EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Distributed source-relay selection scheme for vehicular relaying networks under eavesdropping attacks

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

Abstract

The recent development of vehicular networking technologies brings the promise of improved driving safety and traffic efficiency. Cooperative communication is recognized as a low-complexity solution for enhancing both the reliability and the throughput of vehicular networks. However, due to the openness of wireless medium, the vehicular wireless communications (VWC) is also vulnerable to potential eavesdropping attacks. To tackle with this issue, we in this paper propose a novel user-cooperation scheme with anti-eavesdropping capabilities. Specifically, prior to any frame transmission, a source-relay pair is jointly selected to maximize the achievable secrecy rate. After that, the selected relay assists the source to deliver its data to the destination. The proposed selection scheme can be realized in a fully distributed manner, and the security is guaranteed without using any encryption techniques at the upper layers. The closed-form expressions for the secrecy outage probability and the intercept probability are derived, and the achievable diversity order is also analyzed. Simulation results show that the proposed scheme outperforms the competing counterparts in terms of both the secrecy outage probability and the average secrecy rate.

Keywords: Vehicular relaying networks; Cooperative communications; Physical layer security; Source-relay selection; Distributed implementation

1 Introduction

During the past few years, vehicular networks have received increasing attentions due to their potentials in enhancing road safety, improving traffic efficiency, and providing mobile infotainment services [1]. In vehicular networks, the information exchange among the vehicles can be typically performed in two modes, namely, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The V2V communications do not rely on the existence of the central unit, and the vehicles can communicate with each other directly via either single-hop or multi-hop connections. Comparably, in V2I communications, data is transferred between the vehicle and the fixed infrastructure deployed along the roadside, which is often called the roadside unit (RSU) in the literature. The co-existence of these two modes makes the vehicular networks a hybrid network that supports both the infrastructure-based and *ad hoc* communications.

The interests in vehicular networking dates back to late 1980s. Since then, the idea of leveraging wireless technologies for vehicular communications has fascinated researchers around the globe, and great efforts have been made to develop new architectures, protocols, algorithms, and applications for vehicular networks. Many governmental projects or plans have been set up to explore the potentials of vehicular wireless communications (VWC), including the VSC and VII in United States, the eSafety in Europe, and the ASV series in Japan [2]. From the industrial perspective, several standards have been created, among which the most important ones are the IEEE 802.11p and IEEE 1609 protocol suites. IEEE 802.11p specifies the physical layer (PHY) and medium access control (MAC) layer features such that the existing IEEE 802.11 can work in vehicular environments, and IEEE 1609 mainly deals with the multi-channel operation, routing, and security issues. The academic research in the field of VWC is also fruitful, ranging from the modeling of

*Correspondence: pyren@mail.xjtu.edu.cn
[1]Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China
Full list of author information is available at the end of the article

vehicular channels [3] to the development of MAC and routing algorithms [4-7]. Besides that, some field trials have also been carried out in many countries for objective performance evaluation [8].

So far, simple and basic solutions at almost all layers have been devised for vehicular communications. However, the unique features of vehicular networks make the design of efficient VWC protocols challenging. First, the vehicular networks are expected to support the mixture of both the realtime and non-realtime services. As a result, it is difficult to satisfy the diverse quality-of-service (QoS) requirements by simply adopting the existing techniques. Second, the fast movement of the vehicles makes the network topology and the vehicle density highly dynamic, and hence, the connectivity among the vehicles is hard to be guaranteed. Third, due to the existence of various obstacles along the roads, the propagation conditions for VWC is harsher than those for general mobile *ad hoc* networks. All these factors indicate the necessity for developing innovative wireless techniques to support the emerging applications in vehicular networks.

Among many candidates of VWC technologies, cooperative communication is widely regarded as a promising solution to enhance the performance of vehicular networks from various layers. The key idea of cooperative communication is to let the neighboring terminals relay information for each other. In this way, the spatial diversity gain as well as the spatial multiplexing gain can be harvested without the deployment of multiple antennas. The research in cooperative communications is pioneered by Sendonaris et al. [9]. In [10], several basic cooperative relaying protocols were proposed, and their outage performances were analyzed. Since these two seminal papers, a large body of literature has been devoted to the design, analysis, and implementation of cooperative schemes for various scenarios. In [11], the authors proposed a constellation reassignment scheme at the relay to minimize the symbol error rate at the destination node. In [12], a link adaptive regeneration strategy was developed for decode-and-forward (DF) systems. These works, however, are concerned about the simple scenario where there is only one source and one relay. For multiple-relay systems, advanced relaying mechanisms such as distributed space-time coding [13], relay selection [14], network coding [15], and collaborative beamforming [16] were investigated to further benefit the cooperative systems. Based on the work in [14], the joint source-relay selection schemes were proposed in [17,18] for multi-source multi-relay networks to exploit both the cooperative diversity and the multi-user diversity.

In vehicular networks, there are often a large number of vehicles that can serve as relays to facilitate both the V2V and V2I communications. Therefore, the application of cooperative relaying in vehicular communications is a natural choice. In [19], a dual-hop inter-vehicular transmission with relay selection was considered, and the outage performance as well as the achievable diversity order was analyzed. By incorporating a highway mobility model, the authors in [20] proposed a scheme for locating and selecting the optimal relay station for multi-hop vehicular networks. While [19] and [20] mainly focused on the PHY-layer issues, [5] dealt with the relay-aided MAC protocol design for vehicular communications. Specifically, by adaptively choosing the relay node and the cooperative mode, the proposed protocol can optimize the system throughput and extend the service range. In [21], the cross-layer routing was studied using cooperative relaying technique. Through investigations, the authors pointed out that cooperative transmission can yield more efficient routes than the competing counterparts in terms of both the reliability and the energy consumption. To fully characterize the performance of vehicular relay networks, [22] developed an analytical model and analyzed the access probability and the connectivity probability.

Although there are plenty of schemes proposed so far to take full advantages of cooperative communications to improve the link reliability, increase the achievable throughput, extend the service coverage, and lower the energy consumption, very few works address the security issue for relay-aided vehicular networks, which is also of vital importance due to the openness of wireless channels. Consider a vehicular network consisting of multiple source nodes, multiple relay nodes, and one destination node. The relays can help the sources to deliver their messages to the destination. However, these messages can also be overheard by some eavesdropper nearby the destination. Therefore, the developed relaying protocols should provide the anti-eavesdropping capabilities. Traditional approaches to securing communications rely heavily on the data encryption at the upper layers of the protocol stack. However, since data security is critically important, it is reasonable to incorporate the security measures at all layers, including the physical layer. Since the seminal work of [23] and [24], more and more attentions have been paid to PHY security from an information-theoretic point of view [25-27].

Recently, the secrecy problem in cooperative communications networks has emerged as a hot research topic. In [28], three cooperative schemes, namely, DF, amplify-and-forward (AF), and cooperative jamming (CJ), are utilized to secure the source-destination communications. By allocating transmit power at the source and relays and determining the relay weights, the achievable secrecy rate is maximized subject to the total power budget. PHY security can also be realized via the appropriate selection of relay nodes. Following the idea of jamming, the authors in [29] proposed to select two relays to simultaneously serve the legitimate user and confuse the eavesdropper.

For the same system model, [30] 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. In our previous work [31], the security-embedded relay selection scheme is devised, where the selected relay transmits the superposition of the information-bearing signal and the artificial noise. We have shown through rigorous analysis that full diversity is achieved despite the existence of the eavesdropper. Although the injection of artificial noise is useful in improving the system security level, it also causes additional energy consumption. Aiming at this problem, [32] presents the AF- and DF-based optimal relay selection to maximize the secrecy rate, without using artificial noise. Common to the works [28-32] is that they all assume that there is only one eavesdropper within the considered area. In comparison, [33] studied the relay selection issue for dual-hop networks with multiple eavesdroppers.

Although the aforementioned works [28-33] have exhibited the potentials of physical-layer techniques in securing the wireless cooperative networks, all of them assumed that there is only one node having message to transmit. This assumption simplifies the protocol design and the performance analysis, but may not be realistic for vehicular networks. Different from these works, we in this paper consider a more practical scenario where there are multiple sources sharing the same pool of multiple relays. For this scenario, a source-relay selection strategy with anti-eavesdropping capabilities is proposed. The selected source-relay pair is the one that offers the maximum secrecy rate. A significant advantage of the proposed scheme is that it can be implemented in a distributed manner, which is attractive for vehicular networks.

The rest of this paper is organized as follows. Section 2 presents the system model and introduced the basic assumptions. In Section 3, we give a detailed description of the proposed source-relay selection scheme. In Section 4, we evaluate the system performance in terms of the secrecy outage probability, the intercept probability, and the achievable diversity order. Simulation results are shown in Section 5, from which the superiority of our scheme can be observed. Finally, we conclude our work in Section 6.

2 System model

As is shown in Figure 1, we consider a V2I communications scenario where K vehicles (source nodes) want to deliver their confidential messages to the RSU (the destination), which is located beyond the transmission range of the vehicles, and thus, the direct links between the sources and the destination do not exist. However, there are M trusted vehicles that do not have message to transmit and can serve as relay nodes to help the sources. Meanwhile, near the destination, there exists a malicious node (eavesdropper) that tries to intercept the information intended for the destination. The sources, the relays, the destination, and the eavesdropper are denoted by $S_k, (k = 1, 2, \ldots, K)$, $R_m, (m = 1, 2, \ldots, M)$, D, and E, respectively. It is noted that $K \geq 1$, i.e., there might be several sources having data to transmit at any time instant. To avoid the inter-vehicle interferences and reduce the implementation complexity, we employ a TDMA-based scheduler which selects a single source-relay pair to access the channel during one scheduling unit (the selection criterion will be given in the next section). To facilitate the presentations, we denote the selected source and selected relay as S_{k^*} and R_{m^*}, respectively. After the scheduling is completed, the transmission is carried out in a two-phase manner. Specifically, S_{k^*} transmits its data to R_{m^*} in the first phase, and R_{m^*} re-transmits the received signal to D using standard AF protocol [10] in the second phase. The destination as well as the eavesdropper can hear the transmission from R_{m^*} and will perform decoding at the end of the second phase. Here, we assume that the first phase is secure and the information leakage only occurs during the second phase, which is attributed to the fact the the eavesdropper is near the destination and outside the transmission range of the first hop. It is further assumed that the channel state information (CSI) pertaining to the eavesdropper's channels is available at the legitimate nodes. This assumption is commonly adopted in the PHY-security literature such as [26], [28], and [32], and can be satisfied in cases where the eavesdropper is active and its transmission can be monitored.

Each node is equipped with a single antenna and operates in a half-duplex mode. All channels are assumed to be independent and modeled as flat block fading, which remain constant within one frame (a two-phase duration) and vary independently from frame to frame. The channel coefficient between node i and node j is represented by h_{ij}, which is a complex circularly symmetric Gaussian variable with mean zero and variance μ_{ij}. That is, $h_{ij} \sim \mathrm{CN}(0, \mu_{\mathrm{ij}})$. The average transmit powers at the selected source and the selected relay are denoted by P_{S} and P_{R} respectively, and we assume $P_{\mathrm{S}} = P_{\mathrm{R}} = P$ for simplicity. The additive noise at each receiver is modeled as a complex Gaussian variable with mean zero and variance N_0. The notation $\rho = P/N_0$ is used to represent the average signal-to-noise-ratio (SNR) of the system.

3 Distributed source-relay selection under eavesdropping attacks

3.1 Selection criterion

As is mentioned above, a single source-relay pair is selected for any frame transmission. According to the principle of the AF protocol and the considered system model, the kth ($1 \leq k \leq K$) source's received SNR at the

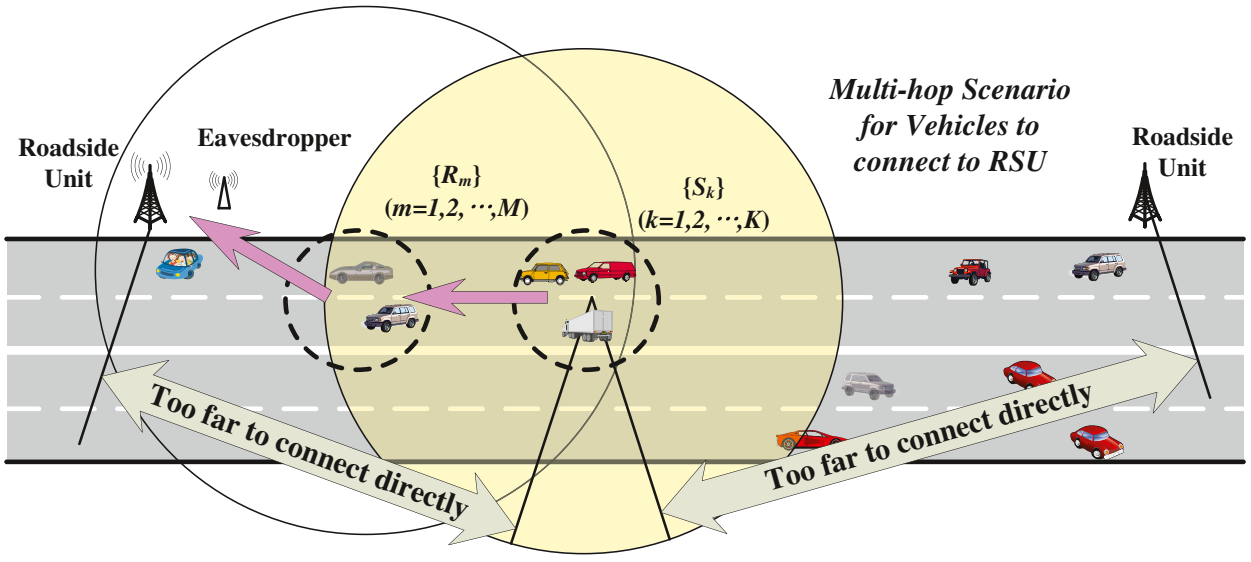

Figure 1 System model. *K* sources communicate with the destination via the help of *M* relays.

destination, with the help of the mth ($1 \le m \le M$) relay, can be expressed as

$$\gamma_{k,m}^{(d)} = \frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}, \tag{1}$$

where $\gamma_{s_k r_m} = P|h_{s_k r_m}|^2/N_0$ and $\gamma_{r_m d} = P|h_{r_m d}|^2/N_0$ are the instantaneous received SNR at the mth relay from the kth source and at the destination from the mth relay, respectively.

Similarly, the received SNR at the eavesdropper can be calculated as well by simply replacing $\gamma_{r_m d}$ in (1) by $\gamma_{r_m e}$, where $\gamma_{r_m e} = P|h_{r_m e}|^2/N_0$ is the instantaneous SNR of the link $R_m \to D$. Therefore, the instantaneous secrecy rate, defined as the difference between the achievable rate of the source-destination link and that of the source-eavesdropper link, can be formulated as

$$C_{\mathrm{S}}^{(k,m)} = \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}\right) - \frac{1}{2}\log_2\left(1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}\right)\right]^+, \tag{2}$$

where $[x]^+ = \max(0,x)$. In order to minimize the secrecy outage probability, defined as the probability that the instantaneous secrecy rate falls below a target secrecy rate, our criterion is to select such a source-relay pair (k^*, m^*) that can maximize the secrecy rate in (2). That is,

$$\begin{aligned}(k^*,m^*) &= \underset{1\le k\le K, 1\le m\le M}{\arg\max}\left\{\frac{1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}}{1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}}\right\} \\ &\triangleq \underset{1\le k\le K, 1\le m\le M}{\arg\max}\left\{\gamma_{e2e}^{(k,m)}\right\}\end{aligned} \tag{3}$$

With this criterion, the achievable secrecy outage probability can be expressed as

$$\begin{aligned}P_{\mathrm{out}}^{\mathrm{S}} &= \Pr\left[C_{\mathrm{S}}^{(k^*,m^*)} < R_{\mathrm{S}}\right] = \Pr\left[\frac{1}{2}\log_2\left(\gamma_{e2e}^{(k^*,m^*)}\right) < R_{\mathrm{S}}\right] \\ &= \Pr\left[\gamma_{e2e}^{(k^*,m^*)} < \nu\right],\end{aligned} \tag{4}$$

where R_{S} represents the target secrecy rate, and $\nu = 2^{2R_{\mathrm{S}}}$. Since R_{S} is positive, ν should be larger than 1.

If the global CSI is available at some node, e.g., the RSU, the criterion in (3) can be implemented in a centralized manner. However, it is non-trivial to obtain the CSI of all the involved links, especially for the networks with a large number of nodes. This motivates us to develop the distributed algorithm with low complexity, the details of which will be given in the next subsection.

3.2 Low-complexity distributed scheme

The proposed low-complexity design is based on the observation of (3), which tells us that the achievable secrecy rate is determined by $\gamma_{e2e}^{(k^*,m^*)}$, the maximum of $K \times M$ $\gamma_{e2e}^{(k,m)}$'s. According to the selection criterion in Sect. III. A, $\gamma_{e2e}^{(k^*,m^*)}$ can also be viewed as $\gamma_{e2e}^{(k^*,m^*)} = \max_{1\le m\le M}\{\gamma_{e2e}^{m}\}$, where γ_{e2e}^{m} is defined as

$$\gamma_{e2e}^{m} = \max_{1\le k\le K}\left\{\frac{1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}}{1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}}\right\} \tag{5}$$

With the above observation in mind, we can divide the overall selection procedure into three steps. First, every

relay node independently evaluates its eligibility for cooperation. After that, each eligible relay selects an appropriate source to maximize its contribution to the achievable secrecy rate. In this way, all the candidate source-relay pairs are generated. Finally, a single pair with the maximum $\gamma_{e2e}^{(k,m)}$ is screened out from the candidate pairs to access the channel. The details of these steps are given in the following:

- Step 1: Generating the Set of Eligible Relays. For any relay node R_m, it can be deduced from (3) that if $\gamma_{r_m d} < \gamma_{r_m e}$, then $\gamma_{e2e}^{(k,m)}$ will be less than 1, irrespective of the source index k. In other words, the system will be in outage if this relay node is selected to access the channel, no matter which source is chosen to form the pair.
  Further, when $\gamma_{r_m d} \geq \gamma_{r_m e}$, the secrecy outage probability, with R_m being the selected relay, can be expressed as

$$\begin{aligned} P_{\text{out}}^{S} &= \Pr\left[\gamma_{e2e}^{(k^*,m)} < \nu\right] \\ &\overset{(a)}{\geq} \Pr\left[\frac{\frac{\gamma_{s_{k^*} r_m}\gamma_{r_m d}}{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m d}}}{\frac{\gamma_{s_{k^*} r_m}\gamma_{r_m e}}{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m e}}} < \nu\right] \\ &= \Pr\left[\frac{\gamma_{r_m d}}{\gamma_{r_m e}} \times \frac{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m e}}{1+\gamma_{s_{k^*} r_m}+\gamma_{r_m d}} < \nu\right] \\ &= \Pr\left[\gamma_{s_{k^*} r_m}\left(\gamma_{r_m d} - \nu\gamma_{r_m e}\right) < \nu\gamma_{r_m e}\left(1+\gamma_{r_m d}\right)\right. \\ &\quad \left. - \gamma_{r_m d}\left(1+\gamma_{r_m e}\right)\right], \end{aligned} \tag{6}$$

  where (a) stems from the fact that $\frac{b+1}{a+1} < \frac{b}{a}$ for $a < b$. If $\gamma_{r_m e} < \gamma_{r_m d} < \nu\gamma_{r_m e}$, we have $\nu\gamma_{r_m e}\left(1+\gamma_{r_m d}\right) - \gamma_{r_m d}\left(1+\gamma_{r_m e}\right) > 0$ and $\gamma_{s_{k^*} r_m}\left(\gamma_{r_m d} - \nu\gamma_{r_m e}\right) < 0$. Therefore, the probability provided by (6) equals to 1, implying that the outage event definitely occurs if we choose such a relay to cooperate.
  Summarizing the discussions above, we can conclude that to support the target secrecy rate, the selected relay has to satisfy the following condition:

$$\gamma_{r_m d} > \nu\gamma_{r_m e} \tag{7}$$

  In other words, if the channel gains regarding R_m does not meet (7), R_m cannot be selected. In steps 2 and 3, we will only focus on the eligible relays satisfying (7).
  It should be emphasized that the eligibility determination process requires the knowledge of $\gamma_{r_m d}$ and $\gamma_{r_m e}$ at R_m. However, this can be guaranteed because we have assumed that both the RSU and the eavesdropper are active entities which will transmit control information or messages, and the corresponding channel gains can be estimated at the relays using the pilots from the received signals.
- Step 2: Source Selection at Eligible Relays. After step 1 has been finished, all the relays satisfying (7) broadcast flag signals to declare its eligibility for cooperation. Upon receiving the flag signals, all the sources will send an ACK to respond. With the received ACKs, any eligible relay R_m can estimate $\gamma_{s_k r_m}$ for all ks. After that, R_m supposes itself to be the selected relay and chooses the 'best' source which can contribute most to $\gamma_{e2e}^{(k,m)}$. To elaborate on how to find such a source node, a lemma will be introduced first.

Lemma 1. *The function*

$$f(\gamma) = \frac{1+\frac{\gamma_1\gamma}{1+\gamma_1+\gamma}}{1+\frac{\gamma_2\gamma}{1+\gamma_2+\gamma}}, \tag{8}$$

where γ_1 and γ_2 are two constants with γ_1 being larger than γ_2, is an increasing function of γ.

Proof. By taking the derivative of $f(\gamma)$ with respect to γ, we can obtain

$$f'(\gamma) = \frac{(1+\gamma_1)(\gamma_1-\gamma_2)}{(1+\gamma+\gamma_1)^2(1+\gamma_2)} \tag{9}$$

which is obviously larger than 0 for $\gamma_1 > \gamma_2$. Therefore, $f(\gamma)$ is an increasing function of γ. □

Based on this lemma, the 'best' source for R_m, i.e., $S_{k^*(m)}$, should be the one with the following property:

$$\begin{aligned} k^*(m) &= \arg\max_{1\leq k\leq K}\left\{\frac{1+\frac{\gamma_{s_k r_m}\gamma_{r_m d}}{1+\gamma_{s_k r_m}+\gamma_{r_m d}}}{1+\frac{\gamma_{s_k r_m}\gamma_{r_m e}}{1+\gamma_{s_k r_m}+\gamma_{r_m e}}}\right\} \\ &= \arg\max_{1\leq k\leq K}\gamma_{s_k r_m} \end{aligned} \tag{10}$$

  It is no doubted that step 2 also enjoys a distributed implementation since the source selection is performed at the eligible relays, and there is no information exchange among different relay nodes.
- Step 3: Distributed Source-Relay Pair Selection. Upon the completion of step 1 and step 2, we can formulate the expression for the maximum achievable secrecy rate by utilizing the mth relay as

$$C_{\text{S}}^{m} = \frac{1}{2}\log_2\left\{\frac{1+\frac{\gamma_{s_{k^*(m)} r_m}\gamma_{r_m d}}{1+\gamma_{s_{k^*(m)} r_m}+\gamma_{r_m d}}}{1+\frac{\gamma_{s_{k^*(m)} r_m}\gamma_{r_m e}}{1+\gamma_{s_{k^*(m)} r_m}+\gamma_{r_m e}}}\right\} \tag{11}$$

  To select the optimal source-relay pair, we adopt the method based on the distributed timer [14]. Specifically,

after calculating C_S^m, each eligible relay R_m will start its timer with the initial value inversely proportional to C_S^m. Therefore, the relay with the largest C_S^m, namely R_{m^*}, has its timer expired first. R_{m^*} then broadcasts the flag signal and the rest of the relays will back off after receiving the flag signal. Noticing the fact that the 'best' source for R_{m^*} has already been determined to be $S_{k^*(m*)}$ in step 2, we now have the selected source-relay pair.

Remark 1. The proposed source-relay selection scheme has two advantages. First, it can be realized in a distributed way, yielding a low implementation complexity. This is of practical significance for vehicular networks. Second, the distributed method, despite of its simplicity, is an optimal solution in the sense that it can select the 'best' source-relay pair to minimize the system secrecy outage probability.

4 Performance analysis

4.1 Secrecy outage probability

The secrecy outage probability (SOP) is widely adopted as a performance metric to evaluate the PHY-security protocol in wireless fading channels. As previously mentioned, it is defined as the probability that the instantaneous secrecy rate falls below a target secrecy rate $R_S > 0$. By noticing that the M γ_{e2e}^m's are independent random variables, the SOP can be expressed as

$$P_{\text{out}}^S = \Pr\left[\gamma_{e2e}^{(k^*,m^*)} < \nu\right] = \prod_{m=1}^{M} \Pr\left(\gamma_{e2e}^m < \nu\right) \tag{12}$$

By combining (5) and (10), γ_{e2e}^m can be expressed as

$$\gamma_{e2e}^m = \frac{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_md}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_md}}}{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_me}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_me}}}, \tag{13}$$

where $\gamma_{s_{k^*(m)}r_m} = \max\limits_{1\le k\le K}\left\{\gamma_{s_kr_m}\right\}$.

Therefore, denoting $\gamma_{s_{k^*(m)}r_m}$, γ_{r_md}, and γ_{r_me} by X, Y, and Z, respectively, the probability $\Pr\left(\gamma_{e2e}^m < \nu\right)$ can be calculated as

$$\begin{aligned}\Pr\left(\gamma_{e2e}^m < \nu\right) &= \Pr\left[\frac{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_md}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_md}}}{1 + \frac{\gamma_{s_{k^*(m)}r_m}\gamma_{r_me}}{1+\gamma_{s_{k^*(m)}r_m}+\gamma_{r_me}}} < \nu\right] \\ &= \int_{y<vz} f_Y(y)f_Z(z)dydz \\ &\quad + \int_{y>vz} \Pr\left[\frac{1+\frac{Xy}{1+X+y}}{1+\frac{Xz}{1+X+z}} < \nu\right] f_Y(y)f_Z(z)dydz,\end{aligned} \tag{14}$$

where $f_X(x)$ is the probability density function (PDF) of the random variable X. The intractability of the PDF of γ_{e2e}^m makes it rather difficult to calculate the accurate result of the integral in the second part of (14). Therefore, we resort to the approximation $\frac{\gamma_1\gamma_2}{1+\gamma_1+\gamma_2} \approx \min\{\gamma_1,\gamma_2\}$, which is rather tight for large values of γ_1 and γ_2 [34]. Then, the second part of the right-hand side of (14), denoted by I, is approximated as

$$\begin{aligned}I &\approx \int_{y>vz} \Pr\left[\frac{1+\min(X,y)}{1+\min(X,z)} < \nu\right] f_Y(y)f_Z(z)dydz \\ &= \int_{vz<y<vz+v-1} f_Y(y)f_Z(z)dydz \\ &\quad + \int_{y>vz+v-1} \Pr\left[X < \nu(1+z)-1\right] f_Y(y)f_Z(z)dydz\end{aligned} \tag{15}$$

Combining (14) and (15), the approximate expression for the probability $\Pr\left(\gamma_{e2e}^m < \nu\right)$ can be given by

$$\begin{aligned}\Pr\left(\gamma_{e2e}^m < \nu\right) \approx &\overbrace{\int_{y<vz+v-1} f_Y(y)f_Z(z)dydz}^{I_1} \\ &+ \overbrace{\int_{y>vz+v-1} \Pr\left[X<\nu(1+z)-1\right] f_Y(y)f_Z(z)dy\,dz}^{I_2}\end{aligned} \tag{16}$$

For the considered Rayleigh fading channels, γ_{ij} follows the exponential distribution with the rate parameter $\lambda_{ij} = \left(\rho\mu_{ij}\right)^{-1}$. Therefore, I_1 in (16) can be obtained as

$$\begin{aligned}I_1 &= \int_0^\infty \int_0^{\nu(z+1)-1} \lambda_{r_md}\lambda_{r_me} e^{-\lambda_{r_md}y-\lambda_{r_me}z} dydz \\ &= 1 - \frac{\lambda_{r_me}e^{-\lambda_{r_md}(\nu-1)}}{\lambda_{r_md}\nu + \lambda_{r_me}}\end{aligned} \tag{17}$$

On the other hand, $X = \gamma_{s_{k^*(m)}r_m}$ is the maximum of K independently and non-identically distributed exponential random variables. According to the order statistics, I_2 in (16) can be simplified as

$$\begin{aligned}I_2 = &\int_{\nu-1}^\infty \left[\int_0^{\frac{y+1-\nu}{\nu}} \prod_{k=1}^{K}\left(1-e^{-\lambda_{s_kr_m}(\nu(1+z)-1)}\right)\lambda_{r_me}e^{-z\lambda_{r_me}}dz\right] \\ &\times\lambda_{r_md}e^{-y\lambda_{r_md}}dy = \int_{\nu-1}^\infty \int_0^{\frac{y+1-\nu}{\nu}} \sum_{n=0}^{K} \sum_{\substack{1\le p_1,p_2,\ldots,p_K\le K \\ p_i\ne p_j,\forall i\ne j \\ p_1<p_2<\cdots<p_n \\ p_{n+1}<p_{n+2}<\cdots<p_K}} \\ &\times(-1)^{K-n}e^{-\left(\sum\limits_{k=n+1}^{K}\lambda_{s_{p_k}r_m}\right)(\nu(1+z)-1)} \times\left(\lambda_{r_me}e^{-\lambda_{r_me}z}\right)dz \\ &\times\left(\lambda_{r_md}e^{-\lambda_{r_md}y}\right)dy,\end{aligned} \tag{18}$$

where we have utilized the multinomial expansion identity given by [35], e.q. (7). After some tedious calculations, I_2 can be finally simplified as

$$I_2 = \sum_{n=0}^{K} \sum_{\substack{1\le p_1,p_2,\ldots,p_K\le K \\ p_i\neq p_j,\forall i\neq j \\ p_1<p_2<\cdots<p_n \\ p_{n+1}<p_{n+2}<\cdots<p_K}} (-1)^{K-n} e^{-\sum_{k=n+1}^{K}\lambda_{s_{p_k}r_m}(\nu-1)} \times \frac{\lambda_{r_me}e^{-\lambda_{r_md}(\nu-1)}}{\lambda_{r_me}+\sum_{k=n+1}^{K}\lambda_{s_{p_k}r_m}\nu} \times \left[1-\frac{\nu\lambda_{r_md}}{\nu\lambda_{r_md}+\lambda_{r_me}+\sum_{k=n+1}^{K}\lambda_{s_{p_k}r_m}\nu}\right] \tag{19}$$

Substituting (17) and (19) into (16), the closed-form expression for $\Pr\left(\gamma_{e2e}^{m}<\nu\right)$ is obtained, and the SOP of the system can also be derived by substituting this result into (12). However, we omit these expressions here due to space limitation. In the next section, we will show through simulations that the derived theoretical result is tight enough for medium to high SNR values.

4.2 Intercept probability

The intercept probability, which is also a key metric in evaluating the performance of PHY-layer security schemes, is defined as the probability that the capacity of the legitimate link falls below that of the wiretap link [32]. Mathematically speaking, the intercept probability can be expressed as

$$P_{\text{intercept}} = \Pr\left[\gamma_{e2e}^{(k^*,m^*)}<1\right] = \prod_{m=1}^{M}\Pr\left(\gamma_{e2e}^{m}<1\right) \tag{20}$$

According to the expression for γ_{e2e}^{m} in (13), the event $\gamma_{e2e}^{m}<1$ is equivalent to

$$\frac{\gamma_{r_md}}{\gamma_{r_me}}\times\frac{1+\gamma_{s_{k^*}r_m}+\gamma_{r_me}}{1+\gamma_{s_{k^*}r_m}+\gamma_{r_md}}<1 \tag{21}$$

Therefore, $\Pr\left[\gamma_{e2e}^{m}<1\right]$ can be calculated as

$$\Pr\left(\gamma_{e2e}^{m}<1\right) = \int_{y<z} f_Y(y)f_Z(z)dydz + \int_{y>z}\Pr\left[\frac{y(1+X+z)}{z(1+X+y)}<1\right]f_Y(y)f_Z(z)dydz, \tag{22}$$

where $X=\gamma_{s_{k^*(m)}r_m}$, $Y=\gamma_{r_md}$, and $Z=\gamma_{r_me}$. The probability in the second integral in (22) can be rewritten as

$$\Pr\left[\frac{y(1+X+z)}{z(1+X+y)}<1\right] = \Pr\left[X(y-z)<z(1+y)-y(1+z)\right] = \Pr\left[X(y-z)<z-y\right] \tag{23}$$

which is always zero for $y>z$. By inserting this result into (22), we have

$$\Pr\left(\gamma_{e2e}^{m}<1\right) = \int_{y<z} f_Y(y)f_Z(z)dydz = \frac{\lambda_{r_md}}{\lambda_{r_md}+\lambda_{r_me}} \tag{24}$$

Combing (24) with (20), the exact expression for the intercept probability can be given by

$$P_{\text{intercept}} = \prod_{m=1}^{M}\frac{\lambda_{r_md}}{\lambda_{r_md}+\lambda_{r_me}} \tag{25}$$

4.3 Diversity order

In order to gain some useful insights into the system performance, we proceed to analyze the achievable diversity order. Since the the intercept probability is not a function of the average SNR, the traditional definition of diversity order is not applicable here. Instead, we adopt the definition of generalized diversity order given in [32], which is formulated as

$$d \triangleq -\lim_{\kappa_{de}\to\infty}\frac{\log P_{\text{intercept}}}{\log\kappa_{de}}, \tag{26}$$

where $\kappa_{de}=\mu_{sd}/\mu_{se}$ is known as the main-to-eavesdropper ratio (MER), defined as the ratio of the average channel gain of the source-destination link to that of the source-to-eavesdropper link.

To simplify the discussions, we assume that there is only one source node. Denoting $\mu_{r_md}=\mu_{sd}\alpha_{r_md}$ and $\mu_{r_me}=\mu_{se}\alpha_{r_me}$, the intercept probability in (25) can be rewritten as

$$\begin{aligned} P_{\text{intercept}} &= \prod_{m=1}^{M}\frac{\frac{1}{\rho\mu_{sd}\alpha_{r_md}}}{\frac{1}{\rho\mu_{sd}\alpha_{r_md}}+\frac{1}{\rho\mu_{se}\alpha_{r_me}}} \\ &= \prod_{m=1}^{M}\frac{1}{1+\frac{\mu_{sd}}{\mu_{se}}\alpha_m} \\ &= \left(\frac{1}{\kappa_{de}}\right)^{M}\prod_{m=1}^{M}\frac{1}{\frac{1}{\kappa_{de}}+\alpha_m}, \end{aligned} \tag{27}$$

where we have introduced α_m to represent $\frac{\alpha_{r_md}}{\alpha_{r_me}}$.

Based on the calculations above, the diversity order can be derived as

$$d = \lim_{\kappa_{de}\to\infty} \frac{M\log\kappa_{de} + \sum_{m=1}^{M}\log\left(\frac{1}{\kappa_{de}+\alpha_m}\right)}{\log\kappa_{de}} = M \quad (28)$$

5 Simulation results and discussions

In this section, we present the simulation results to validate the proposed source-relay selection scheme. In the following simulations, all the nodes (including the sources, the relays, the destination, and the eavesdropper) are distributed in a 2-D plane. The direct links of $S_k \to D$ and $S_k \to E$ are assumed to be absent for all k's, and the the channel gains are modeled according to the system model in Section 2. To be specific, $h_{ij} \sim CN\left(0, \mu_{ij}\right)$, where $\mu_{ij} = d_{ij}^{-\theta}$ with d_{ij} being the distance between any node pair (i,j) and θ being the path loss exponent. In our simulations, θ is fixed as 3. Unless otherwise stated, the target secrecy rate R_S is set to be 0.1 bit/s/Hz, and the notation 'SNR' is used to represent the ratio of P versus N_0, i.e., ρ in the previous sections.

In Figures 2 and 3, we consider the system with three sources and two relays, i.e., $K = 3$ and $M = 2$. These nodes are uniformly generated in the circle with center (0,0) and radius 1. The destination and the eavesdropper are located at (2,0) and (2,2), respectively. Figure 2 shows the SOP-SNR curves for the proposed anti-eavesdropping selection scheme and the conventional joint source-relay selection scheme [17]. The theoretical result is also given to verify the correctness of the analysis in Section 4.1. From Figure 2, it can be seen that by taking the security constraints into account, the proposed scheme brings non-negligible gains compared to the conventional scheme, which only considers the channel qualities regarding the legitimate links. In addition, there is an excellent match between the theoretical curve and the simulated one for medium to high SNR values, implying the soundness of the theoretical analysis.

In Figure 3a, we compare the ergodic secrecy capacity of the proposed scheme (C_1) and that of the conventional scheme (C_2). To illustrate the capacity loss incurred by the secrecy constraint, we calculate the ergodic capacity for the system without eavesdroppers (C_0) and present the differences $C_0 - C_1$ and $C_0 - C_2$ in Figure 3b[a]. One can observe from Figure 3a that the proposed scheme outperforms the conventional scheme in terms of the secrecy capacity. However, the secrecy capacities of both the two schemes almost saturate as the SNR tends to infinity. This is because that as SNR gets larger, the achievable rate of the legitimate link as well as the eavesdropper link increases. Comparably, without the existence of the eavesdroppers, the system capacity increases linearly with SNR, which is due to the multi-user diversity gain [17]. This explains the phenomenon in Figure 3b, which clearly reflects the capacity penalty to support the secrecy constraints.

Figure 4 plots the system intercept probability as a function of the MER κ_{de}. In this figure, we assume $K = 1$ and fix SNR to be 20 dB. The source node and destination node are located at (0,0) and (2,0), respectively. The location of the eavesdropper is determined according to the value of κ_{de}. Other simulation parameters are the

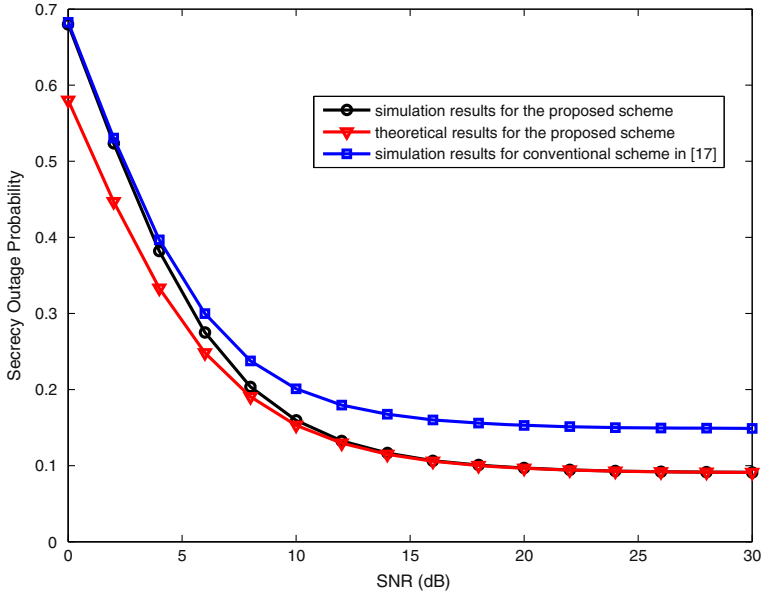

Figure 2 The secrecy outage probability versus the system average SNR. $K = 3, M = 2, R_S = 0.1$ bit/s/Hz.

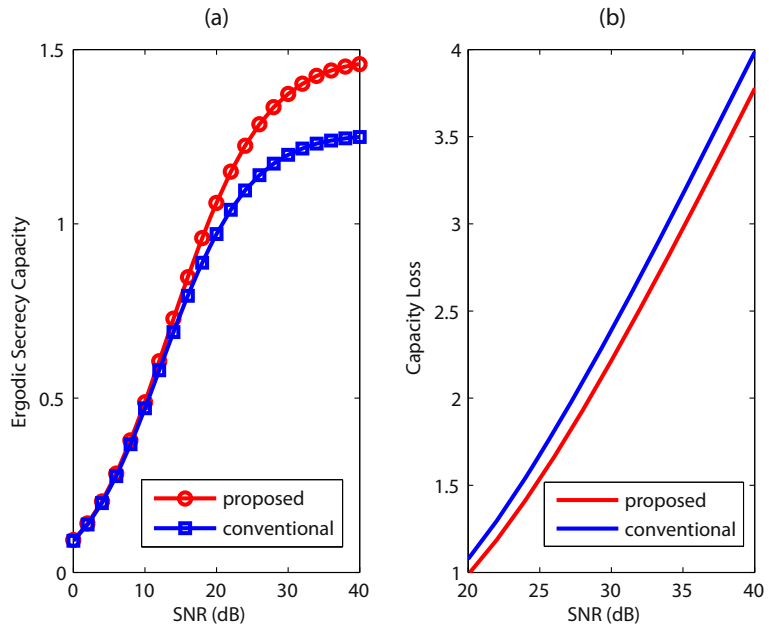

Figure 3 The ergodic secrecy capacity of the system. (a) The secrecy capacity comparison between the proposed and the conventional scheme. **(b)** The capacity loss relative to the system without eavesdroppers. $K = 3, M = 2$.

same as those for producing the results in Figures 2 and 3. From Figure 4, it can be seen that for various values of M, the theoretical results exactly match the simulated ones, indicating the correctness of the performance analysis in Section 4.2. In addition, the slopes of the curves illustrate that the diversity order of M is achieved by our protocol, which is in accordance with the analysis in Section 4.3.

In Figures 5, 6, 7 and 8, the impact of some key parameters on the system secrecy performance will be examined. In these figures, we locate the $K = 3$ sources at $\left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$, $\left(-\frac{1}{\sqrt{2}}, 0\right)$, and $\left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$. The $M = 2$ relays are distributed at $\left(\frac{1}{2}, \frac{1}{2}\right)$ and $\left(\frac{1}{2}, -\frac{1}{2}\right)$. In Figures 5 and 6, the positions of the destination and the eavesdropper are fixed as (2,0) and (2,2), respectively. In Figures 7 and 8, the destination is also located at (2,0), whereas the eavesdropper's position varies within the rectangular region $[-3, 3] \times [-3, 3]$.

Figure 5 presents the curve of the system secrecy outage probability and exhibits how it varies with the target secrecy rate R_S. In this figure, five representative SNR

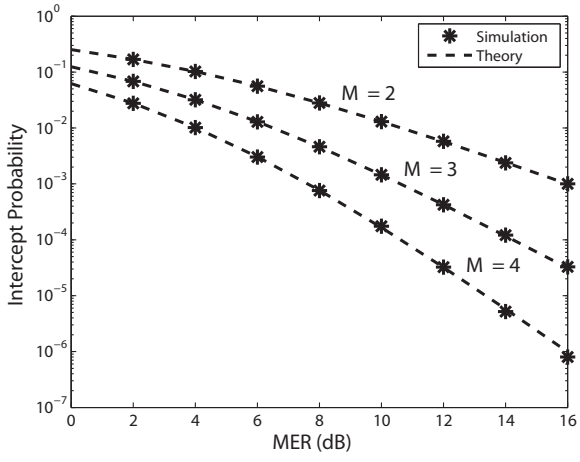

Figure 4 The intercept probability versus the main-eavesdropper ratio (MER). $K = 1; M = 2, 3, 4$; SNR = 20 dB.

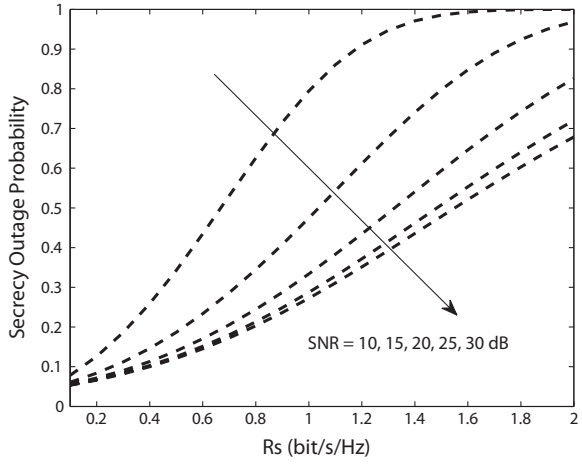

Figure 5 The secrecy outage probability versus the target secrecy rate R_S. $K = 3, M = 2$.

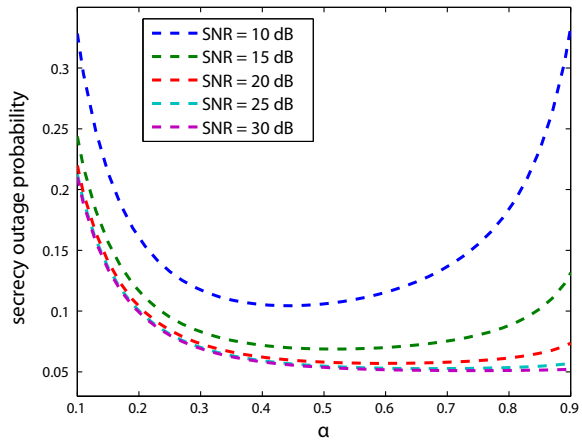

Figure 6 The secrecy outage probability versus the power allocation factor α. $K = 3, M = 2, R_S = 0.1$ bit/s/Hz.

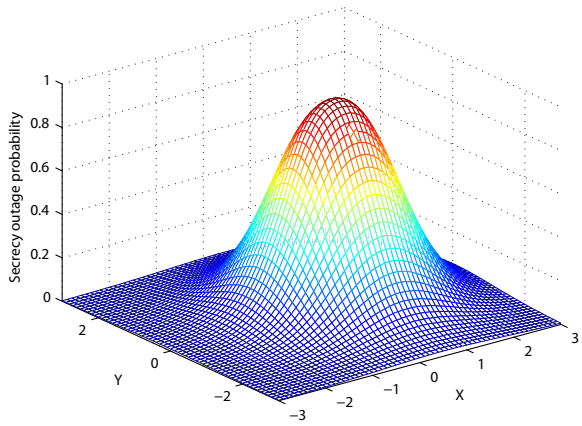

Figure 8 The secrecy outage probability versus the locations of the eavesdropper. $K = 3, M = 2$, SNR = 20 dB.

values are considered. As expected, when the target rate increases, the SOP increases as well.

In Figure 6, the effect of the power allocation ratio on the achievable SOP is investigated. Specifically, given the total transmit power P_{tot}, we allocate αP_{tot} to the selected source, and $(1-\alpha)P_{\text{tot}}$ to the selected relay. As α changes from 0 to 1, the SOP as a function of α is shown in Figure 6. Here, we plot a set of SOP curves, each corresponding to a specific SNR value. It should be pointed out that in Figure 6, the notation 'SNR' represents the ratio of the total transmit power for two phases versus N_0, which is different from the previous figures. An important observation from Figure 6 is that in order to optimize the system performance, α should be neither too large nor too small. The reasons can be briefly given as follows. If α is too large, the relay-destination link will be in poor channel quality, which significantly limits the achievable rate at the destination. On the other hand, if α is too small, implying that more power is allocated to the relay node, the eavesdropper will benefit from the improved quality of the relaying channel, which also decreases the secrecy rate. From Figure 6, we can also find that the system performance is satisfactory for $\alpha = 0.5$. Therefore, the equal power allocation scheme, which is assumed in our work, is near-optimal despite its simplicity.

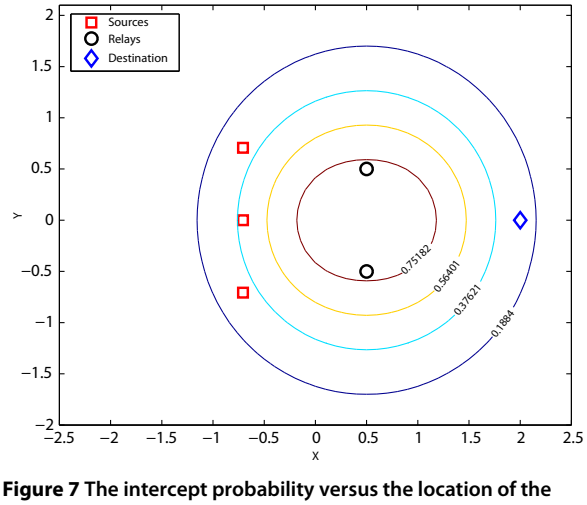

Figure 7 The intercept probability versus the location of the eavesdropper. $K = 3, M = 2$, SNR = 20 dB. The numbers on the curves represent the achievable intercept probabilities.

Figure 7 shows the relationship between the eavesdropper's location and the intercept probability. From this figure, we can observe that the intercept probability increases significantly when the eavesdropper moves towards the relay nodes. This is obvious because the closer the eavesdropper to the relays, the better the channel quality of the relay-eavesdropper link. Figure 8 presents the secrecy outage probability versus the eavesdropper's location. As expected, the impact of the eavesdropper's location on the SOP is similar to that on the intercept probability.

6 Conclusions

In this paper, a joint source-relay selection scheme is proposed for vehicular networks under eavesdropping attacks. The proposed scheme maximizes the instantaneous secrecy rate of the system and, hence, can minimize the achievable secrecy outage probability. We present the selection criterion and also give a low-complexity method to realize this criterion in a distributed manner. The system performance is analyzed in terms of the secrecy outage probability, the intercept probability, and the achievable diversity order. Finally, the effectiveness of the proposed scheme and the correctness of the theoretical analysis are verified through extensive simulations.

There are several interesting issues worthy of further investigations. For example, in this work, we assume that the channel gains regarding the eavesdropper's link is available, which may not be realistic for some scenarios where the eavesdroppers are passive entities. Besides that, it will be of practical significance to generalize the proposed work to the systems with multiple eavesdroppers and (or) multiple destinations.

Endnote

[a]For the multi-source multi-relay network without eavesdroppers, the best source-relay pair is selected according to the method in [17].

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

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. 2013ZX03003004-003), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (No. 2012D04), and the Fundamental Research Funds for the Central Universities of China.

Author details

[1]Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China. [2]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China.

Received: 31 December 2013 Accepted: 16 June 2014
Published: 4 July 2014

References

1. H Hartenstein, KP Laberteaux, A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
2. G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Commun. Surv. Tutor. **13**(4), 584–616 (2011)
3. CF Mecklenbrauker, AF Molisch, J Karedal, F Tufvesson, A Paier, L Bemado, T Zemen, O Klemp, N Czink, Vehicular channel characterization and its implications for wireless system design and performance. Proc. IEEE **99**(7), 1189–1212 (2011)
4. VP Harigovindan, AV Babu, L Jacob, Ensuring fair access in IEEE 802.11p-based vehicle-to-infrastructure networks. EURASIP J. Wireless Commnun. Netw. **2012**, 17 (2012). doi:10.1186/1687–1499-2012-168
5. T Zhou, H Sharif, M Hempel, P Mahasukhon, W Wang, T Ma, A novel adaptive distributed cooperative relaying MAC protocol for vehicular networks. IEEE J. Select. Areas Commun. **29**(1), 72–82 (2011)
6. J Nzouonta, N Rajgure, G Wang, C Borcea, VANET routing on city roads using real-time vehicular traffic information. IEEE Trans. Veh. Technol. **58**(6), 3609–3626 (2009)
7. MH Eiza, Q Ni, An evolving graph-based reliable routing scheme for VANETs. IEEE Trans. Veh. Technol. **62**(4), 1493–1504 (2013)
8. JC Lin, CS Lin, CN Liang, BC Chen, Wireless communication performance based on IEEE 802.11p R2V field trails. IEEE Commun. Mag. **50**(5), 184–191 (2012)
9. A Sendonaris, E Erkip, B Aazhang, User cooperation diversity - part I: system description. IEEE Trans. Commun. **51**(11), 1927–1938 (2003)
10. JN Laneman, DNC Tse, GW Wornell, Cooperative diversity in wireless networks: efficient protocols and outage behavior. IEEE Trans. Inf. Theory **50**(12), 3062–3080 (2004)
11. KG Seddik, AS Ibrahim, KJR Liu, Trans-modulation in wireless relay networks. IEEE Commun. Lett. **12**(3), 170–172 (2008)
12. T Wang, GB Giannakis, R Wang, Smart regenerative relays for link-adaptive cooperative communications. IEEE Trans. Commun. **56**(11), 1950–1960 (2008)
13. W Zhang, KB Letaief, Full-rate distributed space-time codes for cooperative communications. IEEE Trans. Wireless Commun. **7**(7), 2446–2451 (2008)
14. A Bletsas, A Khisti, DP Reed, A Lippman, A simple cooperative diversity method based on network path selection. IEEE J. Select. Areas Commun. **24**(3), 659–672 (2006)
15. Z Ding, KK Leung, DL Goeckel, D Towsley, On the study of network coding with diversity. IEEE Trans. Wireless Commun. **8**(3), 1247–1259 (2009)
16. M Zeng, R Zhang, S Cui, On the design of distributed beamforming for two-way relay networks. IEEE Trans. Signal Process. **59**(5), 2284–2295 (2011)
17. L Sun, T Zhang, L Lu, H Niu, On the combination of cooperative diversity and multiuser diversity in multi-source multi-relay wireless networks. IEEE Signal Process Lett. **17**(6), 535–538 (2010)
18. H Ding, J Ge, DB da Costa, Z Jiang, A new efficient low-complexity scheme for multi-source multi-relay cooperative networks. IEEE Trans. Veh. Technol. **60**(2), 716–722 (2011)
19. M Seyfi, S Muhaidat, J Liang, M Uysal, Relay selection in dual-hop vehicular networks. IEEE Signal Process Lett. **18**(2), 134–137 (2011)
20. Y Ge, S Wen, Y-H Ang, Y-C Liang, Optimal relay selection in IEEE 802.16j multihop relay vehicular networks. IEEE Trans. Veh. Technol. **59**(5), 2198–2206 (2010)
21. Z Ding, KK Leung, Cross-layer routing using cooperative transmission in vehicular ad-hoc networks. IEEE J. Select. Areas Commun. **29**(3), 571–581 (2011)
22. SC Ng, W Zhang, Y Zhang, Y Yang, G Mao, Analysis of access and connectivity probabilities in vehicular relay networks. IEEE J. Select. Areas Commun. **29**(1), 140–150 (2011)
23. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
24. I Csiszár, J Körner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1978)
25. M Bloch, J Barros, MRD Rodrigues, SW McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory **54**(6), 2515–2534 (2008)
26. E Tekin, A Yener, The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming. IEEE Trans. Inf. Theory **54**(6), 2735–2751 (2008)
27. I Krikidis, JS Thompson, S McLaughlin, PM Grant, A feedback-based transmission for wireless networks with energy and secrecy constraints. EURASIP J. Wireless Commun. Netw. **2011**, 11 (2011). doi:10.1155/2011/313269
28. L Dong, Z Han, AP Petropulu, HV Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
29. I Krikidis, JS Thompson, S McLaughlin, Relay selection for secure cooperative networks with jamming. IEEE Trans. Wireless Commun. **8**(10), 5003–5011 (2009)
30. Y Liu, J Li, AP Petropulu, Destination assisted cooperative jamming for wireless physical-layer security. IEEE Trans. Inf. Forensic Secur. **8**(4), 682–694 (2013)
31. L Sun, Q Du, P Ren, Secrecy-enhanced data dissemination using cooperative relaying in vehicular networks. Int. J. Distrib. Sens. Netw. **2013**, 505831 (2013)
32. Y Zou, X Wang, W Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J. Select. Areas Commun. **31**(10), 2099–2111 (2013)
33. V Bao, N L-Trung, M Debbah, Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. IEEE Trans. Wireless Commun. **12**(12), 6076–6085 (2013)
34. S Ikki, MH Ahmed, Performance analysis of cooperative diversity wireless networks over Nakagami-m fading channel. IEEE Commun. Lett. **11**(4), 334–336 (2007)
35. F Xu, FCM Lau, QF Zhou, DW Yue, Outage performance of cooperative communication systems using opportunistic relaying and selection combining receiver. IEEE Signal Process Lett. **16**(4), 237–240 (2009)

doi:10.1186/1687-1499-2014-109
Cite this article as: Sun *et al.*: Distributed source-relay selection scheme for vehicular relaying networks under eavesdropping attacks. *EURASIP Journal on Wireless Communications and Networking* 2014 **2014**:109.