Secure Transmission for Two-Way Vehicle-to-Vehicle Networks with an Untrusted Relay

Zhenzhen Gao

Department of Information and Communication Engineering, Xi'an Jiaotong University, Xi'an, 710049, P. R. China.
zhenzhen.gao@mail.xjtu.edu.cn

***** Corresponding Author: Zhenzhen Gao

Received December 15, 2015; Accepted December 27, 2015; Published December 31, 2015

** Regular Paper*

Abstract**:** This paper considers the physical layer security problem for a two-way vehicle-to-vehicle network, where the two source vehicles can only exchange information through an untrusted relay vehicle. The relay vehicle helps the two-way transmission but also acts as a potential eavesdropper. Each vehicle has a random velocity. By exploiting the random carrier frequency offsets (CFOs) caused by random motions, a secure double-differential two-way relay scheme is proposed. While achieving successful two-way transmission for the source vehicles, the proposed scheme guarantees a high decoding error floor at the untrusted relay vehicle. Average symbol error rate (SER) performance for the source vehicles and the untrusted relay vehicle is analyzed. Simulation results are provided to verify the proposed scheme.

Keywords**:** Vehicle-to-vehicle communications, Physical layer security, Two-way relay, Double differential modulation

1. Introduction

Vehicular ad-hoc networks (VANETs) provide new opportunities to develop innovative and advanced solutions for providing reliable communications among vehicles [1]. Typically, VANETs are expected to provide applications in areas like traffic safety, transport efficiency and information/entertainment. Considering the lack of network infrastructure, especially in suburban areas, cooperation with one or more relay vehicles has been proposed in vehicle-to-vehicle (V2V) networks [2]. Compared to the conventional one-way relay protocol, a two-way relay protocol has drawn a lot of interest due to the potential for improving spectral efficiency [3].

Considering that autonomous relay vehicles could be untrusted, the security of two-way V2V cooperative communications is challenging. To avoid eavesdropping by the relay, cryptographic algorithms can be employed. However, there are difficulties and vulnerabilities associated with key distribution and management in VANETs. Physical layer protocol (PHY) security, which exploits the physical characteristics of wireless channels, has attracted a lot of attention. Many PHY security schemes have been proposed for fixed wireless relay networks when the relay is untrusted [4-7]. In VANETs, each vehicle has a different velocity, and the velocities may change over time. Therefore, it is difficult to obtain channel state information (CSI). However, most of the existing PHY layer security schemes are based on the knowledge of CSI [4-8]. Because these existing PHY security schemes cannot be used in a two-way V2V network, it is necessary to propose a secure transmission scheme for a network that has an untrusted relay vehicle.

To avoid decoding at the relay vehicle, an amplify-and-forward (AF) protocol is used. AF two-way relay communications consists of two phases: the broadcast phase (Phase I) and the relay phase (Phase II). In Phase I, the source vehicles simultaneously broadcast their signals; in Phase II, the relay vehicle amplifies and forwards the mixed signals received in Phase I.

In VANETs, each vehicle has a different velocity, and these velocities may change randomly. Because of the Doppler effect, the channels between any two vehicles are perturbed by random carrier frequency offsets (CFOs). To guarantee successful two-way transmission between the source vehicles, double differential modulation for unknown CFOs is a preferred choice, and has been used in cooperative communications. For conventional DF

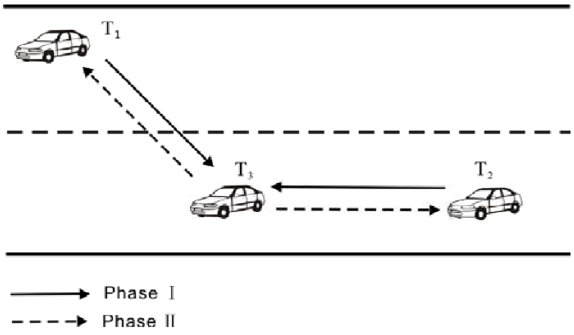

Fig. 1. System model of a V2V system.

cooperative communications systems, double differential modulation [9] and a piecewise linear decoder [10] have been considered. Double differential modulation for AF cooperative communications was studied [11]. Compared to these conventional cooperative communications methods, there are two challenges in the V2V cooperative communications under consideraton: 1) due to the sharing of spectral resources, the signal sent by one source can be delivered not only to the other source, but also back to the original source as self-interference through the relay; and 2) the relay vehicle is untrusted and may be trying to eavesdrop on the sources' information.

In this work, we propose a PHY layer security scheme based on double differential modulation for AF two-way V2V cooperative communications. The symbol error rate (SER) performance of the proposed scheme is analyzed for the source vehicles and the untrusted relay vehicle. An analytical SER upper bound for the source vehicles and an error floor for the relay vehicle are derived. The simulation results coincide with theoretical analysis. Both theoretical results and simulation results show that the proposed scheme creates a high SER at the relay. Moreover, the proposed secure double differential two-way AF relay scheme outperforms the double differential one-way AF relay scheme.

The remainder of the paper is organized as follows. Section 2 presents the two-way vehicle-to-vehicle system model where an untrusted relay exists. In Section 3, a novel physical layer security scheme is proposed for the system being considered. The symbol error performance of the proposed secure transmission scheme is analyzed in Section 4 for the source vehicles and the untrusted relay. In Section 5, simulation results are presented to verify the proposed scheme. Conclusions are made in Section 6.

2. System Model

Consider a two-way relay system with three vehicles: two source vehicles, T_1 and T_2, and one relay vehicle, T_3, as shown in Fig. 1. Each vehicle has a single antenna and operates in half-duplex mode. Let V_i denote the velocity of vehicle $T_i, i = 1, 2, 3$. The velocities are assumed to change randomly within a certain speed interval. Source vehicles T_1 and T_2 need to transmit information to each other with the help of relay vehicle T_3. However, T_3 is untrusted and may eavesdrop on the source vehicle's information. Amplify-and-forward (AF) protocol is applied at the untrusted relay. Specifically, the two-way transmission consists of two phases. In Phase I, T_1 and T_2 transmit simultaneously to T_3. In Phase II, T_3 amplifies and forwards the mixed transmission to T_1 and T_2.

The channel of each link is assumed to be a Rayleigh block fading channel. All links are assumed to be perturbed by different carrier frequency offsets caused by the Doppler effect. Assume that the phases caused by CFOs are randomly distributed over $\left[-\pi,\pi\right\rangle$ and are independent of each other [11]. Assume that these CFOs remain fixed for at least three two-way transmissions.

3. The Proposed Scheme

Due to the randomly relative motion of the vehicles, it is difficult for them to estimate the CFOs caused by the Doppler effect. The good thing is that the random CFOs render the untrusted relay unable to decode the mixed signals received in Phase I. The bad thing is that the source vehicles cannot exchange their information either, due to the unknown random CFOs. Therefore, we need to design a scheme to guarantee successful two-way transmission in the presence of unknown CFOs. Meanwhile, the scheme should prevent the relay from correctly decoding the source information.

Since all links are assumed to be block fading channels, the channel gains of the links do not change during channel coherence time. Meanwhile, the CFOs of the links change randomly. It is difficult for the vehicles to estimate the CFOs for the two-hop links. However, it is easy for each source vehicle to estimate the channel gain of the link between itself and the relay vehicle, which is called the local channel gain. Assume that there are K two-way transmissions during channel coherence time. To avoid getting any channel information at the relay vehicle, a sequence of training signals is transmitted by the relay at the beginning of the two-way transmission. Based on the training signals, each source vehicle can estimate the local channel gain for the current channel coherence time.

The *kth* two-way transmissions of T_1 and T_2 are $s_1[\mathrm{k}]$ and $s_2[\mathrm{k}]$, respectively. They come from a normalized M-array Phase-Shift Keying (M-PSK) constellation $\mathcal{A}$, i.e., the average symbol energy of $\mathcal{A}$ is normalized at 1. After double differential modulation, the transmitted signal $u_i[\mathrm{k}]$ of T_i can be obtained from $s_i[\mathrm{k}]$ as follows:

$$\begin{aligned} &g_i[k] = g_i[k-1]s_i[k], \\ &u_i[k] = u_i[k-1]g_i[k], \\ &k = 2,3,\cdots,K, i = 1,2 \end{aligned} \tag{1}$$

with $u_i[0]{=}u_i[1]{=}g_i[1] = 1$. Because $\left|s_i[\mathrm{k}]\right| = 1$, it follows from (1) that $g_i[\mathrm{k}]{=}u_i[\mathrm{k}]{=}1$.

In Phase I of the *kth* transmission, the received signal at T_3 can be written as

$$y[k]=\sum_{i=1}^{2}\sqrt{P_i}h_{i3}e^{j\omega_{i3}(2k-2)}u_i[k]+n_3[k] \tag{2}$$

where P_i is the transmit power of vehicle $T_i, i=1,2,$ h_{i3} is the channel coefficient of the link between T_i and relay T_3, $\omega_{i3}=2\pi f_{i3}$, f_{i3} is the carrier frequency from T_i to T_3, and n_3[k] is the additive complex white Gaussian noise with mean 0 and variance σ^2.

Considering the Doppler effect, the received frequency is $f=\frac{c+v_r}{c+v_s}f_0$, where f_0 is the carrier frequency, c is the velocity of waves in the medium, and v_r is the velocity of the receiver relative to the medium, which is positive if the receiver is moving towards the source, and negative in the other direction. v_s is the velocity of the source relative to the medium, which is positive if the source is moving away from the receiver, and negative in the other direction. The speeds v_r and v_s are small compared to c. Therefore, the CFOs caused by relative motion of the vehicles have the following relationship: f_{i3}=f_{3i} ,i=1, 2, where f_{3i} is the carrier frequency from T_3 to T_i. Then T_3 forwards βy^* to T_1 and T_2 in Phase II, where $(\cdot)^*$ represents the operation of conjugation, and β is the AF factor. Assume that the transmit powers and the channel statistic information are known at the vehicles, and the AF factor β is $\beta=\sqrt{\frac{1}{\sum_{i=1}^{2}P_i\sigma_{i3}^2+\sigma^2}}$, where σ_{i3}^2 is the variance of $h_{i3}, i=1,2.$ Due to channel reciprocity, $h_{13}=h_{31}$ and $h_{23}=h_{32}$, so the received signal at T_1 becomes

$$\begin{aligned}r_1[k]&=\sqrt{P_1P_3}\beta\,|h_{13}|^2\,u_1^*[k]\\&+\sqrt{P_2P_3}\beta h_{23}^*h_{31}e^{j\Delta\omega(2k-2)}u_2^*[k]+n_1'[k]\end{aligned} \tag{3}$$

where $n_1'[k]=\sqrt{P_3}\beta h_{31}e^{j\omega_{31}(2k-2)}n_3^*[k]+n_1[k]$ and $n_1[k]$ is the additive complex white Gaussian noise with mean 0 and variance σ^2. $\Delta\omega=\omega_{13}-\omega_{23}$. The first term in (3) can be subtracted by T_1, which is called self-interference cancellation. Therefore, the received signal at T_1 can be rewritten as

$$r_1[k]=\sqrt{P_2P_3}\beta h_{23}^*h_{13}e^{j\Delta\omega(2k-2)}u_2^*[k]+\tilde{n}_1[k] \tag{4}$$

where $\tilde{n}_1[k]=n_1'[k]+n_e[k]$ and $n_e[k]$ is caused by the channel gain estimation error; $n_e[k]=\sqrt{P_1P_3}\beta\Delta_{|h_{13}|^2}u_1^*[k]$ with $\Delta_{|h_{13}|^2}=|h_{13}|^2-|\hat{h}_{13}|^2$ and $|\hat{h}_{13}|^2$ being the channel gain estimation.

In the following, only the decoding at T_1 is illustrated because the decoding at T_2 is similar. By using (1), we get the following equations:

$$\begin{aligned}r_1[k]&=r_1[k-1]g_2^*[k]e^{2j\Delta\omega}+\eta_1[k]\\r_1^*[k]r_1[k-1]&\\&=s_2[k]r_1^*[k-1]r_1[k-2]+\tilde{\eta}_1[k]\end{aligned} \tag{5}$$

where

$$\begin{aligned}&\eta_1[k]=-\tilde{n}_1[k-1]g_2^*[k]e^{2j\Delta\omega}+\tilde{n}_1[k]\\&\tilde{\eta}_1[k]=\eta_1^*[k]r_1[k-2]g_2^*[k-1]e^{2j\Delta\omega}+\\&\eta_1[k-1]r_1^*[k-1]g_2[k-1]e^{-2j\Delta\omega}+\qquad.\\&\eta_1^*[k]\eta_1[k-1]\end{aligned}$$

Therefore, without the knowledge of CFOs, T_1 can decode T_2 's information as follows:

$$\begin{aligned}\hat{s}_2[k]=arg\min\nolimits_{s_2\in\mathcal{A}}\Big|&r_1^*[k]r_1[k-1]\\&-s_2r_1^*[k-1]r_1[k-2]\Big|^2\end{aligned} \tag{6}$$

The untrusted relay vehicle T_3 tries to decode the source vehicle T_i 's information $(i=1,2)$ based on the received signal in (2). However, T_3 cannot differentiate T_1 's signal from T_2 's. To decode one source's signal, T_3 has to take the other source's signal as interference as follows:

$$y[k]=\sqrt{P_1}h_{13}e^{j\omega_{13}(2k-2)}u_1[k]+I_1[k]+n_3[k] \tag{7}$$

or

$$y[k]=\sqrt{P_2}h_{23}e^{j\omega_{23}(2k-2)}u_2[k]+I_2[k]+n_3[k] \tag{8}$$

where $I_1[k]=\sqrt{P_2}h_{23}e^{j\omega_{23}(2k-2)}u_2[k]$ and $I_2[k]=\sqrt{P_1}h_{13}e^{j\omega_{13}(2k-2)}u_1[k]$ are the inter-vehicle interference. Then T_3 tries to decode T_i 's signal $(i=1,2)$ by using the structure of double differential modulation as follows:

$$\begin{aligned}y[k]&=y[k-1]g_i[k]e^{2j\omega_{i3}}\\&+\xi_i[k]-\xi_i[k-1]g_i[k]e^{2j\omega_{i3}}\\y[k]y^*[k-1]&\\&=s_i[k]y[k-1]y^*[k-2]+\tilde{\xi}_i[k]\end{aligned} \tag{9}$$

where $\xi_i[k]=I_i[k]+n_3[k]$ is the interference plus noise, and $\tilde{\xi}_i[k]$ is the equivalent interference plus noise. If

$\bar{\xi}_i[k] = \xi_i[k] - \xi_i[k-1]g_i[k]e^{2j\omega_{i3}}$, the equivalent interference plus noise $\tilde{\xi}_i[k]$ can be written as

$$\begin{aligned}\tilde{\xi}_i[k] = \bar{\xi}_i[k]\Big[& y[k-2]g_i[k-1]e^{2j\omega_{i3}} \\ & +\bar{\xi}_i[k-1]\Big] \\ & +\bar{\xi}_i^*[k-1]y[k-1]g_i[k]e^{2j\omega_{i3}}\end{aligned} \tag{10}$$

Then, the untrusted relay can decode T_i's signal $(i = 1, 2)$ as follows:

$$\begin{aligned}\tilde{s}_i[k] = arg\min_{s_i \in \mathcal{A}} \Big| & y[k]y^*[k-1] \\ & -s_i y[k-1]y^*[k-2]\Big|^2\end{aligned} \tag{11}$$

4. Performance Evaluation

4.1 Average SER Analysis at the Source Vehicles

In this subsection, the average SER performance for source vehicle T_1 is analyzed when perfect self-interference cancellation is performed. Because $n_i[k]$ is statistically independent Gaussian random variables with mean 0 and variance σ^2 for different i and k, we can get the statistical characteristics of the equivalent noise $\tilde{\eta}_1[k]$ as follows:

$$\begin{aligned}& E\tilde{\eta}_1[k] = 0 \\ & D\tilde{\eta}_1[k] = 4\beta^2 P_2 P_3 |h_{23}|^2 |h_{13}|^2 \ \sigma_e^2 + \sigma_e^4\end{aligned} \tag{12}$$

where $\sigma_e^2 = (\beta^2 P_3 |h_{13}|^2 + 1)\sigma^2$. From (5), the signal power of s_2[k] is $(\beta^2 P_2 P_3 |h_{23}|^2 |h_{13}|^2 + \sigma_e^2)^2$. The signal-to-noise ratio (SNR) at source vehicle T_1 is

$$SNR = \frac{(\gamma+1)^2}{4\gamma+2} \tag{13}$$

where $\gamma = \dfrac{\beta^2 P_2 P_3 |h_{23}|^2 |h_{13}|^2}{(\beta^2 P_3 |h_{13}|^2 + 1)\sigma^2}$. To make the analysis mathematically feasible, we take the following high SNR approximation [11]:

$$SNR \approx \frac{\gamma}{4} + \frac{1}{8} \tag{14}$$

To check the approximation, the exact SNR in (13) and the approximate SNR in (14) are compared in Fig. 2. We can see that the approximation becomes almost perfect when $\gamma > 10dB$.

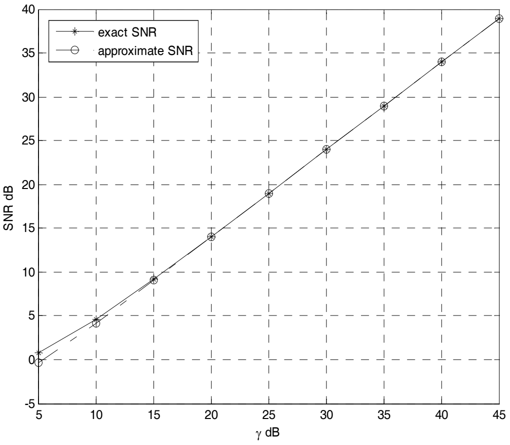

Fig. 2. Comparison of the approximate SNR and exact SNR of the double differential two-way transmission.

Let $\gamma_{13} = \dfrac{P_3 |h_{13}|^2}{\sigma^2}$, $\gamma_{23} = \dfrac{P_2 |h_{23}|^2}{\sigma^2}$, and γ can be written as

$$\gamma = \frac{\gamma_{23}\gamma_{13}}{\gamma_{13} + \bar{\gamma}_s + 1} \tag{15}$$

where $\bar{\gamma}_s = \dfrac{P_1\sigma_{13}^2 + P_2\sigma_{23}^2}{\sigma^2}$. Since the channel coefficients are independent complex Gaussian random variables, the channel gains are independent exponential random variables with parameters $\dfrac{1}{\sigma_{i3}^2}$, $i = 1, 2$, respectively. The probability density function (PDF) of γ can be derived as follows [12]:

$$\begin{aligned}f_\gamma(\gamma) = {} & 2\frac{\bar{\gamma}_s + 1}{\bar{\gamma}_{13}\bar{\gamma}_{23}} e^{-\frac{\gamma}{\bar{\gamma}_{23}}} K_0\left(b\sqrt{\gamma}\right) \\ & + \frac{2}{\bar{\gamma}_{13}\bar{\gamma}_{23}} \sqrt{\frac{\gamma(\bar{\gamma}_s + 1)\bar{\gamma}_{13}}{\bar{\gamma}_{23}}} e^{-\frac{\gamma}{\bar{\gamma}_{23}}} K_1\left(b\sqrt{\gamma}\right)\end{aligned} \tag{16}$$

where $\bar{\gamma}_{13} = \dfrac{P_3\sigma_{13}^2}{\sigma^2}$, $\bar{\gamma}_{23} = \dfrac{P_2\sigma_{23}^2}{\sigma^2}$, $b = 2\sqrt{\dfrac{\bar{\gamma}_s + 1}{\bar{\gamma}_{13}\bar{\gamma}_{23}}}$, and $K_0(\bullet)$ and $K_1(\bullet)$ denote the zeroth order and the first order modified Bessel function of the second kind [13]. From (14) and (16), the PDF of the SNR can be given as

$$f_{SNR}(x) = 4 f_\gamma\left(4(x - \frac{1}{8})\right) \tag{17}$$

The SER conditioned on the SNR at source vehicle T_1 is $P_e(SNR) = 2Q\left(\sqrt{2SNR}\sin\left(\dfrac{\pi}{M}\right)\right)$ [14]. An exponential expression of the Q-function can be derived with Eq. (14) [15] as $Q(x) \approx \dfrac{1}{4}e^{-\frac{2}{3}x^2} + \dfrac{1}{12}e^{-\frac{x^2}{2}}, x > 0,$ which is a tight upper bound for $x > 0.5$ [15]. By using the approximate

SNR in (14) and the bound of the Q-function, the average SER can be upper bounded by

$$\begin{aligned}P_e &\le \int_0^\infty \left(\frac{1}{6}e^{-x\sin^2\left(\frac{\pi}{M}\right)}+\frac{1}{2}e^{-\frac{4}{3}x\sin^2\left(\frac{\pi}{M}\right)}\right) f_{SNR}(x)dx \\ &= \sum_{i=1}^{2}\left[k_i a_i^{-\frac{1}{2}} c_i b^{-1}\frac{\overline{\gamma}_s+1}{\overline{\gamma}_{13}\overline{\gamma}_{(23)}}W_{-\frac{1}{2},0}\left(\frac{b^2}{4a_i}\right)\right. \\ &\quad \left. +k_i a_i^{-1}c_i b^{-1}\frac{1}{\overline{\gamma}_{23}}\sqrt{\frac{(\overline{\gamma}_s+1)}{\overline{\gamma}_{13}\overline{\gamma}_{23}}}W_{-1,\frac{1}{2}}\left(\frac{b^2}{4a_i}\right)\right] \end{aligned} \tag{18}$$

where $k_1=\frac{1}{3}, k_2=1, a_1=\frac{1}{4}\sin^2\left(\frac{\pi}{M}\right)+\frac{1}{\overline{\gamma}_{23}}$, $a_2=\frac{1}{3}\sin^2\left(\frac{\pi}{M}\right)+\frac{1}{\overline{\gamma}_{23}}$ and $c_1=e^{\frac{b^2}{8a_1}-\frac{1}{8}\sin^2\left(\frac{\pi}{M}\right)}$, $c_2=e^{\frac{b^2}{8a_2}-\frac{1}{6}\sin^2\left(\frac{\pi}{M}\right)}$. $W_{\lambda,\mu}(\bullet)$ is the Whittaker function [13].

4.2 Average SER Analysis at the Untrusted Relay

In this subsection, the average SER performance at the untrusted relay vehicle is analyzed. The performance limit at T_3 is investigated when noise is ignored and the inter-vehicle's interference dominates the decoding ability of the untrusted relay.

Without loss of generality, let us take the decoding of T_1's signal as an example. Based on (9), the signal power of $s_1[k]$ is $(P_1|h_{13}|^2+P_2|h_{23}|^2)^2$. The equivalent interference, $\tilde{\xi}_i[k]$, has a zero mean, and the variance is $2(P_1P_2|h_{13}|^2|h_{23}|^2+P_2^2|h_{23}|^4)$. The signal-to-interference ratio (SIR) at the relay vehicle can be written as

$$\begin{aligned}SIR &= \frac{(P_1|h_{13}|^2+P_2|h_{23}|^2)^2}{2(P_1P_2|h_{13}|^2|h_{23}|^2+P_2^2|h_{23}|^4)} \\ &= \frac{P_1|h_{13}|^2}{2P_2|h_{23}|^2}+\frac{1}{2}\end{aligned} \tag{19}$$

Based on the distribution of $|h_{i3}|^2, i=1,2,$ the PDF of the SIR can be calculated as

$$f_{SIR}(x)=\frac{P_1\sigma_{13}^2}{2P_2\sigma_{23}^2}\Big/(x-\frac{1}{2}+\frac{P_1\sigma_{13}^2}{2P_2\sigma_{23}^2})^2 \tag{20}$$

The SER conditioned on the SIR at relay vehicle T_3 is $P_e(SIR)=2Q\left(\sqrt{2SIR}\sin\left(\frac{\pi}{M}\right)\right)$. Since $Q(x)\approx\frac{1}{4}e^{-\frac{2}{3}x^2}+\frac{1}{12}e^{-\frac{x^2}{2}}$, $x>0$ [15], the average SER at T_3 is approximated by

$$\begin{aligned}P_e &\approx \int_0^\infty \left(\frac{1}{6}e^{-x\sin^2\left(\frac{\pi}{M}\right)}+\frac{1}{2}e^{-\frac{4}{3}x\sin^2\left(\frac{\pi}{M}\right)}\right) f_{SIR}(x)dx \\ &= \frac{1}{2}\left[\lambda_1 e^{\lambda_1}Ei(-\lambda_1)+1\right]e^{-\frac{2}{3}\sin^2\left(\frac{\pi}{M}\right)+\lambda_1} \\ &\quad +\frac{1}{6}\left[\lambda_2 e^{\lambda_2}Ei(-\lambda_2)+1\right]e^{-\frac{1}{2}\sin^2\left(\frac{\pi}{M}\right)+\lambda_2}\end{aligned} \tag{21}$$

where $\lambda_1=\frac{2P_1\sigma_{13}^2}{3P_2\sigma_{23}^2}\sin^2\left(\frac{\pi}{M}\right)$ and $\lambda_2=\frac{P_1\sigma_{13}^2}{2P_2\sigma_{23}^2}\sin^2\left(\frac{\pi}{M}\right)$. From (21), we can see that the average SER at T_3 is related to the transmit power and channel conditions of the source-to-relay links. Considering a practical scenario, where $P_1=P_2$ and the channel variances are the same, the average SER at the relay is a constant determined by the modulation. For binary phase shift keying (BPSK), the average SER is $P_e=0.3311$, which is the best performance limit that the untrusted relay can ever achieve.

5. Simulation Results

In the simulation, a simple channel gain estimation method is used before the two-way V2V transmission. Assume that there are $K=50$ two-way transmissions during channel coherence time. A training sequence of L symbols is first transmitted from relay vehicle T_3 to source vehicles T_1 and T_2. Let $\mathbf{x}_T=\left[x[1],\cdots x[L]\right]$ be the transmitted signal sequence. Assume that $\left|x[l]\right|^2=1, \forall l\in[1, L]$. The received signal at $T_i, i=1,2$ is

$$r_{T_i}[l]=\sqrt{P_T}h_{3i}e^{j\omega_{3i}(l-1)}x[l]+n_{T_i}[l], \quad l=1,2,\cdots,L$$

where P_T is the training power, and $n_{T_i}[l]$ is the additive complex white Gaussian noise. Each source vehicle estimates its local channel gain by

$$|\hat{h}_{i3}|^2=\frac{\sum_{l=1}^{L}|r_{T_i}[l]|^2}{LP_T}, \quad i=1,2$$

After that, T_1 and T_2 begin to transmit their information.

In the following, we will show some simulation results of the proposed scheme for a two-way V2V system with an untrusted relay vehicle. In the simulations, BPSK is used. The transmit power of each vehicle is $P_i=P_t$, $i=1,2,3$. The channel variances are $\sigma_{13}^2=\sigma_{23}^2=1$. The channels are perturbed by independent random CFOs, and the phases are uniformly distributed in the range of $\left[-\pi,\pi\right\rangle$.

Fig. 3 compares the theoretical performance and the

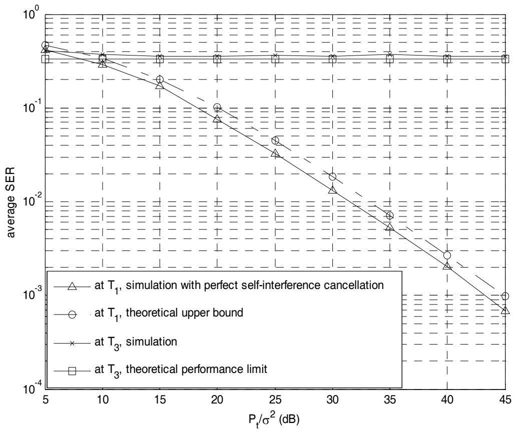

Fig. 3. Theoretical and simulation results for the source vehicles and the untrusted relay vehicle.

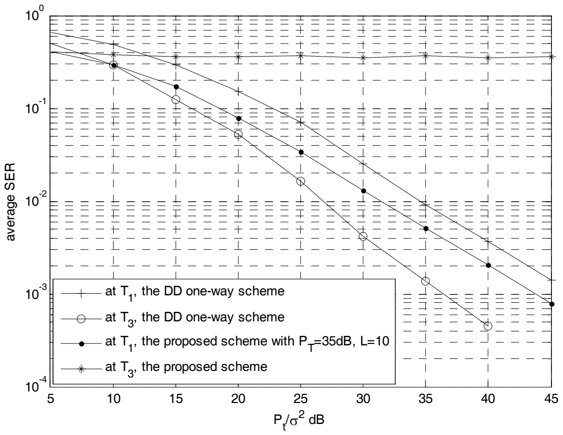

Fig. 5. Performance comparison of the proposed scheme and the DD one-way scheme.

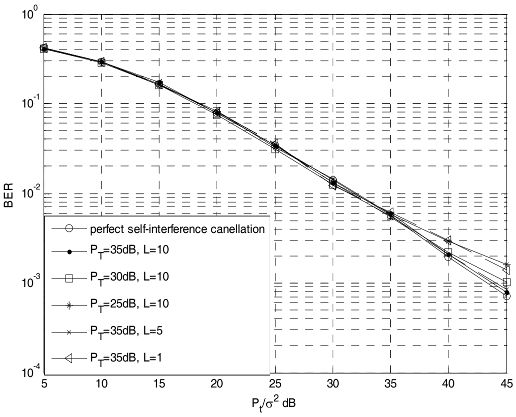

Fig. 4. Average SER performance at T_1 of the proposed scheme with different overhead.

simulation results of the source vehicles and the untrusted relay vehicle. First, we can see that the untrusted relay has an error floor around 0.37, which is slightly higher than the theoretical performance limit of 0.3311. Therefore, the untrusted relay cannot correctly decode the source signal. At the same time, both the analytical result and the simulation result show that the proposed secure scheme can guarantee successful two-way transmission in the V2V relay network. The analytical upper bound in (18) is presented. The simulated SER performance with perfect self-interference cancellation is also given for comparison. We can see that the bound follows the shape of the simulated SER curve.

In the proposed scheme, for self-interference cancellation at the source vehicles, a training sequence is transmitted by the relay vehicle. This sequence can be regarded as overhead of the secure double differential transmission scheme. Fig. 4 shows the average SER performance of the source vehicles with different overhead. To show the influence of the overhead, the average SER performance with perfect self-interference cancellation is given as a benchmark. From Fig. 4, we can see that when the training SNR $P_T/\sigma^2 = 35dB$, L = 10, the average SER performance is almost the same as the performance with perfect self-interference cancellation. Performance degradation occurs when P_T/σ^2 is reduced or the sequence length lessens.

Double differential one-way (DD one-way) relay is an existing transmission scheme for AF two-hop cooperative communications with random CFOs [11]. In Fig. 5, the average SER performance of the DD one-way scheme is compared with the proposed secure double differential two-way relay scheme. Quadrature Phase-Shift Keying (QPSK) is used for the DD one-way scheme so that both schemes have the same transmission rate. However, we can see that the DD one-way scheme cannot provide any security against the untrusted relay vehicle. The reason is that in a one-way relay scheme, the two source signals do not interfere with each other, and the relay vehicle can utilize the structure of the double differential modulation. The average SER at T_3 is even better than that at T_1 due to the amplification of the forwarded noise.

6. Conclusion

In this paper, we propose a secure double differential transmission scheme for an AF two-way V2V network with an untrusted relay vehicle. The average SER performance of the proposed scheme is analyzed for the source vehicles and the untrusted relay vehicle. Theoretical results and simulation results prove that the proposed secure transmission scheme can provide successful two-way V2V transmission and prevent the relay from eavesdropping on the source vehicles' information.

Acknowledgement

The work was supported in part by the National Natural Science Foundation of China under Grant No. 61302067, Specialized Research Fund for the Doctoral Program of Higher Education under grant 20130201120020

References

[1] H. Hartenstein, K. P. Laberteaux, "A Tutorial Survey on Vehicle Ad Hoc Networks," *IEEE Communications Magazine*, vol. 46, no. 6, June 2008, pp. 164-171. Article (CrossRef Link)

[2] Y. Choi, D. Kim, "Quality-Supporting Duration for Dual-Hop Vehicle-to-Vehicle Cooperative Communications," in *Proc. Int. Conference on Information and Communication Technology*, Bandung, Indonesia, March 20-22, 2013, pp. 33-37. Article (CrossRef Link)

[3] M. W. Baidas, A. B. MacKenzie, and R. M. Buehrer, "Network-Coded Bi-Directional Relaying for Amplify-and-Forward Cooperative Networks: A Comparative Study," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, July 2013, pp. 3238–3252. Article (CrossRef Link)

[4] Z. Gao, Y. Yang, and K. J. R. Liu, "Anti-Eavesdropping Space-Time Network Coding for Cooperative Communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, Nov. 2011, pp. 3898-3908. Article (CrossRef Link)

[5] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical Layer *Security* for Two-Way Untrusted Relaying with Friendly Jammers," *IEEE Trans. On Vehicular Technology*, vol. 61, no. 8, June 2012, pp. 3693-3704. Article (CrossRef Link)

[6] Z. Gao, X. Liao, X. Sun and S. Zhu, "A Secure Space-Time Code for Asynchronous Cooperative Communication Systems with Untrusted Relays," in *Proc. IEEE Wireless Communications and Networking Conference*, Shanghai, China, April 7-10, 2013, pp. 4192-4196. Article (CrossRef Link)

[7] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure Beamforming for MIMO Two-Way Communications with an Untrusted Relay," *IEEE Trans. Signal Processing*, vol. 62, no. 9, Sept. 2014, pp. 2185-2199. Article (CrossRef Link)

[8] H. Zhang, H. Xing, X. Chu, et.al., "Secure Resource Allocation for OFDM Two-Way Relay Networks," in Proc. IEEE Globecom, Anaheim, California, USA, December 3-7, 2012, pp. 3649-3654. Article (CrossRef Link)

[9] M. R. Bhatnagar, A. Hjorungnes, L. Song, and R. Bose, "Double-Differential Decode-and-Forward Cooperative Communications over Nakagami-m Channels with Carrier Offsets," in *Proc. IEEE Sarnoff Symposium*, Princeton, NJ, April 28-30, 2008, pp. 1-5. Article (CrossRef Link)

[10] M. R. Bhatnagar and O. Tirkkonen, "PL Decoding in Double Differential Modulation based Decode-and-Forward Cooperative System," *IEEE Commun. Lett.*, vol. 17, no. 5, May 2013, pp. 860-863. Article (CrossRef Link)

[11] M. R. Bhatnagar, A. Hjorungnes, and L. Song, "Amplify-and-Forward Cooperative Communications using Double-Differential Modulation over Nakagami-m Channels," in *Proc. IEEE Wireless Communications and Networking Conference*, Las Vegas, NV, March 31-April 3, 2008, pp. 350-355. Article (CrossRef Link)

[12] Q. Zhao and H. Li, "Performance of Differential Modulation with Wireless Relays in Rayleigh Fading Channels," *IEEE Commun. Lett.*, vol. 9, no. 4, April 2005, pp. 343-345. Article (CrossRef Link)

[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integral, Series, and Products*, 5th ed., Academic Press, 1994. Article (CrossRef Link)

[14] J. G. Proakis, *Digital communications*, 4th ed., New York: McGra-Hill, 2000.

[15] M. Chiani, D. Dardari, and M. K. Simon, "New Exponential Bounds and Approximations for the Computation of Error Probability in Fading Channels," *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, April 2003, pp. 840-845. Article (CrossRef Link)

Zhenzhen Gao received the B.S. and Ph.D. in Communication Engineering in 2005 and 2011 from Lanzhou University and Xi'an Jiaotong University respectively. Now she is with the Department of Information and Communication Engineering, Xi'an Jiaotong University, Xi'an, China. She received a scholarship from China Scholarship Council (CSC) in 2009. From September 2009 to August 2011, she was a visiting student in the Department of Electrical and Computer Engineering at the University of Maryland, College Park, MD, USA. Her current research interests are in the areas of wireless communications and networks, including Physical Layer security, space-time coding and network coding, 5G networks.