Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 505831, 11 pages
http://dx.doi.org/10.1155/2013/505831

Research Article

Secrecy-Enhanced Data Dissemination Using Cooperative Relaying in Vehicular Networks

Li Sun,[1,2] Qinghe Du,[1,2] and Pinyi Ren[1]

[1] *Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China*
[2] *The State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Pinyi Ren; pyren@mail.xjtu.edu.cn

Received 25 July 2013; Accepted 9 September 2013

Academic Editor: Kun Hua

Due to the potentials in promoting the driving safety and easing the traffic congestion, vehicular networks, especially vehicle-to-vehicle (V2V) communications, have recently been receiving much attention. The data dissemination protocol for V2V applications should not only provide end-to-end transmissions with low error probability and high throughput but also offer antieavesdropping capabilities. To achieve this goal, we in this paper propose a secrecy-enhanced relaying protocol for vehicular environments. Based on the network topology and the velocity of the moving vehicles, the proposed scheme first generates the relay candidate set, from which a single relay is then selected opportunistically to assist the source. By using the superposition coding strategy, the selected relay jointly sends the source message and the artificial interference to enable secure communications. We derive the tight closed-form expressions for the upper and lower bounds of the secrecy outage probability, based on which we analyze the diversity order of the system. The method to generate the interference signal is introduced, and the choice of superposition weight factor is also given. The analytical and simulation results show that the proposed relay-aided protocol yields a better performance than the competing alternatives in terms of both the secrecy performance and the implementation complexity.

1. Introduction

In the last few years, we have witnessed a large increase in the number of vehicles and critical traffic accidents as well. This calls for the development of Intelligent Transportation Systems (ITS), which integrates communications and information technology (CIT) into the transportation systems to provide a safer and more efficient driving experience. Vehicular network, as an embodiment of ITS, is a promising application-oriented network for enhancing the driving safety, improving the traffic management efficiency, and providing infotainment services [1]. Since the late 1980s, there has been an increasing research interest in the field of vehicular networks, from both the industry and the academia. Several standards have been established, including DSRC (dedicated short range communications), IEEE 802.11 p, IEEE 1609, and so forth. Meanwhile, university research efforts have also been made to characterize and model the wireless vehicular channels [2], develop medium access control (MAC) protocols [3, 4], design routing algorithms [5, 6], and carry out field trials in real-world environments [7].

There are basically two types of data dissemination modes in vehicular networks, namely, V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure). For the former, vehicles communicate with each other directly through a single-hop or a multihop connection, while for the latter, vehicles exchange the information with the fixed infrastructure (called the roadside unit or RSU) that is installed along the roadside. In practice, the data transfer for any source-destination pair can be performed in V2V, V2I, or the hybrid manner. However, in this paper, we only focus on the V2V communications.

Although many communication technologies have been devised so far for wireless networks, it is nontrivial to design a highly efficient data dissemination protocol for V2V communications. The main challenge comes from the unique feature of the vehicular networks. First, due to the fast movement of vehicles, the connectivity among the vehicle

nodes may change frequently, and the resulting network topology is highly dynamic. Second, the propagation conditions for vehicular communications are more complicated compared to traditional wireless systems. The existence of the obstacles such as buildings, trees, and traffic lights will lead to poor channel quality. These two factors make the wireless communications for vehicular networks error-prone, which indicates the necessity for developing novel protocols to support the stringent QoS requirements in vehicular environments.

To achieve this goal, more and more efforts have been made to enhance the performance of the physical layer (PHY) of the vehicular networks. Among many candidates of physical layer techniques, cooperative relaying is widely recognized as a powerful tool, which can provide the spatial diversity and multiplexing gain by letting neighboring users cooperate with each other. Since the seminal works of [8, 9], a large body of literature has appeared dealing with the relaying protocol design for various systems, and many cooperative techniques have been proposed, including distributed space-time code (DSTC), relay selection, coded cooperation, collaborative beamforming, and so forth [10–14]. In vehicular communications, the destination node may be outside the transmission range of the source node; however, there are often many intermediate vehicles that can serve as relays. Therefore, the application of cooperative relaying in vehicular communications is an appealing solution to provide reliable end-to-end data delivery. In [4], a relay-aided distributed MAC protocol is proposed to optimize the system throughput and extend the service range of vehicular networks. The key idea is to adaptively select the relay node and the cooperative mode according to the channel quality and the relay positions. In [15], cooperative communication is exploited to improve the performance of routing algorithm, and a path selection criterion is developed to obtain a better tradeoff between the end-to-end reliability and the energy efficiency. The main drawback of the works [4, 15] is that they do not take into account the impact of some network parameters (such as the vehicle density, the road structure, etc.) on the protocol design. Aiming at this problem, [16] investigates the collective impact of the internode distance, the vehicle density, and the transmission range of the vehicles on the access and connectivity probability for vehicular relay networks. In [17], a cooperative data dissemination mechanism is introduced. The authors explore the symbol-level network coding to enhance the reception reliability and the content downloading rate.

Common to the aforementioned works is that they mainly focus on the use of cooperative relaying to enhance the transmission reliability, improve the end-to-end throughput, or extend the service coverage of vehicular networks. However, the openness of the wireless vehicular channels makes the transmitted data available to unauthorized users as well as the intended receiver. For example, Vehicle A wants to transmit a confidential message to Vehicle B via some trusted relays. Meanwhile, there is some malicious entity (called Vehicle E)within the transmission range that attempts to extract this information.Therefore, guaranteeing the secrecy of the data transmission process is also of vital importance. Existing approaches to securing communications rely heavily on the data encryption at the upper layers of the protocol stack. Taking vehicular networks as an example, IEEE 1609.2 specifies the formats for the secure messages and the corresponding encryption/decryption procedure. In contrast with this paradigm, the physical layer (PHY) security exploits the characteristics of the physical channel to guarantee secrecy. Since the pioneering work of [18, 19], more and more attentions have been paid to PHY security from an information-theoretic point of view [20–23]. Recently, the secrecy problem was considered under the framework of cooperative networks. Reference [24] studied the use of decode-and-forward (DF) and amplify-and-forward (AF) relays to enhance the PHY security, and [24–26] discussed the cooperative jamming (CJ) technique with sending artificial noise as its core. To reduce the implementation complexity without sacrificing the achievable secrecy performance, relay selection is introduced as an efficient mechanism to fulfill secure cooperation. In [27], an opportunistic selection technique was reported to minimize the secrecy outage probability. Following the idea of jamming, the authors of [28] proposed several schemes to select two relays to protect the legitimate receiver from being eavesdropped, significantly enhancing the performance. Reference [29] also adopts the relay selection and cooperative jamming to secure communications, but the jamming signal is sent from the destination rather than the selected relay.

Although the developed PHY-security methods in [28, 29] are effective in improving the secrecy performance of relay systems, none of them take the characteristic of the vehicular networks into consideration. Besides that, in these schemes, the channel state information (CSI) regarding the eavesdropping link is assumed to be available, which may not hold for vehicular applications. Unlike the existing works, a secrecy-enhanced data dissemination protocol is proposed in this paper for vehicular networks, using relay transmission and cooperative jamming techniques. The protocol works as follows: first, the relay candidate set is formed, based on the road structure, the vehicle locations, and the velocity of the moving vehicles. Then, a single vehicle is selected opportunistically from the set, which jointly transmits the source message and the intentional interference. By exploiting the CSI of the relaying link (not the eavesdropper link), we make the interference signal completely known at the destination but unknown at the eavesdropper. In this manner, the secrecy outage probability of the system is obviously decreased.

The rest of this paper is organized as follows. Section 2 introduces the system model and notations. In Section 3, the proposed relaying protocol is described. In Section 4, the secrecy outage probability of the proposed protocol is analyzed in details, and a simple power allocation scheme is also given. Simulation results are shown in Section 5, from which the superiority of our protocol can be observed. Finally, we conclude our work and point out some further directions in Section 6.

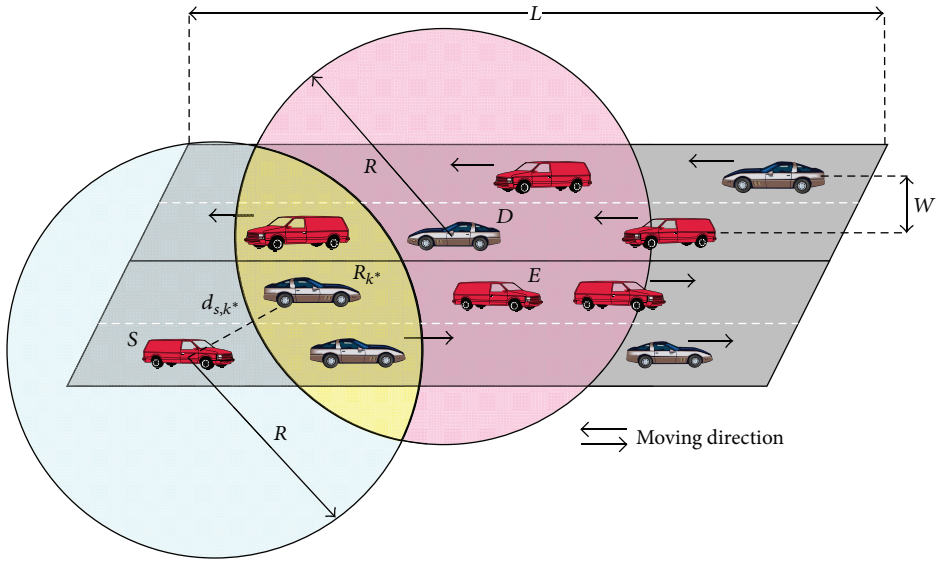

FIGURE 1: An example of the considered system with $M = 4$.

2. System Model

As is shown in Figure 1, we consider a segment of the road, which consists of M straight lanes with length of L meters each. The width for every lane is W meters. Within the considered $L \times MW$ rectangular area, K vehicles are uniformly distributed. The vehicles on the upper two lanes are moving from the right to the left, whereas the vehicles on the lower two lanes are moving towards the opposite direction. At any time instant, there might be several vehicles having data to transmit. To avoid the intervehicle interference, a TDMA-based scheduler is adopted, and only one source-destination pair is allowed to communicate with each other. The scheduled transmitter and the corresponding receiver are labelled as S and D, respectively. Meanwhile, a malicious node may also exist in the area, which tries to eavesdrop the information intended for D. The transmission range of any vehicle is R meters. Each node has a single antenna and operates in a half-duplex mode; that is, it cannot transmit and receive simultaneously. E is assumed to be passive and thus the CSI pertaining to the eavesdropper channel is not available. We further assume that the direct link between S and D does not exist, which can be attributed to the fact that D is outside the transmission range of S. Thus, the communications between these two nodes can only be completed via the help of other vehicles serving as relays. Prior to the source transmission, the relay candidate set is first formed according to the positions and the behaviors (such as the moving directions and the velocity) of the vehicles. After that, the source divides its data into frames, and the transmission of each frame is performed in a two-phase manner. During the first phase, S broadcasts its message x_S, and all the vehicles in the candidate set attempt to decode the message. The ones that successfully perform decoding constitute the decoding set $D(s)$, from which a single "best" relay, denoted by k^*, is selected to cooperate. The details on how to generate the candidate set and select the best relay will be given in the next section. To focus on the design of the relaying protocol, we assume that the broadcast phase is secure. That is, E cannot hear the signal from S directly (This assumption, which was made in several related literature, e.g., [27, 28, 30], may correspond to some practical scenarios. Examples include the applications where the source transmission power is too small to be heard by the eavesdropper, or the networks with orthogonal components (e.g., frequencies.) where the eavesdropper node can hear only one of the orthogonal channels.) During the second phase, R_{k^*} transmits the sum of the information-bearing signal x_S and the artificial interference signal (In this paper, the terms "artificial interference" and "artificial noise" are interchangeable.) x_I in the form of $x_{k^*} = \alpha x_S + \sqrt{1-\alpha^2}x_I$, where $0 < \alpha < 1$ is the weight factor. In this way, the relay plays a dual role as both a helper to serve the destination and a jammer to confound the eavesdropper. At the end of the second phase, the destination makes decisions based on the received signal from the relay.

We model the velocity of any vehicle $i(v_i)$ as a random variable, which follows a truncated Gaussian distribution within the interval $[v_{\min}, v_{\max}]$. The mean and the variance of the variable are denoted as $\overline{v}$ and σ_v^2, respectively. The distance between node i and j is represented by d_{ij}. We suppose that the speeds of the vehicles remain unchanged during the whole period of the source transmission. All channels are assumed to be independent, flat, and slow fading, which remain constant within one frame and vary independently from frame to frame. The channel coefficient h_{ij} is a complex circularly symmetric Gaussian variable with mean zero and variance μ_{ij}. That is, $h_{ij} \sim CN(0, \mu_{ij})$. P_S and P_R are the average transmit powers of the source and the selected relay, respectively. For simplicity, we assume $P_S = P_R = P$.

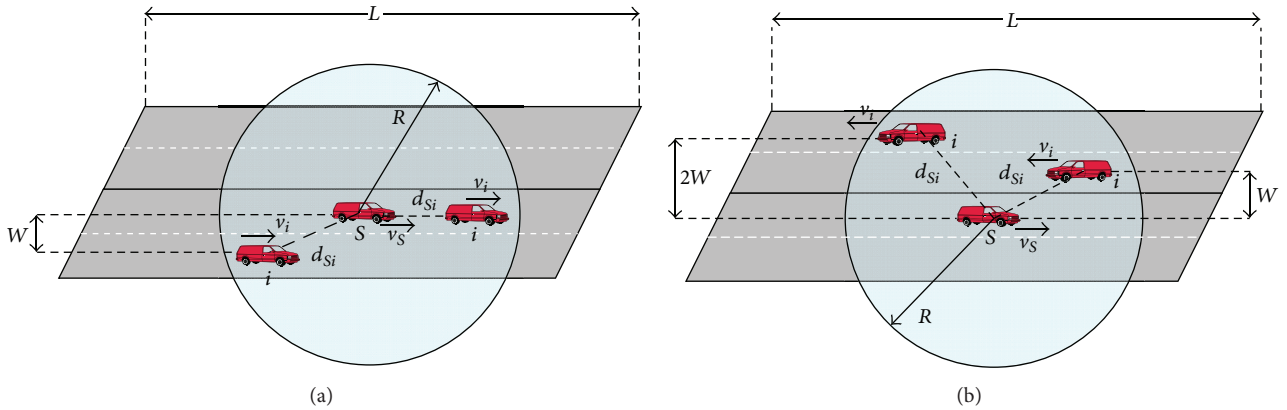

FIGURE 2: The geometry to calculate the links durations. (a) represents the case where S and i are moving towards the same direction, and (b) corresponds to the scenario where S and i are moving towards the opposite direction.

The additive noise at each receiver is modeled as zero-mean, complex Gaussian variable with variance N_0. The notation $\rho = P/N_0$ is introduced to denote the average signal-to-noise-ratio (SNR) of the system. Since this paper is dedicated to the information-theoretic analysis, the impact of channel estimation errors will not be taken into consideration. In other words, all the involved channel estimation operations are assumed to be perfect.

3. Secrecy-Enhanced Relaying Protocol

The proposed secrecy-enhanced relaying protocol includes four stages: the relay candidate set generation, the data broadcasting, the distributed relay selection, and the secure relaying. In what follows, the design details of these stages will be shown.

3.1. Relay Candidate Set Generation. As we have mentioned before, a TDMA-based scheduler is adopted to decide which source-destination pair can access the channel. Once a specified $S - D$ pair is scheduled, a prescreen process will be activated to determine the region where potential relays may exist. To be specific, potential relays should be inside the transmission ranges of both the source and the destination. Mathematically speaking, the following condition has to be satisfied:

$$\max\{d_{Si}, d_{iD}\} \leq R. \tag{1}$$

Then, for all the vehicles satisfying (1), the duration of the link $S \rightarrow R_i \rightarrow D$ is estimated as follows [31].

If vehicle S and i are moving towards the same direction (see Figure 2(a)), the duration of $S \rightarrow i$ link can be calculated as

$$t_{Si} = \begin{cases} \left(\dfrac{R \mp \sqrt{d_{Si}^2 - W^2}}{|v_S - v_i|}\right)^+, & i \notin L(S), \\ \left(\dfrac{R \mp d_{Si}}{|v_S - v_i|}\right)^+, & i \in L(S), \end{cases} \tag{2}$$

where $[x]^+ = \max(0, x)$, and $L(S)$ denotes the lane to which S belongs. When i is in front of S, the sign "$\mp$" becomes "$-$", otherwise "$\mp$" will be "$+$".

On the other hand, if vehicle S and i are moving towards the opposite direction (see Figure 2(b)), the duration of $S \rightarrow i$ link can be calculated as

$$t_{Si} = \left(\frac{R \pm \sqrt{d_{Si}^2 - (kW)^2}}{v_S + v_i}\right)^+, \tag{3}$$

where the sign "$\pm$" becomes "$+$" if i is in front of S and "$-$" otherwise. The value of k may be 1 or 2 for the considered topology, depending on the relative positions of the vehicles. Readers may refer to Figure 2(b) for details.

Similarly, the duration of the link $D \rightarrow i$ (i.e., t_{Di}) can be estimated as well by simply replacing S in (2) and (3) with D.

Based on the above calculations, the duration of the two-hop link $S \rightarrow R_i \rightarrow D$ can be expressed by $\min\{t_{Si}, t_{Di}\}$, and the vehicle i belongs to the relay candidate set only if the following inequality holds:

$$\min\{t_{Si}, t_{Di}\} > T_{\text{th}}, \tag{4}$$

where T_{th} is a preset threshold which is dependent on the size of the transmitted file, the transmission rate, the overhead involved in relay selection, and so forth. In the following discussions, we assume that the cardinality of the relay candidate set is N.

3.2. Data Broadcasting. After the relay candidate set has been formed, the actual data transmission will start. As previously mentioned, the whole procedure is composed of several frame transmissions, with each consisting of the broadcast phase and the relaying phase. During the broadcast phase, S sends its message and all the relays belonging to the candidate set receive the message. The received signal at R_k, denoted by y_k, is expressed as

$$y_k = h_{Sk} x_S + n_k, \tag{5}$$

where h_{ij} stands for the channel coefficient between node i and j, and n_i represents the additive noise at node i. The relays that can successfully decode constitute the decoding set $D(S)$, from which a single best relay will be selected.

3.3. Distributed Relay Selection. The proposed relay selection scheme aims at maximizing the secrecy rate, which is characterized by the difference in the data rate of the channel between S and D and that between the S and E. In respect of our system model, the secrecy rate is zero if $D(s)$ is null. On the other hand, for a nonempty $D(s)$, we suppose $k \in D(s)$ to be the selected relay. Then, at the end of the relaying phase, the received signals at D and E are, respectively, expressed by

$$y_D = h_{kD}x_k + n_D, \tag{6}$$

$$y_E = h_{kE}x_k + n_E. \tag{7}$$

Recall that x_k is the weighted sum of the information-bearing signal and the artificial noise; that is, $x_k = \alpha x_S + \sqrt{1-\alpha^2}x_I$. If x_I can be made completely known at D but unknown at E, the instantaneous secrecy rate can be represented as

$$\begin{aligned} C_k &= \left[\frac{1}{2}\log_2\left(1+\alpha^2\gamma_{kD}\right) - \frac{1}{2}\log_2\left(1+\frac{\alpha^2\gamma_{kE}}{1+\left(1-\alpha^2\right)\gamma_{kE}}\right)\right]^+ \\ &= \left[\frac{1}{2}\log_2\frac{1+\alpha^2\gamma_{kD}}{1+\left(\alpha^2\gamma_{kE}/\left(1+\left(1-\alpha^2\right)\gamma_{kE}\right)\right)}\right]^+ \\ &\overset{\text{high SNR}}{\approx} \left[\frac{1}{2}\log_2\frac{1+\alpha^2\gamma_{kD}}{1+\left(\alpha^2/\left(1-\alpha^2\right)\right)}\right]^+, \end{aligned} \tag{8}$$

where $\gamma_{ij} \triangleq \rho|h_{ij}|^2$ denotes the instantaneous received SNR of the $i \rightarrow j$ link. According to (8), the proposed relay selection criterion is described by

$$k^* = \arg\max_{k\in D(s)}\left\{\gamma_{kD}\right\} \tag{9}$$

which is the same as the protocol for conventional relay networks [11] and can be implemented using the method based on the distributed timer. The result of (9) is attractive because it indicates that, when considering the security issue, the *relay selection policy* (not the whole relaying protocol) designed for conventional systems without secrecy constraints is still applicable, and thus major architecture modifications are not needed.

In the above derivations, a key assumption is that x_I is completely known at D and thus the introduced interference does no harm to the legitimate receiver. This can be realized by exploiting the channel reciprocity ($h_{ij} = h_{ji}$) and the RTS/CTS mechanism involved in relay selection procedure [11], as follows.

Prior to any frame transmission, RTS (ready-to-send) and CTS (clear-to-send) packets are sent from S and D, respectively. On receiving the CTS, each relay R_i estimates the channel h_{iD} and utilizes the result to generate a random sequence, which will be used as the interference signal x_I (In practice, the random sequence, which is actually an artificial noise, is generated according to a specific algorithm, and the value of h_{iD} (or its function) is used as the input parameter (e.g., the seed) of the algorithm. That is to say that the intentionally produced interference signal is controlled by two factors: the adopted algorithm and the CSI.) In the relay selection process, if R_i is selected, it will send the flag signal to declare its presence. From the pilot included in the flag signal, h_{iD} can be estimated at the destination. Since the adopted algorithm to generate the random sequence is public information, D can get full knowledge of x_I (recall that x_I is only determined by the algorithm and h_{iD}) Nevertheless, E knows nothing about x_I because the CSI of h_{iD} is private and only available at R_i and D. Consequently, at the end of the second phase of data transmission, D is able to subtract x_I from y_D, and the decoding of x_S is free of interference. On the other hand, E has to decode x_S from y_E while being affected by x_I, which increases the difficulties of eavesdropping.

3.4. Secure Relaying. In the relaying phase, the selected relay transmits the superposition of the source message and the artificial noise. The legitimate receiver (D) and the eavesdropper (E) try to extract the source information x_S from (6) and (7), respectively.

4. Performance Analysis

4.1. Secrecy Outage Probability. The secrecy outage probability (SOP), which is widely adopted to evaluate the performance of secrecy protocols in fading channels, is defined as the probability that the instantaneous secrecy rate falls below a target secrecy rate $R_S > 0$. For the considered two-hop relaying system, SOP can be expressed as

$$\begin{aligned} P_{\text{out}} = &\prod_{n=1}^{N}\Pr\left(\frac{1}{2}\log_2\left(1+\gamma_{sn}\right) < R_S\right) \\ &+ \sum_{n=1}^{N}\sum_{|D(s)|=n}\left(\Pr\left\{D\left(s\right)\right\}P_{\text{out}}^{D(s)}\right), \end{aligned} \tag{10}$$

where $\Pr(A)$ denotes the probability of A, and $|A|$ stands for the cardinality of the set A. The first part of (10) corresponds to the outage event that no relay can correctly decode the source message, and the remainder calculates the combination of all the conditional secrecy outage probabilities. Under the assumption of Rayleigh fading, γ_{ij} obeys exponential distribution and thus we have

$$\begin{aligned} &\Pr\left(\frac{1}{2}\log_2\left(1+\gamma_{sn}\right) < R_S\right) = \Pr\left(\gamma_{sn} < u\right) = 1-\exp\left(-\lambda_{sn}u\right), \\ &\Pr\left\{D\left(s\right)\right\} = \prod_{l\notin D(s)}\Pr\left(\frac{1}{2}\log_2\left(1+\gamma_{sl}\right) < R_S\right) \\ &\qquad\times\prod_{l\in D(s)}\Pr\left(\frac{1}{2}\log_2\left(1+\gamma_{sl}\right) > R_S\right) \\ &\qquad= \prod_{l\notin D(s)}\left(1-\exp\left(-\lambda_{sl}u\right)\right)\prod_{l\in D(s)}\exp\left(-\lambda_{sl}u\right), \end{aligned} \tag{11}$$

where $u = 2^{2R_S} - 1$ and $\lambda_{ij} = (\rho\mu_{ij})^{-1}$. For a given $D(s)$, the conditional secrecy outage probability $P_{\text{out}}^{D(s)}$ can be derived as

$$\begin{aligned}
P_{\text{out}}^{D(s)} &= \sum_{k\in D(s)} \Pr\left[k \text{ selected}, \ C_k < R_S\right] \\
&= \sum_{k\in D(s)} \Pr\left[\max_{l\in D(s), l\neq k} \{\gamma_{lD}\} < \gamma_{kD}, \right. \\
&\qquad \left. \frac{1+\alpha^2\gamma_{kD}}{1+\left(\alpha^2\gamma_{kE}/\left(1+\left(1-\alpha^2\right)\gamma_{kE}\right)\right)} < v\right] \\
&= \sum_{k\in D(s)} \int_0^\infty \left[\int_0^{(v(1+(\alpha^2 y/(1+(1-\alpha^2)y)))-1)/\alpha^2} f_{\gamma_{kD}}(x) \right. \\
&\qquad \left. \times \prod_{l\in D(s), l\neq k} F_{\gamma_{lD}}(x)\, dx\right] f_{\gamma_{kE}}(y)\, dy,
\end{aligned} \tag{12}$$

where $v = 2^{2R_S}$, $f_X(x)$ and $F_X(x)$ are the probability density function (PDF) and the cumulative distribution function (CDF) of random variable X, respectively. Note that in (12) we have used the exact expression of C_k rather than its high-SNR approximation form.

It is extremely difficult, if not impossible, to obtain the exact result of (12). Therefore, we resort to some approximate methodologies to derive its bounds. It can be easily observed that

$$\frac{\alpha^2 y}{2\ \max\left(\left(1-\alpha^2\right)y, 1\right)} < \frac{\alpha^2 y}{\left(1-\alpha^2\right)y+1} < \frac{\alpha^2}{1-\alpha^2}. \tag{13}$$

Applying (13) to (12) and making use of [32, equation (33)], the lower and upper bounds of $P_{\text{out}}^{D(s)}$ can be, respectively, obtained, after some tedious calculations, as

$$\begin{aligned}
P_{\text{out},LB}^{D(s)} &= \sum_{k\in D(s)} \sum_{m=0}^{|D(s)|-1} \sum_{|S_m^k|=m, S_m^k\subseteq D(s)-\{k\}} (-1)^m \frac{\lambda_{kD}}{\xi} \\
&\quad \times \left\{1 - \exp\left(-\xi p_1 - \frac{\lambda_{kE}}{1-\alpha^2}\right) \right. \\
&\qquad - \lambda_{kE} \exp\left(-\xi\frac{v-1}{\alpha^2}\right) \\
&\qquad \left. \times \frac{1-\exp\left(-\left(1/\left(1-\alpha^2\right)\right)\left(\left(v\xi/2\right)+\lambda_{kE}\right)\right)}{\lambda_{kE}+(v/2)\xi}\right\},
\end{aligned} \tag{14}$$

$$\begin{aligned}
P_{\text{out},UB}^{D(s)} &= \sum_{k\in D(s)} \sum_{m=0}^{|D(s)|-1} \sum_{|S_m^k|=m, S_m^k\subseteq D(s)-\{k\}} (-1)^m \frac{\lambda_{kD}}{\xi} \\
&\qquad \times \left(1 - \exp\left(-\xi p_2\right)\right),
\end{aligned} \tag{15}$$

where $\xi = \lambda_{kD} + \sum_{l\in S_m^k} \lambda_{lD}$, $p_1 = ((v-1)/\alpha^2) + (v/2(1-\alpha^2))$ and $p_2 = p_1 + (v/2(1-\alpha^2))$. S_m^k is the subset of $D(s)-\{k\}$ with m elements.

Substituting (11), (14), and (15) into (10), the closed-form expressions for the lower and upper bound of the SOP are obtained. However, we omit the results due to space limitation. In the next section, it will be verified through simulations that the derived two bounds are rather tight for all the SNR values.

4.2. Diversity Order Analysis. In order to gain some useful insight into the system performance, we proceed to analyze the achievable diversity order, defined as $d \triangleq -\lim_{\rho\to\infty}(\log P_{\text{out}}/\log\rho)$.

When $\rho \to \infty$, we have $\lambda_{ij} \to 0$. By noticing that $e^x \approx 1 + x$ when $x \to 0$, (14) can be approximated by

$$\begin{aligned}
P_{\text{out},LB}^{D(s)} &\approx \sum_{k\in D(s)} \sum_{m=0}^{|D(s)|-1} \sum_{|S_m^k|=m, S_m^k\subseteq D(s)-\{k\}} (-1)^m \frac{\lambda_{kD}}{\xi} \\
&\quad \times \left[\left(\xi p_1 + \frac{\lambda_{kE}}{1-\alpha^2}\right) \right. \\
&\qquad \left. - \frac{\lambda_{kE}}{1-\alpha^2}\left(1 - \xi\frac{v-1}{\alpha^2}\right)\right] \\
&= \sum_{k\in D(s)} \lambda_{kD}\left(p_1 + \frac{(v-1)\lambda_{kE}}{\alpha^2\left(1-\alpha^2\right)}\right) \\
&\quad \times \sum_{m=0}^{|D(s)|-1} \sum_{|S_m^k|=m, S_m^k\subseteq D(s)-\{k\}} (-1)^m \\
&= \sum_{k\in D(s)} \lambda_{kD}\left(p_1 + \frac{(v-1)\lambda_{kE}}{\alpha^2\left(1-\alpha^2\right)}\right) \\
&\qquad \times \delta\left(|D(s)| - 1\right),
\end{aligned} \tag{16}$$

where $\delta(n)$ equals to one if $n = 0$ and zero otherwise. The last equation of (16) is obtained with the help of [32, equation (33)].

As $\rho \to \infty$, by combining (16), (11) with (10), we arrive at

$$\begin{aligned}
P_{\text{out},LB} &\approx \prod_{n=1}^{N}\left(u\lambda_{sn}\right) + \sum_{|D(s)|=1} \prod_{l\notin D(s)} \left(\lambda_{sl}u\right) \\
&\quad \times \prod_{l\in D(s)} \left(1-\lambda_{sl}u\right) \sum_{k\in D(s)} \lambda_{kD}\left(p_1 + \frac{(v-1)\lambda_{kE}}{\alpha^2\left(1-\alpha^2\right)}\right)
\end{aligned}$$

$$\propto \rho^{-N} + \sum_{|D(s)|=1} \rho^{-(N-|D(s)|)} \rho^{0} \sum_{k \in D(s)} \rho^{-1}$$
$$= \rho^{-N} + \sum_{|D(s)|=1} \sum_{k \in D(s)} \rho^{-(N-1+1)} \propto \rho^{-N}, \tag{17}$$

where we have already applied the asymptotic expression for e^x to (11).

Employing the limit operation that $\rho \to \infty$ leads to

$$d_1 \triangleq -\lim_{\rho \to \infty} \frac{\log P_{\text{out},LB}}{\log \rho} = N. \tag{18}$$

Following similar steps, it can be proven that $P_{\text{out},UB} \propto \rho^{-N}$ when $\rho \to \infty$. Therefore, $d_2 \triangleq -\lim_{\rho \to \infty}(\log P_{\text{out},UB}/\log \rho)$ equals to N as well. Recalling that

$$-\frac{\log P_{\text{out},UB}}{\log \rho} < -\frac{\log P_{\text{out}}}{\log \rho} < -\frac{\log P_{\text{out},LB}}{\log \rho} \tag{19}$$

we can conclude from the Squeezing Theorem that the achievable diversity order of the system (d) is N, which indicates that the proposed strategy provides full diversity gain while guaranteeing security.

4.3. Choice of the Superposition Weight Factor. By choosing the weight factor optimally, a lower secrecy outage probability can be achieved. Nevertheless, it is not convenient to perform this optimization based on the derived bounds. Instead, we focus on the asymptotic behavior of the system and try to find a suboptimal one.

For sufficiently large SNR, it is reasonable to assume that all the relays are capable of successful decoding [27, 28]. Furthermore, the approximation in (8) holds with a high probability. Motivated by these, we formulate the asymptotic expression of the secrecy outage probability as

$$P_{\text{out}}^{\text{asymp}} = \prod_{n=1}^{N} \Pr\left[\frac{1}{2}\log_2\left(\frac{1+\alpha^2\gamma_{nD}}{1+\left(\alpha^2/\left(1-\alpha^2\right)\right)}\right) < R_S\right]$$
$$= \prod_{n=1}^{N}\left[1 - \exp\left(-\lambda_{nD}\frac{\nu\left(1+\left(\alpha^2/\left(1-\alpha^2\right)\right)\right)-1}{\alpha^2}\right)\right] \tag{20}$$

from which it is indicated that minimizing $P_{\text{out}}^{\text{asymp}}$ is equivalent to minimizing $g(\alpha) \triangleq (\nu(1 + (\alpha^2/(1-\alpha^2))) - 1)/\alpha^2$. By differentiating $g(\alpha)$ with respect to α and equating the result to zero, the required α can be given by

$$\alpha^* = \sqrt{\sqrt{\nu(\nu-1)} - (\nu-1)} \tag{21}$$

which definitely lies in the interval (0, 1), because $\nu = 2^{2R_S}$ is a positive number.

5. Simulation Results and Discussions

This section presents the simulation results to validate the proposed protocol. In Figures 3–6, we simply assume that a group of N relay candidates already exists, and only focus on the performance of the relay selection criterion and the secure relaying scheme. The impact of the network topology and the mobility of the vehicles on the relay candidate generation will be investigated in Figures 7-8. In the following simulations, the direct links of $S \to D$ and $S \to E$ do not exist. The channel model follows the descriptions of Section 2, that is, $h_{ij} \sim CN(0, \mu_{ij})$. We assume $\mu_{ij} = d_{ij}^{-\theta}$, where d_{ij} is the distance between node i and j, and $\theta = 3$ is the path loss exponent. The notation "SNR" in Figures 3–6 represents the ratio of P versus N_0, that is, ρ in the previous sections.

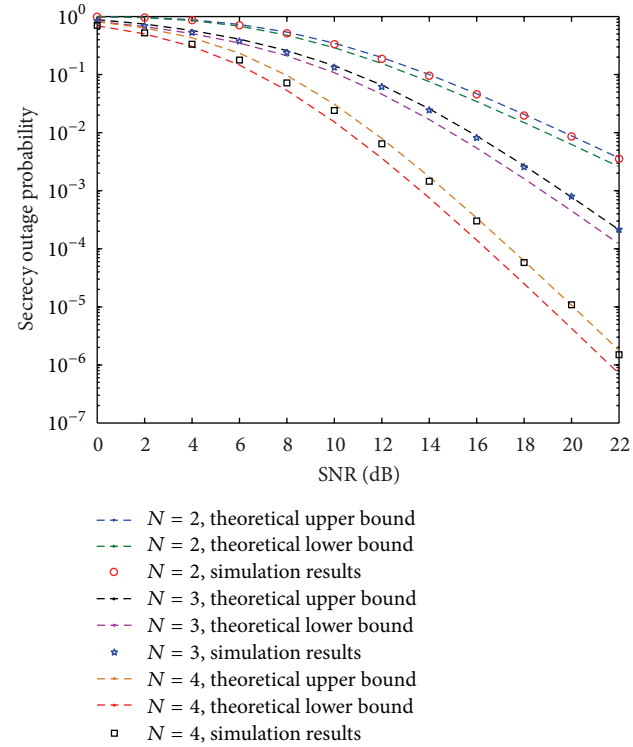

FIGURE 3: The simulated secrecy outage probability and the theoretical bounds. $N = 2, 3, 4$. R_S=1 bit/s/Hz.

In Figures 3–6, the source node, the destination node, and the eavesdropper are located at (0, 0), (1, 0), and (1, 1), respectively. N relay nodes are uniformly distributed in the first quadrant of the 1×1 rectangular coordinate system. Unless otherwise stated, R_S is chosen as 1 bit/s/Hz.

The correctness of the theoretical analysis for the secrecy outage probability is verified in Figure 3, from which it can be seen that the derived bounds are accurate for all the SNR values, and the tightness does not change significantly when the number of relays varies. In particular, there is an excellent match between the upper bound and the simulated result. Additionally, the slopes of the curves illustrate that the diversity order of N, that is, full diversity, is achieved by our protocol.

Figure 4 compares the secrecy outage probability of the proposed scheme to that of some representative counterparts, including the conventional opportunistic selection (CS) [11], the optimal selection without jamming (OS) [27], the optimal

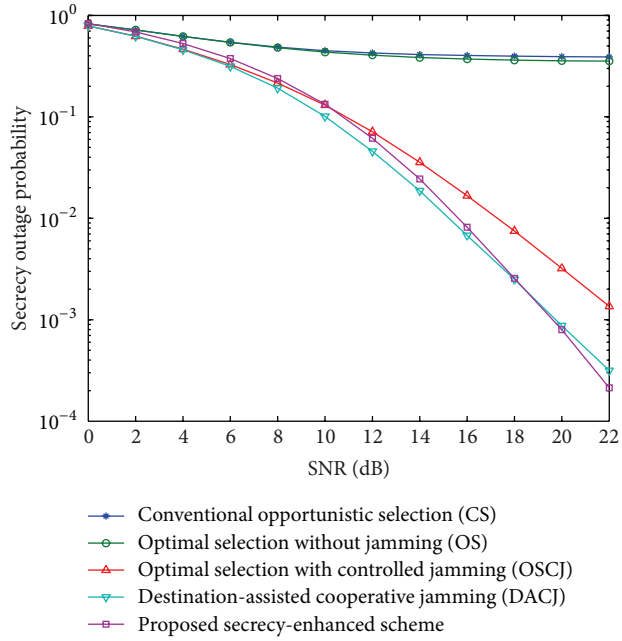

FIGURE 4: Simulation results of the secrecy outage probability for CS, OS, OSCJ, DACJ, and the proposed scheme. $N = 3$ and R_S=1 bit/s/Hz.

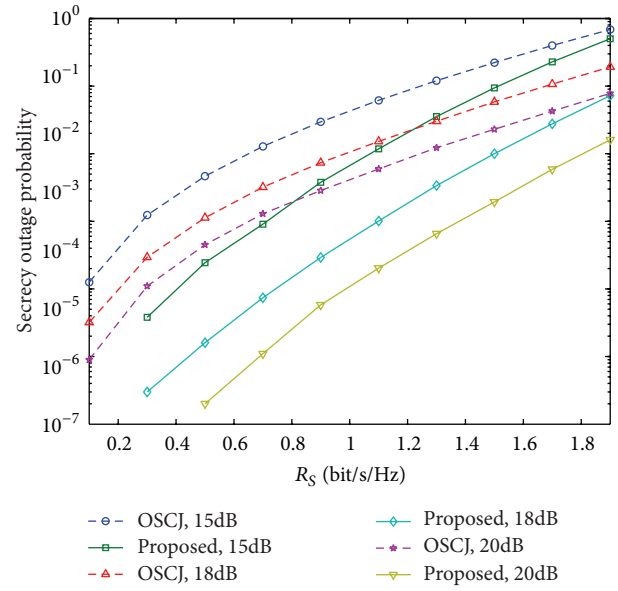

FIGURE 5: Simulation results of the secrecy outage probability for different values of R_S. $N = 4$.

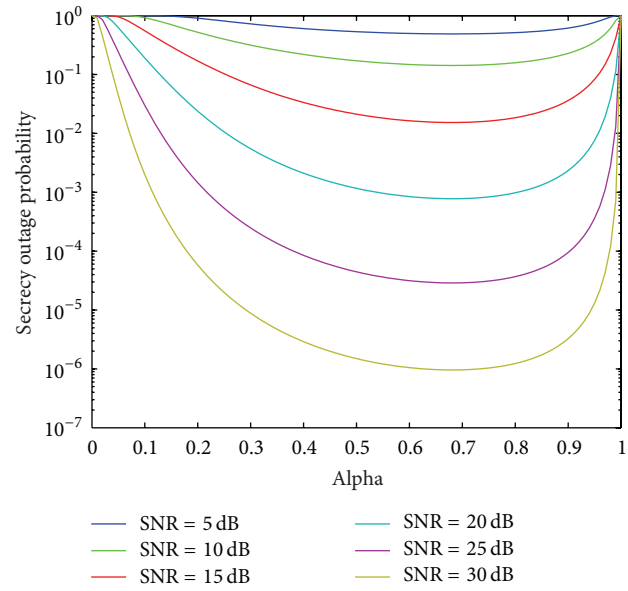

FIGURE 6: The secrecy outage probability versus the superposition weight factor for various SNR values. $N = 3$ and R_S=1 bit/s/Hz.

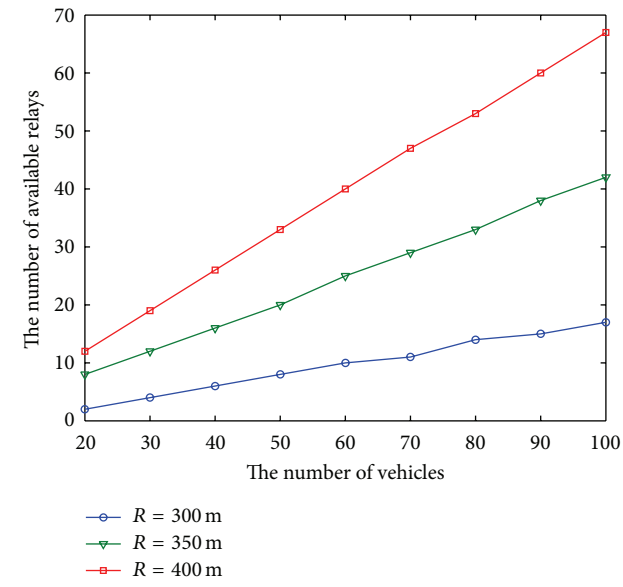

FIGURE 7: The relationship between the number of vehicles and the number of available relays.

selection with controlled jamming (OSCJ) [28], and the destination-assisted cooperative jamming (DACJ) [29]. It should be pointed out that the considered system model in [29] is not the same as ours; therefore, some revisions to the DACJ scheme are performed to make it applicable to our system. Specifically, since the direct links of $S \rightarrow D$ and $S \rightarrow E$ do not exist, the antieavesdropping in the broadcast phase is not needed. Besides that, a dedicated jammer (instead of the source) will cooperate with the relay to transmit in the relaying phase. The jammer and the relay are selected jointly to maximize the achievable secrecy rate. For fairness, we restrict the total transmit powers within a frame to be the same for all the schemes, and if there are more than one transmitters sending signals during some slot, the power will be equally distributed among these nodes (In OSCJ and DACJ schemes, two nodes transmit simultaneously in the second phase. For OSCJ, we have done extensive simulations and found that the equal power allocation can provide the lowest secrecy outage probability (the best performance) for almost all the SNR values. In this sense, equal power allocation is (at least) a near-optimal choice for OSCJ. For DACJ, although

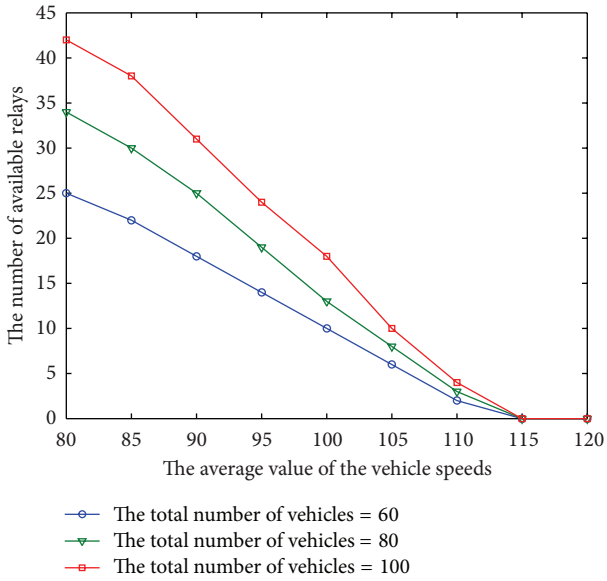

FIGURE 8: The relationship between the number of available relays and the average vehicle speed.

optimal power allocation policy is given in [29], it requires the instantaneous CSI of the eavesdropper link, which will incur additional complexity. Therefore, to make the comparison fair, we do not consider the use of optimal power allocation in DACJ.)

It is evident from Figure 4 that both CS and OS exhibit a significant error floor, which is due to high eavesdropper SNR as the total power increases. By introducing the controlled artificial noise, OSCJ can obtain a remarkable performance gain compared to CS and OS, indicating the effectiveness of jamming technique in supporting secrecy. In contrast with these alternatives, our scheme brings a nonnegligible enhancement in medium to high SNR regimes. For example, at the secrecy outage probability of 10^{-3}, about 3 dB SNR gain is obtained compared to OSCJ. It is also shown from Figure 4 that the performance of DACJ is comparable to that of the proposed scheme. However, considering that our method does not rely on any knowledge of the eavesdropper channel and just selects a single relay for cooperation, we conclude that the proposed strategy has advantages over DACJ in terms of implementation complexity (In DACJ, the knowledge of the eavesdropper channel is required to design the beamformer, which may not be easily satisfied in practice. In addition to that, two nodes have to transmit simultaneously to fulfil cooperative jamming in the second phase, leading to additional overhead to handle the synchronization issues.)

Figure 5 plots the curve of the system secrecy outage probability and exhibits how it varies with the target secrecy rate R_S. In this figure, the number of relays equals to 4, and three SNR values are considered. As expected, when the target rate increases, the SOP increases as well. Nevertheless, the achieved SOP of our scheme is always less than that of the OSCJ scheme.

In Figure 6, we examine the effect of the weight factor (α) on the system performance. For a set of SNR values, the curves of the secrecy outage probability are plotted as a function of α. An important observation from Figure 6 is that the system performance is not very sensitive to $\alpha \in (0.55, 0.75)$, and the suboptimal factor derived in Section 4.3 (for $R_S = 1$ bit/s/Hz, $\alpha^* \approx 0.681$) is competent for the secrecy outage probability optimization, validating the proposed approximate technique.

Finally, Figures 7-8 study the effect of the network topology and the mobility of the vehicles on the relay candidate set generation. In these simulations, the length of the road (L) is set to be 400 m. The number of lanes is 4 and the width of each lane (W) is 4 m. As described in Section 2, the velocity of all vehicles follows a truncated Gaussian distribution over the interval (60 kmph, 180 kmph), with standard variance 5 kmph. The source and the destination are located at (0, 2) and (400, 14), respectively. For any vehicle i, it is added to the candidate set only when the duration of the corresponding $S \rightarrow i \rightarrow D$ link is larger than 10 s. That is, T_{th} equals to 10.

Figure 7 shows the relationship between the number of vehicles and the number of available relays, with R taking three different values. The mean value of the vehicle speeds is 100 kmph. From this figure we can see that the highly dynamic characteristic of the vehicular networks and the limited transmission power of the vehicles contribute to the phenomenon that the number of available relays is much less than the total number of existing vehicles. Therefore, it is necessary to take both the large-scale effect and the small-scale fading into consideration when we design the data dissemination protocol.

In Figure 8, we fix the transmission range of the vehicles to be 300 m and present the number of available relays as a function of the average vehicle speed. As expected, the number of potential relays decreases as the vehicle velocity increases. This is because the fast movement of the nodes will yield a rapid change in the network topology. As a result, the durations of the links will become shorter.

6. Concluding Remarks and Future Works

In this paper, a relay-aided data dissemination protocol is presented for vehicular networks with secrecy constraints. Based on the idea of jamming, we propose to use the superposition coding and the opportunistic relaying techniques to achieve secure communications. The relay selection policy is given, and the details involved in the design of the protocol are also discussed. We evaluate the system performance via both theoretical analysis and numerical simulations.

Developing relay transmission approaches for vehicular networks under the PHY-security framework is a brand new research topic, and there are a lot of issues worthy of investigation. First, in this paper, we only focus on the information-theoretic analysis, yet how to make the proposed idea work in realistic systems is still open. For example, the protocol design based on imperfect channel estimation and (or) practical coding/modulation strategies is needed. Second, it would be of interest to generalize the proposed

method to more complicated network environments, such as the scenarios where there are multiple eavesdroppers and (or) the broadcast phase is not secure. Moreover, the combination of our scheme with other techniques, for example, MIMO and adaptive transmission, may also be valuable directions for further study.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (no. 61201207), the National Science and Technology Major Project of China (no. 2013ZX03003001-002), the Open Research Fund of State Key Laboratory of Integrated Services Networks, Xidian University (no. ISN12-12), the Research Fund for the Specialized Doctoral Program of Higher Education of China (no. 20120201110066), and the Fundamental Research Funds for the Central Universities of China.

References

[1] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[2] C. F. Mecklenbraüker, A. F. Molisch, J. Karedal et al., "Vehicular channel characterization and its implications for wireless system design and performance," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1189–1212, 2011.

[3] J. Zhang, Q. Zhang, and W. Jia, "VC-MAC: a cooperative MAC protocol in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1561–1571, 2009.

[4] T. Zhou, H. Sharif, M. Hempel, P. Mahasukhon, W. Wang, and T. Ma, "A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 72–82, 2011.

[5] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3609–3626, 2009.

[6] H. Zhao, L. Lu, C. Song, and Y. Wu, "IPARK: location-aware-based intelligent parking guidance over infrastructures VANETs," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 280515, 12 pages, 2012.

[7] J. C. Lin, C. S. Lin, C. N. Liang, and B. C. Chen, "Wireless communication performance based on IEEE 802. 11p R2V field trails," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 184–191, 2012.

[8] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity—part I: system description," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1938, 2003.

[9] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[10] W. Zhang and K. B. Letaief, "Full-rate distributed space-time codes for cooperative communications," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2446–2451, 2008.

[11] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Transactions on Wireless Communications*, vol. 6, no. 9, pp. 3450–3460, 2007.

[12] L. Sun, T. Zhang, L. Lu, and H. Niu, "On the combination of cooperative diversity and multiuser diversity in multi-source multi-relay wireless networks," *IEEE Signal Processing Letters*, vol. 17, no. 6, pp. 535–538, 2010.

[13] M. Janani, A. Hedayat, T. E. Hunter, and A. Nosratinia, "Coded cooperation in wireless communications: space-time transmission and iterative decoding," *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 362–371, 2004.

[14] M. Zeng, R. Zhang, and S. Cui, "On design of collaborative beamforming for two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2284–2295, 2011.

[15] Z. Ding and K. K. Leung, "Cross-layer routing using cooperative transmission in vehicular ad-hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 571–581, 2011.

[16] S. C. Ng, W. Zhang, Y. Zhang, Y. Yang, and G. Mao, "Analysis of access and connectivity probabilities in vehicular relay networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 140–150, 2011.

[17] M. Li, Z. Yang, and W. Lou, "CodeOn: cooperative popular content distribution for vehicular networks using symbol level network coding," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 1, pp. 223–235, 2011.

[18] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[19] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[20] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[21] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[22] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[23] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 616–627, 2011.

[24] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[25] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, 2011.

[26] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3801–3807, 2012.

[27] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787–1791, 2010.

[28] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, 2009.

[29] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security.*, vol. 8, no. 4, pp. 682–694, 2013.

[30] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1132–1138, Monticello, Ill, USA, September 2008.

[31] J. Liu, P. Ren, S. Xue, and H. Chen, "Expected path duration maximized routing algorithm in CR-VANETs," in *Proceedings of the 1st IEEE International Conference on (ICCC '12)*, pp. 659–663, Beijing, China, August 2012.

[32] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Interference-limited opportunistic relaying with reactive sensing," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 14–20, 2010.