular value decomposition," *IEEE Trans. Comm.*, vol. 46, no. 7, pp. 931-939, July 1998. Article (CrossRef Link)
[19] P. Hoeher, S. Kaiser and P. Robertson, "Pilot-symbol-aided channel estimation in time and frequency," in *Proc. of IEEE Global Telecomm.*, pp. 90-96, Nov. 1997. Article (CrossRef Link)
[20] Y. Li, L. J. Cimini, Jr. and N. R. Sollenberger, "Robust Channel Estimation for OFDM Systems with Rapid Dispersive Fading Channels," *IEEE Trans. Commun.*, vol. 46, no.7, pp. 902-915, July 1998. Article (CrossRef Link)
[21] S. Coleri, M. Ergen, A. Puri and A. Bahai, "A study of channel estimation in OFDM systems," in *Proc. IEEE VTC*, vol. 2, pp. 894- 898, Vancouver, Canada, September 2002. Article (CrossRef Link)

[22] Y. Qiao, S. Yu, P. Su and L. Zhang, "Research on an iterative algorithm of LS channel estimation in MIMO OFDM systems," *IEEE Trans. Broadcast*, vol. 51, no. 1, pp. 149-153, Mar. 2005. Article (CrossRef Link)
[23] Abraham Wald, "Sequential Tests of Statistical Hypotheses," *Annals of Mathematical Statistics* 16 (2): 117-186, June, 1945. Article (CrossRef Link)

HongWen was born in Chengdu, China. She received the M.Sc. degrees from Sichuan Union University of Sichuan, China, in 1997 and got her Ph.D. degree in Communication and Computer Engineering Dept. of Southwest Jiaotong University in 2004. Then she worked as Associate Professor at National Key Laboratory of Science and Technology on Communications of UESTC, China. From January 2008 to August 2009, she was research visitor and Postdoctoral Fellowship in Electrical Engineering Dept. at University of Waterloo. Her major interests are wireless communication system security and channel coding.

Pin Han Ho received his B.Sc. and M.Sc. degree from the Electrical Engineering department in National Taiwan University in 1993 and 1995, respectively, and Ph.D. degree from Queen's University at Kingston at 2002. He is now an associate professor in the department of Electrical and Computer Engineering, University of Waterloo, Canada. Professor Pin-Han Ho is the author/co-author of more than 150 refereed technical papers, several book chapters, and the co-author of a book on optical networking and survivability. His current research interests cover a wide range of topics in broadband wired and wireless communication networks, including survivable network design, wireless Metropolitan Area Networks such as IEEE 802.16 networks, Fiber-Wireless (FIWI) network integration, and network security. He is the recipient of Distinguished Research Excellent Award in the ECE department of U of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in SPECTS'02, ICC'05 Optical Networking Symposium, and ICC'07 Security and Wireless Communications symposium, and the Outstanding Paper Award in HPSR'02.