Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 9624856, 15 pages
https://doi.org/10.1155/2018/9624856

*Research Article*

# A Novel Approach to Enhance the Physical Layer Channel Security of Wireless Cooperative Vehicular Communication Using Decode-and-Forward Best Relaying Selection

**Esraa M. Ghourab**,[1] **Mohamed Azab**,[2,3] **Mohamed F. Feteiha**,[2,4,5] **and Hesham El-Sayed**[6]

[1]*Electrical Engineering Department, Alexandria University, Alexandria, Egypt*
[2]*Informatics Research Institute, The City of Scientific Research and Technological Applications, Alexandria, Egypt*
[3]*ACIS, Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA*
[4]*Electrical and Computer Engineering Department, Faculty of Engineering, University of Waterloo, Waterloo, Ontario, Canada*
[5]*Systems Design Engineering Department, Smart-Nations Technology Development Inc., Ontario, Canada*
[6]*Computer and Network Engineering Department, United Arab Emirates University, Al-Ain, UAE*

Correspondence should be addressed to Esraa M. Ghourab; esraa.m.ghourab@mena.vt.edu

Received 24 October 2017; Revised 30 January 2018; Accepted 15 April 2018; Published 28 May 2018

Academic Editor: Hongwei Wang



This paper proposes a novel approach to enhance wireless vehicle-to-vehicle channel-secrecy capacity by imposing signal transmission diversity. This work exploits cooperative vehicular relaying to extract the associated underlying multipath and Doppler diversity using precoding techniques. We evaluated the capacity and diversity gain for the presented approach to ensure its effectiveness and efficiency. The abundance of moving vehicles, operating in an ad hoc fashion, can eliminate the need to establish a dedicated relaying infrastructure. A relay selection scheme is deployed, taking advantage of the potentially large number of available relaying vehicles. Further, we derivate a closed-form mathematical expression for the channel-secrecy capacity, diversity order gain, and the intercept probability. We used the direct transmission scenario as a reference to assess our analysis. Our analytical and simulation results for the presented model showed that channel-secrecy capacity and performance-indicators improved significantly.

## 1. Introduction

In large cities, the complex network of diverse people and the exponentially increasing service demands urge leading telecommunication networking to improve the communication capabilities.

In the search for ways to enhance network performance and security, researchers and practitioners started to consider offloading such heavy burden to road-traveling vehicles. The abundant on-vehicle computing resources may be underutilized by the traditional vehicular applications. Many wireless communication technologies are available for "Vehicular Ad hoc Networks (VANETs)" communications, including traditional wireless technologies or technologies specifically introduced for the vehicular environment.

In most practical scenarios, due to the broadcast nature of the system, legal user's data can be easily overheard, altered, or blocked by malicious parties (eavesdropping attacks). VANETs physical layer designs need to cope with tremendous security challenges. However, the conventional physical layer security technique depends mainly on the replication for reliability and encryption for security [1–6]. Antenna diversity is used to address the aforementioned challenges by enhancing signal quality, such as MIMO and cooperative diversity using replication.

Additionally, researchers proved that, even with computationally expensive resources, eavesdropper can still decrypt heavily encrypted data [7]. In [8, 9], Wyner presented the concept of channel secrecy as an indication of data transmission security. Channel secrecy is defined as the

relation between the channel capacity of the main link (from source to destination) and the wire-tap link (from source to eavesdropper). Channel-secrecy capacity was evaluated in Gaussian wire-tap channel as the difference between the channel capacity of the main link and that of the wire-tap link [9].

Cooperative communication has the ability to improve the overall channel-secrecy capacity for any given set of bandwidths [10, 11], with the appropriate relay selection.

In [12], authors presented the effect of Decode-and-Forward (DF) relay selection mechanisms on channel secrecy and intercept probability without a direct link. They presented the optimal and traditional (Max-Min) relay selection mechanisms.

Authors presented in [6] performance comparison between both cooperative diversity protocols Amplify-and-Forward (AF) and Decode-and-Forward (DF) for ergodic channel-secrecy capacity and intercept probability. They proved that AF cooperative protocol has better intercept probability than DF protocol. Furthermore, in [11], authors presented the ergodic channel-secrecy capacity for DF cooperative protocol in case of a direct link. Their analysis was derived from Independent Nonidentical Distribution (i.n.i.d) cooperative link, assuming Maximal Likelihood (ML) scenario at the destination node. They proved that the (i.n.i.d) DF cooperative protocol with the existence of direct link has low intercept probability.

In this paper, we adopted the model presented in [13, 14] to device an enhanced version towards more secure vehicular networks. Additionally, we present a vehicle-to-vehicle communication model assessment using intercept probability and channel secrecy as an indication of how secure the system can be in the presence of attackers.

Authors in [13] presented precoded multihop vehicular transmission with cooperative DF relaying to forward the signal from a source vehicle to a destination vehicle in the absence of a direct link. Moreover, they determined the analytical tight upper bound expressions for the Pairwise Error Probability (PEP) and diversity gain. Their performance analysis through PEP showed that, via proper precoding, the proposed system is able to extract the maximum available diversity in multiple dimensions. These dimensions can be summarized as follows: time dimension (through Doppler diversity), frequency dimension (through multipath diversity), and space dimension (through best relaying vehicle selection).

In this paper, we use the above-mentioned modified system [13], considering that there is a direct link between vehicles. We exploit direct transmission and cooperative terminals links to increase the channel-secrecy capacity of VANETs system without increasing the bandwidth.

However, our vehicle model assumes that vehicles are traveling on a highway with a fixed speed. Given the fact that our presented model relies mainly on moving vehicles with no presence of roadside units, considering the vehicle speed in this scenario is not applicable. Our future work will consider vehicle speed among other communication characteristics in totally different scenarios to be presented in our sequel papers.

The main contributions of this paper can be summarized as follows:

(i) Derive a closed form for the optimal channel-secrecy capacity and intercept probability for both direct and DF cooperative links. We rely on a precoded cooperative transmission technique to extract the underlying rich multipath-Doppler-spatial diversity.

(ii) Evaluate the proposed best relay selection scheme in presence of eavesdropper among large number of moving vehicle relays.

(iii) Derive a mathematical closed-form expression for diversity order by combining direct and cooperative links diversity.

(iv) Derive closed form for the outage probability of our proposed model, showing the benefits of combining direct and cooperative links in the vehicular diversity model.

The paper is organized as follows: Section 2 describes the proposed two-phase dual-hop cooperative system model, with best relay selection. Section 3 presents the derivation of channel-secrecy capacity and intercept probability closed-form expressions. Section 4 presents numerical results to confirm the analytical derivations. Finally, we conclude the paper in Section 5.

## 2. System Model

In this section, we explain an overview of the system model from a communication point of view and provide a description of how the presented approach improves the system performance. Secondly, we explain the system model in the presence of an eavesdropper and provide description of security improvement. Finally, we discuss the optimal relay selection technique to improve the secrecy capacity.

*2.1. Base System Model.* In this section, we explain the idea of the overall system from the communication and security points of view. We propose an efficient cooperative vehicular transmission technique to create advanced heterogeneous telecommunication networks in an approach for increasing the networking capabilities of heavily populated urban areas. Our transmission scheme is built by making use of on-road vehicles equipped with low-elevation antennas as well as short- and medium-range wireless communication technologies.

Vehicular networks are expected to offer reasonable throughput, lower operational cost, and more flexible configuration. The realization of cooperative vehicular relaying entails many challenges, all of which require dynamic and real-time remedies. The full potential for expanding any network of this scale entails complexities referring to a reliable communication link, optimized transmission schemes, and eventually information extraction.

We remark that there are mainly two approaches to handle this type of high communication mobility. The first approach involves adaptive transmission in which one or more transmission parameters (coding, modulation, power,

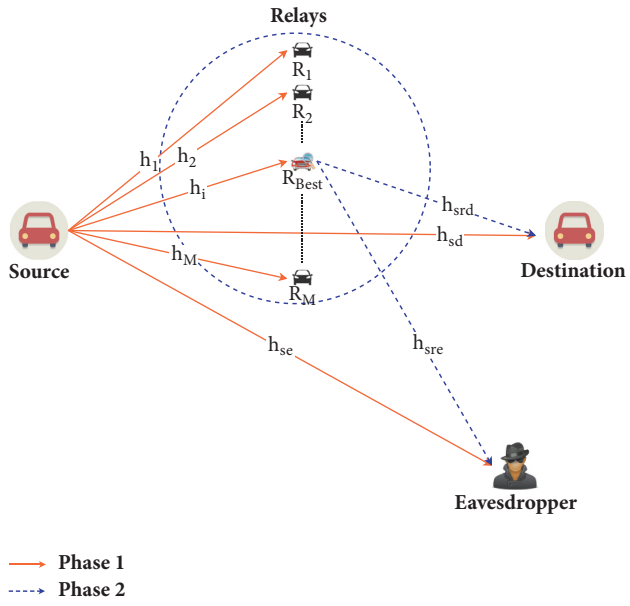



FIGURE 1: System model of cooperative relay communication in the presence of an eavesdropper node with existing direct link.

etc.) are varied according to the channel conditions. This builds on closed-loop implementation in which a feedback from the receiver to the transmitter is required. The second approach is based on using either outer coding or precoding. This approach is open-loop implementation and does not require any feedback from the transmitter. Such techniques are particularly useful over time-varying channels, where reliable feedback is difficult to obtain.

Considering the time-selective nature of the vehicular system under consideration in this paper, we used the linear constellation precoding (LCP) approach [15]. Taking this into consideration, we built our communication scheme over orthogonal transmission protocols, cooperative relaying, and linear signal precoding.

*2.2. Proposed Model.* This paper proposes a cooperative communication scenario shown in Figure 1, which consists of one source, one destination, and a set of $M$ Decode-and-Forward (DF) trusted relays that help to prevent passive/active eavesdropper attacks. Specifically, the source node communicates directly with the destination node and indirectly through relaying vehicles $R_i \mid i = 1, 2, \ldots, M$, which serve as a best selected relaying terminal. All terminals are assumed to be equipped with a single transmit-and-receive antenna and operate in half-duplex mode.

Such cooperative system consists of two phases [13, 15, 16] as illustrated in Figure 2. In the broadcasting phase (phase 1), the source transmits its precoded signal to all relaying vehicles and to a destination node in the presence of an active/passive eavesdropper. In the relaying phase (phase 2), the best-selected relay is engaged in forwarding the received signal only if it was decoded correctly; otherwise, the relay remains silent. The relay decodes and then forwards a fresh decoded copy of the precoded signal to the destination. The destination makes its decision based on the two received signals over the broadcasting and relaying phases. The distances between nodes are arbitrary and identical. Additionally, the signal experiences independent relay fading. As a result, the composite channel becomes independent and identically distributed (i.i.d).

Figure 3 illustrates that, in the presence of an active/passive eavesdropper, the system model consists of two channels: the main channel from source to destination and the wire-tap channel between source and an eavesdropper. The source node transmits a signal ($S(n)$) to destination and to vehicle relays during the broadcast phase in the presence of an eavesdropper.

The time-sampled OFDM signal $s(n)$ is converted into the frequency domain by implementing a Discrete Fourier Transform (DFT) [13, 15, 16]. DFT renders a discrete finite sequence of complex coefficients, which are given by

$$S(n) = \sum_{q=0}^{Q} s(n)\, e^{-jw_q}, \tag{1}$$

where $w_q = 2\pi(q - Q/2)/N_t$ is the finite Fourier basis that captures the time variation.

From (1), the Basis Expansion Model (BEM) can be used to represent a discrete-time base-band equivalent channel for the vehicular doubly selective channel under consideration and is given by

$$h_B(\iota; l) = \sum_{q=0}^{Q} h_q(n; l)\, e^{j2w_q t}, \quad \iota \in [0, L], \tag{2}$$

where $h_q(n; l)$ is zero-mean complex Gaussian.

$\iota$, denotes the serial index for the input data symbols. The block index is given by $[n = \iota/N_t]$.

The block diagram of the proposed cooperative scheme is shown in Figure 4. The input data blocks (generated from an M-QAM constellation) of length $N_t$ are divided into shorter subblocks of length $N_s \mid (N_s \leq N_t)$. Let each of these subblocks be denoted by $s(n)$ which are the input to a linear prerecord $\ominus$ of size $N_s \times N_t$.

We assumed that eavesdropper used the same cooperative schemes shown in Figure 4(d), with the same precoder length and the same number of resolvable multipath components [15, 16].

The aggregate channel model of this paper takes into account both small-scale fading and path loss [15]. Path loss is proportional to $d^a$, where $a$ is the path loss coefficient and $d$ is the propagation distance. The path loss, associated with the distance $d_{srd}$ from the source node to the destination node, is modeled as

$$\Omega(d) = 10^{\beta_{sd}}, \tag{3}$$

where

(i) $\beta_{sd} = 128.1 - 36.7 \times \log_{10}(d_{srd})/10$,

(ii) $d_{sd}$ denotes the distance from source to destination,

(iii) $d_{(sr_i)}$ and $d_{(r_i d)}$ are the distances from source to relays ($R_i$) and from relays ($R_i$) to destination, respectively.

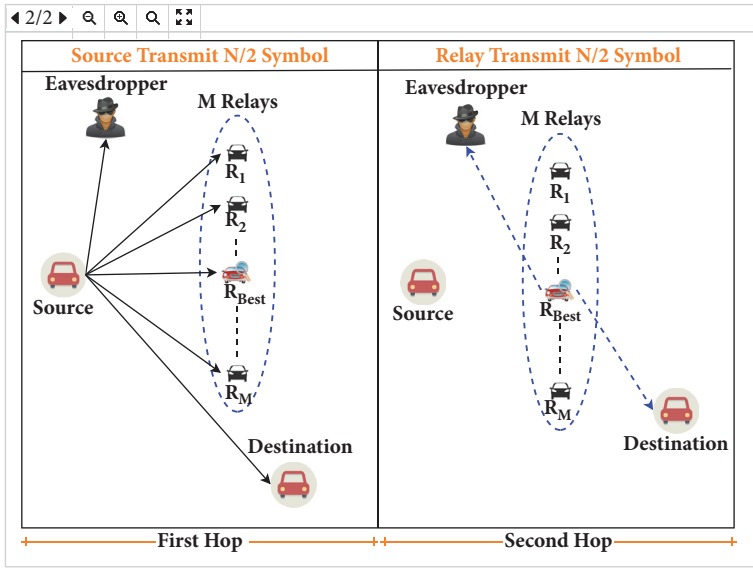



Figure 2: Half-duplex dual-hop VANET cooperative communication scenario.

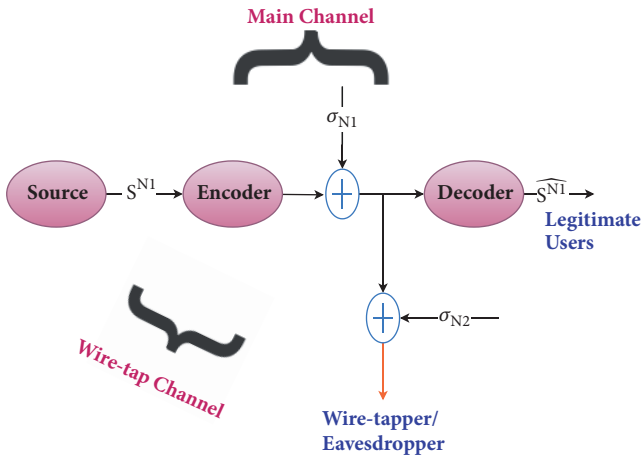



Figure 3: The block diagram of the Gaussian wire-tap channel (including the channel from source to destination in the presence of active/passive eavesdropper).

The relative geometrical gains are defined as

(i) $G_{(sr_i)} = (d_{sd}/d_{sr_i})^a$. $G_{(r_id)} = (d_{sd}/d_{r_id})^a$.

*2.3. System Model Strategy Equations.* In this section, we introduce an equation derivation in case of direct transmission and dual-hop relays (broadcasting and relaying phases) transmission.

*2.3.1. Direct Transmission*

*(i) Received Signal at Destination*

$$y_{sd}^{\text{direct}}(n) = \sqrt{P_t} h_{sd}(n)\, s(n) + n_{sd}(n), \quad (4)$$

where

(i) $y_{sd}^{\text{direct}}(n)$ is direct transmission between source and destination nodes,

(ii) $s(n)$ is transmitted signal from source node where, $E(|s(n)|^2) = 1$,

(iii) $P_t$ is transmitted power,

(iv) $n_{sd}(n)$ is the Additive White Gaussian Noise (AWGN) from source to destination with zero mean and variance $N_0/2 = \sigma_n^2$,

(v) $h_{sd}(n)$ are fading coefficients of the channel from source to destination and are modeled as Rayleigh fading, which corresponds to an ideal OFDM sub-channel,

(vi) $\sigma_{sd}^2 = E(|h_{sd}|^2)$ is the variance of main channel fading coefficients.

*(ii) Received Signal at Eavesdropper.* Due to the broadcast nature of the wireless cooperative system model, the eavesdropper attempts to overhear the transmitted signal.

$$y_{se}^{\text{direct}}(n) = \sqrt{P_t} h_{se}(n)\, s(n) + n_{se}(n), \quad (5)$$

where

(i) $y_{se}^{\text{direct}}(n)$ is direct transmission between source and eavesdropper nodes,

(ii) $n_{se}(n)$ is AWGN from source to eavesdropper with zero mean and variance $N_0/2 = \sigma_n^2$,

(iii) $h_{se}(n)$ are fading coefficients of the channel from source to eavesdropper; they are modeled as Rayleigh fading, which corresponds to an ideal OFDM sub-channel,

(iv) $\sigma_{se}^2 = E(|h_{se}|^2)$ is the variance of wire-tap channel fading coefficients.

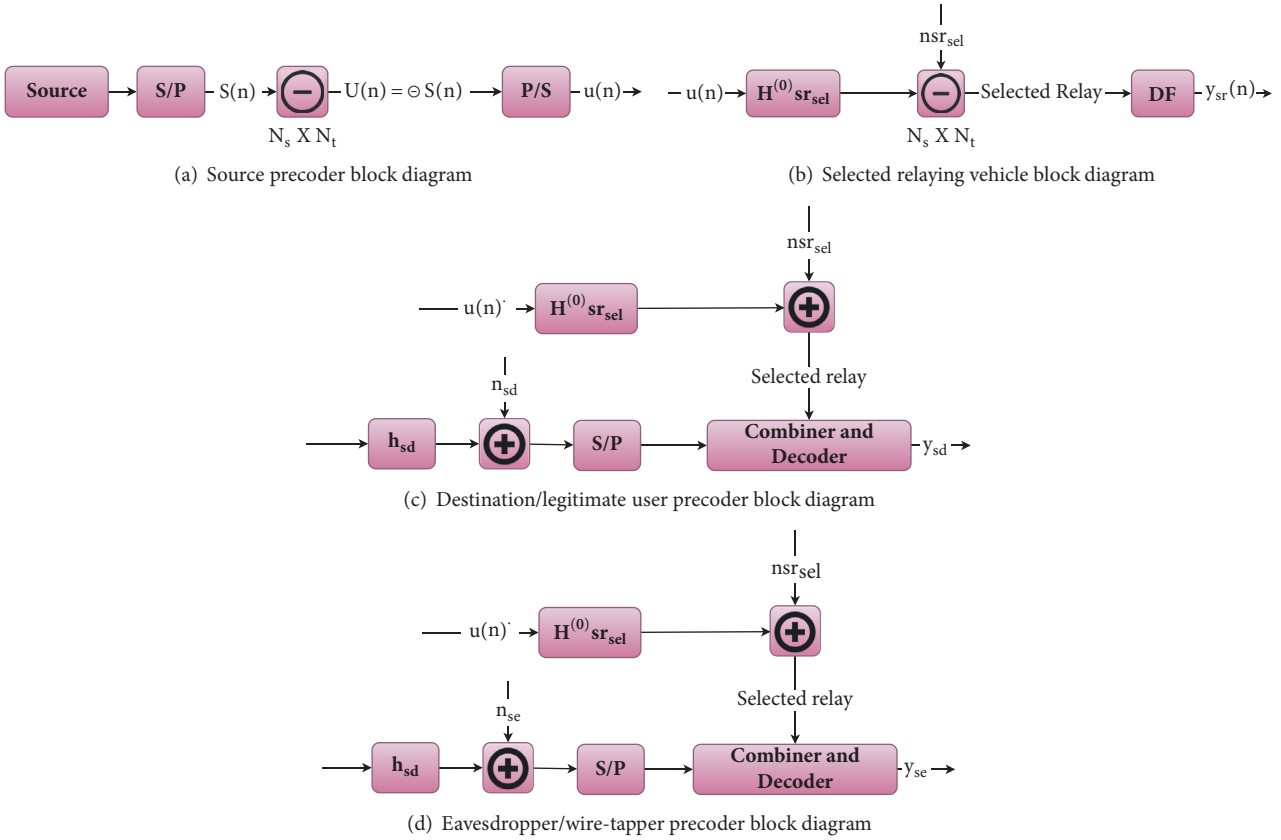



Figure 4: Precoder block diagram of the proposed DF cooperative scheme for an eavesdropper wire-tapper.

*2.3.2. Dual-Hop DF Relays Transmission*

*During Broadcast Phase*

*(i) Received Signal at Destination*

$$y_{sd}^{\mathrm{DF}}(n) = \sqrt{\frac{P_t}{2}} h_{sd}(n)\, s(n) + n_{sd}(n). \tag{6}$$

*(ii) Received Signal at Relays*

$$y_{sr}^{\mathrm{DF}}(n) = \sqrt{\frac{P_t G_{sr}}{2}} h_{sr}(n)\, s(n) + n_{sr}(n), \tag{7}$$

where

(i) $h_{sr}$ are fading coefficients of the channel from source to relays,

(ii) $n_{sr}$ is AWGN from source to relays with zero mean and variance $N_0/2 = \sigma_n^2$.

*(iii) Received Signal at Eavesdropper*. Meanwhile, due to the broadcast nature of wireless transmission, the eavesdropper also receives a copy of the source signal $s(n)$ and the corresponding received signal is written as

$$y_{se}^{\mathrm{DF}}(n) = \sqrt{\frac{P_t}{2}} h_{se}(n)\, s(n) + n_{se}(n), \tag{8}$$

where

(i) $h_{se}$ are fading coefficients of the channel from source to eavesdropper,

(ii) $|h_{sd}|^2$ and $|h_{se}|^2$ are independent and exponentially distributed with variances $\sigma_{sd}^2$ and $\sigma_{se}^2$, respectively.

*During Relaying Phase*. Without loss of generality, consider that $R_i$ is selected as the optimal relay to reencode and forward its decoded signal to the destination. In DF relaying protocol, relays first decode their received signal from the source and then they transmit the decoded outcome version to the destination node. Considering equal power allocation, to make a fair comparison with the direct transmission, we obtain the transmitted power at the source and relay nodes as $Pt/2$.

Therefore, the received signal at destination via $R_i$ is given by

$$y_{rd}^{DF}(n) = \sqrt{\frac{P_t G_{rd}}{2}} h_{rd}(n)\, s(n) + n_{rd}(n). \tag{9}$$

Similarly, considering that $R_i$ is selected as the optimal relay, the eavesdropper is able to overhear this optimal selected relay. An eavesdropper is located randomly around the source and relay nodes ($R_i$). In our model, we consider the worst-case scenario, where the eavesdropper overhears

the transmissions of both the source and relay nodes and attempts to decode the transmitted signal.

$$y_{re}^{\mathrm{DF}}(n) = \sqrt{\frac{P_t}{2}} h_{re}(n)\, s(n) + n_{re}(n). \tag{10}$$

In the next section, we introduce the ergodic channel-secrecy capacity concept in the proposed vehicle cooperative system to evaluate the system security. Additionally, from the security evaluation, we deduct the optimal conditions to achieve the maximum secrecy capacity and the lowest intercept probability.

## 3. Security Assessment Analysis

Traditional security techniques fail to retain the overall system security. Currently, researchers focus on improving the security of the physical layers instead of the higher layers. Their work tries to provide perfect transmission security from source to the legal receivers of the physical layer [17].

The channel-secrecy capacity is the difference between main and wire-tap channels as described in the following equation: $C_s = C_m - C_{mw}$ on the condition that $C_m > C_{mw} \rightarrow C_s > 0$.

Furthermore, the Shannon coding theorem explains the conditions for an efficient secure data transmission. It proved that the legitimate receiver does not recover the transmitted data if the main channel capacity ($C_m$) is less than the effective transmission rate ($R$) (i.e., $C_m < R$). However, the eavesdropper is still able to intercept the transmitted data even when the secrecy capacity falls below zero ($P_{\text{intercept}} = P(C_s < 0)$).

*3.1. Ergodic Channel-Secrecy Capacity Derivation.* In this section, we derive a closed-form equation for ergodic channel-secrecy capacity with the existence of a direct link. We assume that the destination node receives two different signals during the two phases (i.e., broadcast and relay phases) on different orthogonal time slots. Therefore, the main channel consists of two different components: the first component is from source to destination (direct link) and the second component is from source to vehicle relays (cooperative link). Additionally, as we consider the worst-case scenario, the wire-tap channel consists of two-link component. The eavesdropper is able either to overhear data from the source directly during the broadcast phase or to overhear during the vehicle relays from the selected best relay.

*3.1.1. Direct Transmission.* The direct channel-secrecy capacity is the difference between the main and wire-tap links. Therefore, the channel-secrecy equation of the direct transmission is defined as

$$C_{sd}^{\mathrm{direct}} = C_m - C_{mw}. \tag{11}$$

Assuming that the optimal Gaussian codebook is used at the source, the maximal achievable rate (also known as channel capacity) of direct transmission from source to destination is obtained from (5) as follows:

$$C_{sd}^{\mathrm{direct}} = \log_2\left(1 + \frac{|h_{sd}|^2 P_t}{\sigma_n^2}\right). \tag{12}$$

Similarly, from (6), wire-tap capacity link from source to eavesdropper during direct transmission is given by

$$C_{se}^{\mathrm{direct}} = \log_2\left(1 + \frac{|h_{se}|^2 P_t}{\sigma_n^2}\right). \tag{13}$$

$h_{sd}$ and $h_{se}$ represent the fading coefficient of the channel from source to destination and from source to eavesdropper, respectively.

*3.1.2. Dual-Hop DF Relays Transmission.* The capacity of dual-hop DF relaying transmission is the minimum of both capacities from source to relays and that from relays to destination [2]. This means that the dual-hop DF transmission results in failure when either source-relays link or relays-destination link is in failure. Therefore, considering $R_i$ is the optimal relay, we can obtain the capacity of dual-hop DF transmission as

$$C_{srd}^{\mathrm{DF}} = \min\left(C_{sr}, C_{rd}\right), \tag{14}$$

where $C_{sr}$ and $C_{rd}$ are the channel capacities from source to $R_i$ and from $R_i$ to a destination, respectively. These capacities can be given by

$$C_{sr} = \log_2\left(1 + \frac{|h_{sr}|^2 P_t G_{sr}}{2\sigma_n^2}\right), \tag{15}$$

$$C_{rd} = \log_2\left(1 + \frac{|h_{rd}|^2 P_t G_{rd}}{2\sigma_n^2}\right). \tag{16}$$

Based on our proposed model, the destination node is capable of decoding the transmitted signal even when the relays are silent. Additionally, when at least one of the relaying vehicles succeeds in decoding the transmitted signal, the destination node will select the maximum capacity of both received signals. Specifically, using the selection diversity combining, the destination-secrecy capacity with help of the optimal relay selection scheme is the highest of $C_{sd}^{\mathrm{DF}}$ and $C_{srd}^{\mathrm{DF}}$ yielding to

$$\begin{aligned} C_m^{\mathrm{DF}} &= \max\left(C_{sd}^{\mathrm{DF}}, C_{srd}^{\mathrm{DF}}\right) \\ &= \log_2\left(1 + \frac{\max\left(|h_{sd}|^2, \min\left(|h_{sr}|^2, |h_{rd}|^2\right)\right) P_t}{2\sigma_n^2}\right). \end{aligned} \tag{17}$$

Similarly, due to the broadcast nature, the eavesdropper attempts to decode the transmitted signal either from the source node or from the best relay selected (if any). This means that even if the relays fail to decode the transmitted signal, the eavesdropper might still decode the transmitted signal from the source node.

Moreover, if at least one relay succeeds in decoding the transmitted signal, eavesdropper overhears the transmissions of both source and selected vehicle relay. Specifically, using the selection diversity combining, the eavesdropper-secrecy capacity with optimal relay selection scheme is the highest one of $C_{se}^{\mathrm{DF}}$ and $C_{sre}^{\mathrm{DF}}$, yielding to

$$C_{mw}^{\mathrm{DF}} = \max\left(C_{se}^{\mathrm{DF}}, C_{sre}^{\mathrm{DF}}\right), \tag{18}$$

where $C_{se}^{\mathrm{DF}}$ and the $C_{sre}^{\mathrm{DF}}$ are the secrecy capacity from the source to an eavesdropper directly and from source to eavesdropper via $R_i$, respectively.

The secrecy capacity $C_{sre}^{\mathrm{DF}}$ is the minimum of both capacities from source to relays and from relays to eavesdropper [2]. Therefore, considering that $R_i$ is the optimal relay, we can obtain the capacity of dual-hop DF transmission as follows:

$$C_{sre}^{\mathrm{DF}} = \min\left(C_{sr}, C_{re}\right), \tag{19}$$

where $C_{re}$ is the channel capacity from $R_i$ to eavesdropper. It can be given by

$$C_{re} = \log_2\left(1 + \frac{\left|h_{re}\right|^2 P_i G_{re}}{2\sigma_n^2}\right). \tag{20}$$

Therefore, the wire-tap channel-secrecy capacity can be obtained as

$$C_{mw}^{\mathrm{DF}} = \log_2\left(1 + \frac{\max\left(\left|h_{se}\right|^2, \min\left(\left|h_{sr}\right|^2, \left|h_{re}\right|^2\right)\right) P_t}{2\sigma_n^2}\right). \tag{21}$$

Combining (17) and (21), the secrecy capacity of dual-hop DF relaying transmission via $R_i$ is given by

$$C_r^{\mathrm{DF}} = \log_2\left(1 + \frac{\max\left(\left|h_{sd}\right|^2, \min\left(\left|h_{sr}\right|^2, \left|h_{rd}\right|^2\right)\right) P_t}{2\sigma_n^2}\right) - \log_2\left(1 + \frac{\max\left(\left|h_{se}\right|^2, \min\left(\left|h_{sr}\right|^2, \left|h_{re}\right|^2\right)\right) P_t}{2\sigma_n^2}\right). \tag{22}$$

*3.1.3. Relay Selection Technique.* This section presents a defined relay selection equation that may be applied to enhance the physical layer security of vehicle relay communication in presence of an active/passive eavesdropper node with the existence of a direct link. Several best relay selection techniques are used to effectively overcome the eavesdropper attacks and maintain the whole system physical layer security.

As mentioned in Figure 2, in Phase 1, the source transmits its precoded signal to the $M$ relay vehicles and to the destination. In Phase 2, relays are engaged in forwarding the received signal only if it was decoded correctly; otherwise, relays remain silent. These relay nodes, which succeed in perfectly decoding the source signal, forward a fresh decoded copy of the precoded signal to the destination. After that, destination makes its decision based on the two received signals over the broadcasting and relaying phases.

Successive decoding relays are represented by the successful decoding set $\Delta$. Given $M$ relay nodes, there are $2^M$ possible *Source − Relays* pairs.

Therefore, the resultant successful decoding set $\Delta$ is given by the following equation:

$$\Delta = \left\{\phi, \Delta_1, \Delta_2, \ldots, \Delta_n, \ldots, \Delta_{2^M-1}\right\}, \tag{23}$$

where $\phi$ is the empty set, meaning that no relay node succeeds in perfectly decoding the transmitting signal $s(n)$, while $\Delta_n$ is a nonempty set of $M$ relays node, meaning that a specific relay will be selected to forward its decoded signal to the destination node.

Specifically, the selection techniques are based on the channel state information (CSI) to perform single best relay selection mechanism accurately. In case the CSI of wire-tap link is available, the proposed relay selection will be considered; then, by minimizing $C_{mw}^{\mathrm{DF}}$, the channel secrecy will be maximized ($C_s$) [6].

In contrast, traditional relay selection will be used to maximize $C_m$, when only the CSI of the main link is known [18].

*3.1.4. Proposed Relay Selection Mechanism.* In this section, we consider the relay that maximizes the channel-secrecy capacity of the dual-hob DF relaying transmission as the optimal relay. The optimal relay selection requires the global CSI for both main and wire-tap links. Therefore, the proposed relay of DF relaying based on optimal relay selection can be obtained from (22) as follows:

$$\begin{aligned} \textit{optimal relay} &= \arg\max_{r\in R} C_r^{\mathrm{DF}} \\ &= \arg\max_{r\in R}\left(\frac{\max\left(\left|h_{sd}\right|^2, \chi_{srd}\right) P_t + 2\sigma_n^2}{\max\left(\left|h_{se}\right|^2, \chi_{sre}\right) P_t + 2\sigma_n^2}\right), \end{aligned} \tag{24}$$

where $\chi_{srd} = \min(|h_{sr}|^2, |h_{rd}|^2)$ and $\chi_{sre} = \min(|h_{sr}|^2, |h_{re}|^2)$.

*3.1.5. Traditional Relay Selection Mechanism.* In this section, we consider the relay that maximizes the capacity of DF relaying transmission as the traditional relay. The traditional relay selection requires only the CSI of the main link without considering that of wire-tap link. Therefore, the traditional relay of DF relaying based on optimal relay selection can be obtained from (17) as follows:

$$\begin{aligned} \textit{optimal relay} &= \arg\max_{r\in R} C_m^{\mathrm{DF}} \\ &= \arg\max_{r\in R} \max\left(\left|h_{sd}\right|^2, \min\left(\left|h_{sr}\right|^2, \left|h_{rd}\right|^2\right)\right). \end{aligned} \tag{25}$$

Additionally, the ergodic channel-secrecy capacity can be obtained by averaging the instantaneous secrecy capacity $C_r^{\mathrm{DF}^+}$ over the fading channels coefficient [19], where

$$C_r^{\mathrm{DF}^+} = \mathrm{mean}\left(\max\left(C_r^{\mathrm{DF}}, 0\right)\right). \tag{26}$$

*3.2. Intercept Probability Derivation.* In this section, we extract a closed form for the intercept probability based on the calculated channel-secrecy capacity equations. Wyner mentioned that [8] when the channel secrecy falls below zero ($C_m < C_{me} \rightarrow C_s < 0$), the eavesdropper will succeed in attacking the transmitted data and receive a copy of the transmitted signal.

*3.2.1. Direct Transmission.* In this section, we analyze the intercept probability of the direct link transmission as a benchmark for comparison purpose. Therefore, based on (11), the intercept probability equation can be written as follows:

$$\begin{aligned} P_{\mathrm{intercept}}^{\mathrm{direct}} &= P_r\left(C_{sd}^{\mathrm{direct}} < C_{se}^{\mathrm{direct}}\right) = P_r\left(|h_{sd}|^2 < |h_{se}|^2\right) \\ &= \frac{\sigma_{se}^2}{\sigma_{sd}^2 + \sigma_{se}^2}. \end{aligned} \tag{27}$$

Notice that the following random variables $|h_{sd}|^2$ and $|h_{se}|^2$ follow exponential distribution with means $\sigma_{sd}^2 = E(|h_{sd}|^2)$ and $\sigma_{se}^2 = E(|h_{se}|^2)$, respectively. For simplicity, we assumed that the main link $|h_{sd}|^2$ and wire-tap link $|h_{se}|^2$ are independent and identically distributed (i.i.d.) random variables.

In this paper, we denote the ratio of the channel gain of the main link to that of the wire-tap link by $\lambda_{me} = \sigma_{sd}^2/\sigma_{se}^2$. Throughout this paper, we refer to $\lambda_{me}$ as the main-to-eavesdropper ratio (MER). Thereof, we can simplify (27) as follows:

$$P_{\mathrm{intercept}}^{\mathrm{direct}} = \frac{1}{1 + \lambda_{me}}. \tag{28}$$

Equation (28) shows that the intercept probability is independent of the transmitted power $P_t$; then the security level cannot improve by adjusting the power. This motivates the employment of optimal relay selection scheme for the security improvements in the cooperative vehicle systems.

*3.2.2. Dual-Hop DF Relays Transmission*

*(i) Proposed Relay Selection Mechanism.* This section drives a closed form for the intercept probability expression for the proposed relay selection. Based on the definition of the intercept event occurrence, the intercept probability of the proposed relay selection is obtained from Eq. (24) as

$$\begin{aligned} P_{\mathrm{intercept}}^{\mathrm{DF}} &= P_r\left(\max_{r\in R} C_r^{\mathrm{DF}} < 0\right) \\ &= \prod_{r=1}^{M} P_r\left\{\max\left(|h_{sd}|^2, \min\left(|h_{sr}|^2, |h_{rd}|^2\right)\right)\right. \\ &\quad \left. < \max\left(|h_{se}|^2, \min\left(|h_{sr}|^2, |h_{re}|^2\right)\right)\right\}. \end{aligned} \tag{29}$$

Denote

(i) $X = \min(|h_{sr}|^2, |h_{rd}|^2)$,
(ii) $Y = \min(|h_{sr}|^2, |h_{re}|^2)$,
(iii) $Z = \max(|h_{sd}|^2, X)$,
(iv) $W = \max(|h_{se}|^2, Y)$.

We can easily obtain the Cumulative Distribution Function (CDF) of $X$, $Y$, $Z$, and $W$, respectively, as

$$P_X(X < x) = 1 - e^{-((x/\sigma_{sr}^2)+(x/\sigma_{rd}^2))}, \tag{30a}$$

$$P_Y(Y < x) = 1 - e^{-((x/\sigma_{sr}^2)+(x/\sigma_{re}^2))}, \tag{30b}$$

$$\begin{aligned} P_Z(Z < x) &= P\left(|h_{sd}|^2 < x\right) P(X < x) \\ &= \left(1 - e^{-(x/\sigma_{sd}^2)}\right)\left(1 - e^{-((x/\sigma_{sr}^2)+(x/\sigma_{rd}^2))}\right), \end{aligned} \tag{30c}$$

$$\begin{aligned} P_W(W < x) &= P\left(|h_{se}|^2 < x\right) P(Y < x) \\ &= \left(1 - e^{-(x/\sigma_{sd}^2)}\right)\left(1 - e^{-((x/\sigma_{sr}^2)+(x/\sigma_{rd}^2))}\right), \end{aligned} \tag{30d}$$

where $x \geq 0$. Starting from (29), we can get (31) as follows:

$$\begin{aligned} P_{\mathrm{intercept}}^{\mathrm{DF}} &= \prod_{r=1}^{M} P_r\left\{\max\left(|h_{sd}|^2, \min\left(|h_{sr}|^2, |h_{rd}|^2\right)\right) < \max\left(|h_{se}|^2, \min\left(|h_{sr}|^2, |h_{re}|^2\right)\right)\right\} \\ &= \int_0^{\infty} \frac{1}{\sigma_{re}^2}\left[\left(1 - e^{-(x/\sigma_{sd}^2)}\right)\left(1 - e^{-((x/\sigma_{sr}^2)+(x/\sigma_{rd}^2))}\right)\right]\left[\left(1 - e^{-(x/\sigma_{se}^2)}\right)\left(1 - e^{-((x/\sigma_{sr}^2)+(x/\sigma_{re}^2))}\right)\right] dx, \\ P_{\mathrm{intercept}}^{\mathrm{DF}} &= \prod_{r=1}^{M}\left(\frac{\sigma_{sd}^2\sigma_{rd}^2\sigma_{se}^2\sigma_{re}^2 + \sigma_{sd}^2\sigma_{sr}^2\sigma_{se}^2\sigma_{re}^2 + \sigma_{sd}^2\sigma_{sr}^2\sigma_{rd}^2\sigma_{se}^2 + \sigma_{sd}^2\sigma_{sr}^2\sigma_{rd}^2\sigma_{re}^2}{\sigma_{sr}^2\sigma_{rd}^2\sigma_{se}^2\sigma_{re}^2 + \sigma_{sd}^2\sigma_{rd}^2\sigma_{se}^2\sigma_{re}^2 + \sigma_{sd}^2\sigma_{sr}^2\sigma_{se}^2\sigma_{re}^2 + \sigma_{sd}^2\sigma_{sr}^2\sigma_{rd}^2\sigma_{se}^2 + \sigma_{sd}^2\sigma_{sr}^2\sigma_{rd}^2\sigma_{re}^2}\right). \end{aligned} \tag{31}$$

*(ii) Traditional Relay Selection Mechanism.* This section drives a closed form for the intercept probability expression for the traditional relay selection in the Rayleigh fading channel. Based on the definition of the intercept event occurrence,

the intercept probability of the proposed relay selection is obtained from (25) as follows:

$$P_{\text{intercept}}^{\text{DF}} = P_r\left(\max_{r\in R} C_m^{\text{DF}} < C_{oe}^{\text{DF}}\right), \tag{32}$$

where $C_{oe}^{\text{DF}}$ is the channel-secrecy capacity from the optimal relay to an eavesdropper. Using the law of total probability and the intercept probability of traditional relay selection, the optimal relay selection scheme is obtained as follows:

$$\begin{aligned} &P_{\text{intercept}}^{\text{DF}} \\ &= \sum_{i=1}^{M} \frac{1}{M} P_r\left(\max_{r\in R}\left(\max\left(\left|h_{sd}\right|^2, \min\left(\left|h_{sr}\right|^2, \left|h_{rd}\right|^2\right)\right)\right)\right. \\ &\left. < \left|h_{ie}\right|^2\right). \end{aligned} \tag{33}$$

Using (33) and letting $|h_{ie}|^2 = \tau$, we can obtain the traditional intercept probability as in (34). Based on binomial expansion, $A_k$ represents the $k-th$ nonempty subcollection of $M$ relays, and $|A_k|$ is the element's number in set $A_k$.

$$\begin{aligned} P_{\text{intercept}}^{\text{DF}} &= \sum_{i=1}^{M} \int_0^{\infty} \prod_{r=1}^{M}\left[1 - e^{-((\tau/\sigma_{sr}^2)+(\tau/\sigma_{rd}^2))}\right] \\ &\cdot \left[1 - e^{-(\tau/\sigma_{sd}^2)}\right]\left[\frac{1}{\sigma_{ie}^2} e^{-\tau/\sigma_{ie}^2}\right] d\tau. \\ &= \sum_{i=1}^{M} \frac{1}{M} \int_0^{\infty} \left(1 + \sum_{k=1}^{2^M-1} (-1)^{|A_k|} \exp\left(\frac{\tau}{\sigma_{sd}^2}\right)^{|A_k|}\right. \\ &\left. \cdot \exp\left[-\sum_{r\in A_K} \frac{\tau}{\sigma_{sd}^2} + \frac{\tau}{\sigma_{sr}^2} + \frac{\tau}{\sigma_{rd}^2}\right]\right) \\ &\cdot \frac{1}{\sigma_{ie}^2} \exp\left(-\frac{\tau}{\sigma_{ie}^2}\right) d\tau \\ &= \sum_{i=1}^{M} \left(1 + \sum_{k=1}^{2^M-1} (-1)^{|A_k|}\right. \\ &\left. \cdot \left[1 + \frac{1}{\sigma_{sd}^2} \sum_{r\in A_k} \left(\frac{\sigma_{ie}^2}{\sigma_{sd}^2} + \frac{\sigma_{ie}^2}{\sigma_{sr}^2} + \frac{\sigma_{ie}^2}{\sigma_{rd}^2}\right)^{-1}\right]\right) \end{aligned} \tag{34}$$

*3.3. Diversity Order Analysis.* In this section, we derive the diversity order performance of the direct transmission and the dual-hop DF relaying transmission based on proposed and traditional selection schemes.

The traditional diversity gain order is based onSNR, where SNR is the Signal to Noise Ratio [20], which is given by

$$d = -\lim_{\text{SNR}\to\infty} \frac{\log P_e\,(\text{SNR})}{\log \text{SNR}}, \tag{35}$$

where $P_e$(SNR) is the bit error rate. It is observed from the intercept probability equations that the traditional diversity is not applicable here. Therefore, the generalized diversity gain is given by

$$d_{\text{generalized}} = -\lim_{\lambda_{me}\to\infty} \frac{\log\left(P_{\text{intercept}}\right)}{\log\left(\lambda_{me}\right)}. \tag{36}$$

*3.3.1. Direct Transmission.* In this section, we analyze the benchmark diversity order gain of the direct transmission. By substituting (28) for (36), the diversity order gain is obtained as follows:

$$d_{\text{direct}} = -\lim_{\lambda_{me}\to\infty} \frac{\log\left(1/\left(1+\lambda_{me}\right)\right)}{\log\left(\lambda_{me}\right)} = 1, \tag{37}$$

meaning that the direct transmission achieves a single diversity order.

*3.3.2. Dual-Hop DF Relays Transmission*

*(i) Proposed Relay Selection Mechanism.* This section presents the diversity order gain analysis of the optimal relay selection. Substituting (31) for (36) gives the diversity order gain as follows:

$$d_{\text{Proposed}}^{\text{DF}} = -\lim_{\lambda_{me}\to\infty} \frac{\log\left(P_{\text{DF}}^{\text{intercept}}\right)}{\log\left(\lambda_{me}\right)}. \tag{38}$$

For simplicity, we denote $\sigma_{sr}^2 = \alpha_{sr}\sigma_{sd}^2$, $\sigma_{rd}^2 = \alpha_{rd}\sigma_{sd}^2$, and $\sigma_{re}^2 = \alpha_{se}\sigma_{se}^2$, where $\alpha_{sr}$, $\alpha_{rd}$, and $\alpha_{re}$ are constants. The intercept probability can be rewritten as

$$P_{\text{intercept}}^{\text{DF}} = \frac{\alpha_{re}\alpha_{sr}^{-1} + \alpha_{re}\alpha_{rd}^{-1} + \left(1+\alpha_{re}\right)\lambda_{me}}{\alpha_{re} + \alpha_{re}\alpha_{sr}^{-1} + \alpha_{re}\alpha_{rd}^{-1} + \left(1+\alpha_{re}\right)\lambda_{me}}. \tag{39}$$

By substituting (39) for (38), the diversity order will be

$$d_{\text{Proposed}}^{\text{DF}} = M. \tag{40}$$

Equations show that the proposed relay selection transmission achieves the diversity order by $M$.

*(ii) Traditional Relay Selection Mechanism.* This section presents the diversity order gain analysis of the traditional relay selection. Substituting (34) for (36) gives the diversity order gain as

$$d_{\text{Traditional}}^{\text{DF}} = -\lim_{\lambda_{me}\to\infty} \frac{\log\left(P_{\text{DF}}^{\text{intercept}}\right)}{\log\left(\lambda_{me}\right)}. \tag{41}$$

For simplicity, we can obtain

$$\begin{aligned} &\left[1 - \exp - \left(\frac{\tau}{\sigma_{sr}^2} + \frac{\tau}{\sigma_{rd}^2}\right)\right]\left[1 - \exp - \left(\frac{\tau}{\sigma_{sd}^2}\right)\right] \\ &= \left[\frac{\tau}{\sigma_{sr}^2} + \frac{\tau}{\sigma_{rd}^2} + \frac{\tau}{\sigma_{sd}^2}\right] \quad \text{for } \lambda \longrightarrow \infty. \end{aligned} \tag{42}$$

Using Taylor series expansion and ignoring the higher-order terms, the intercept probability can be rewritten as follows:

$$P_{\mathrm{DF}}^{\mathrm{intercept}} = \sum_{i=1}^{M} (M-1)! \prod_{r=1}^{M} \left( \frac{\gamma_{ie}}{\gamma_{sr}} + \frac{\gamma_{ie}}{\gamma_{rd}} + \frac{\gamma_{ie}}{\gamma_{sd}} \right) \times \left( \frac{1}{\lambda_{me}} \right)^{M}, \tag{43}$$

where $\gamma_{sr} = \sigma_{sr}^2/\sigma_{sd}^2$, $\gamma_{rd} = \sigma_{rd}^2/\sigma_{sd}^2$, and $\gamma_{ie} = \sigma_{ie}^2/\sigma_{sd}^2$. Substituting (43) for (41) gives

$$d_{\mathrm{Traditional}}^{\mathrm{DF}} = M, \tag{44}$$

meaning that the traditional relay selection transmission achieves the diversity order also by $M$. From (37), (40), and (44), it is obvious that the dual-hop DF optimal relay selection achieves the same diversity order gain $M$. This means that, at high MER, for $M > 1$, the intercept probabilities of DF relay selection schemes are reduced faster than the direct transmission. This implies that the physical layer improves by using the dual-hop DF optimal relay selection.

*3.4. Outage Probability Derivation.* In this section, we present the outage probability analysis for our proposed system model. Based on Shannon capacity [21] and Wyner's results [8, 9], eavesdropper fails to decode the transmitted signal when the wire-tap channel is lower than the data rate ($R_d$). Whenever the wire-tap channel overcomes $R_d$, eavesdropper may succeed in decoding the transmitting signal; then the intercept probability occurs.

One of the basic solutions for security level improvement is to increase the data rate ($R_d$). In contrast, as $R_d$ increases, this comes at the cost of transmission reliability degradation, which leads to the decrease of the vehicular cooperative systems throughput.

*3.4.1. Reliability Derivation Of Direct Transmission.* The outage probability of the main link ($S - D$) increases when $R_d$ increases. Therefore, based on Shannon capacity [21], the outage probability $P_{\mathrm{out}}$ of a direct transmission is obtained as follows:

$$P_{\mathrm{out}} = P_r\left(C_{sd} < R_d\right) = P_r\left(|h_{sd}|^2 < R_d\right) = 1 - \exp\left(-\frac{\delta}{\sigma_{sd}^2}\right), \tag{45}$$

where $\delta = (2^{R_d} - 1)/\gamma$ and $\gamma = P_t/\sigma_n^2$.

*3.4.2. Reliability Derivation Of Dual-Hop DF Relays.* Figure 1 shows that the destination node is capable of decoding the transmitted signal even when the relay decoding set is empty ($\Delta = \phi$).

Additionally, when at least one of the vehicle relays succeeds in decoding the transmitted signal ($\Delta = \Delta_n$), the destination node will select the maximum capacity of both received signals (from source and $R_{\mathrm{best}}$).

Using the law of total probability [22], the outage probability of the main link is formulated as follows:

$$P_{\mathrm{out}}^{\mathrm{DF}} = P_r\left(\Delta = \phi\right) P_r\left(C_{sd}^{\mathrm{DF}} < R_d\right) + \sum_{n=1}^{2^M-1} \left[ P_r\left(\Delta = \Delta_n\right) P_r\left(C_m^{\mathrm{DF}} < R_d\right) \right]. \tag{46}$$

The $|h_{sr}|^2$ and $|h_{rd}|^2$ factors of different vehicle relay nodes are independent and follow exponential distribution with a mean of $\sigma_{sr}^2$ and $\sigma_{rd}^2$.

The probability of occurrence for the event ($\Delta = \phi$) is obtained from (14):

$$\begin{aligned} P_r\left(\Delta = \phi\right) &= \prod_{r=1}^{M} P_r\left[ \log_2\left( 1 + \frac{\min\left(|h_{sr}|^2, |h_{rd}|^2\right) P_t}{2\sigma_n^2} \right) < R_d \right] \\ &= \prod_{r=1}^{M} \left[ P_r\left(|h_{sr}|^2 < \Gamma\right) P_r\left(|h_{rd}|^2 < \Gamma\right) \right] \\ &= \prod_{r=1}^{M} \left[ 1 - \exp\left(-\frac{\Gamma}{\sigma_{rd}^2}\right) - \exp\left(-\frac{\Gamma}{\sigma_{sr}^2}\right) + \exp\left(-\left(\frac{\Gamma}{\sigma_{sr}^2} + \frac{\Gamma}{\sigma_{rd}^2}\right)\right)\right], \end{aligned} \tag{47}$$

where $M$ is the number of vehicle relay nodes and $\Gamma = (2^{2R_d} - 1)/\gamma$. For simplicity, we considered i.i.d. as randomly generated variables. The fading coefficients of all main links (i.e., $|h_{sd}|^2$, $|h_{sr}|^2$, and $|h_{rd}|^2$) are independent and have identical channel gain $\sigma_m^2$.

Therefore, the above equation can be simplified as follows:

$$P_r\left(\Delta = \phi\right) = \left[ 1 - 2\exp\left(-\frac{\Gamma}{\sigma_m^2}\right) + \exp\left(-\frac{2\Gamma}{\sigma_m^2}\right)\right]^M. \tag{48}$$

From (12), with $P_t = P_t/2$, we can obtain $P_r(C_{sd}^{\mathrm{DF}} < R_d)$ as follows:

$$P_r\left(C_{sd}^{\mathrm{DF}} < R_d\right) = P_r\left[|h_{sd}|^2 < \Gamma\right] = 1 - \exp\left(\frac{\Gamma}{\sigma_m^2}\right). \tag{49}$$

The probability of occurrence for event ($\Delta = \Delta_n$) can be obtained as follows:

$$P_r\left(\Delta = \Delta_n\right) = \begin{cases} P_r\left(C_{sr_id}^{\mathrm{DF}} > R_d\right), & R_i \in \Delta_n \\ P_r\left(C_{sr_jd}^{\mathrm{DF}} < R_d\right), & R_j \in \overline{\Delta_n}, \end{cases} \tag{50}$$

where $\overline{\Delta_n} = (R - \Delta_n)$ is the complement of $\Delta_n$, given that $\Delta$ is not empty, and a vehicle relay $R_i$ is selected to forward a fresh

decoded copy of the transmitted signal $\hat{s}$ to destination node. When the received signal at destination node is ($\hat{s} = s$), this means that the relays perfectly decode the transmitted signal.

The probability of occurrence for event $\Delta = \Delta_n$ can be obtained from (50) as follows:

$$\begin{aligned} P_r(\Delta = \Delta_n) &= \prod_{R_i \in \Delta_n} P_r\left(\left(\left|h_{sr_i}\right|^2 > \Gamma\right)\right)\left(P_r\left(\left|h_{r_i d}\right|^2 > \Gamma\right)\right) \\ &\quad \times \prod_{R_j \in \overline{\Delta_n}} P_r\left(\left(\left|h_{sr_j}\right|^2 > \Gamma\right)\right)\left(P_r\left(\left|h_{r_j d}\right|^2 > \Gamma\right)\right) \\ &= \prod_{R_i \in \Delta_n}\left[\exp\left(-\frac{\Gamma}{\sigma^2_{sr_i}}\right)\exp\left(-\frac{\Gamma}{\sigma^2_{r_i d}}\right)\right] \\ &\quad \times \prod_{R_j \in \overline{\Delta_n}}\left[1 - \exp\left(-\frac{\Gamma}{\sigma^2_{sr_j}}\right)\exp\left(-\frac{\Gamma}{\sigma^2_{r_i d}}\right)\right]. \end{aligned} \tag{51}$$

Considering $\sigma^2_{sr} = \sigma^2_{rd} = \sigma^2_{sd} = \sigma^2_m$, we can simplify (51) as follows:

$$\begin{aligned} P_r(\Delta = \Delta_n) &= \left[\exp\left(-\frac{2\Gamma\left|\Delta_n\right|}{\sigma^2_m}\right)\right] \\ &\quad \cdot \left[1 - 2\exp - \frac{\Gamma}{\sigma^2_m} + \exp - \frac{2\Gamma}{\sigma^2_m}\right]^{\left|\overline{\Delta_n}\right|}. \end{aligned} \tag{52}$$

Finally, based on (17), we can obtain $P_r(C^{\mathrm{DF}}_m < R_d)$ as follows:

$$\begin{aligned} P_r\left(C^{\mathrm{DF}}_m < R_d\right) &= P_r\left(\max\left(C_{sd}, C_{srd}\right) < R_d\right) \\ &= P_r\left(\left|h_{sd}\right|^2 < \Gamma\right) P_r\left(\min_{r \in M}\left(C_{sr}, C_{rd}\right) < \Gamma\right) \\ &= \left(1 - \exp\left(-\frac{\Gamma}{\sigma_m}\right)^2\right) \\ &\quad \cdot \left(1 - 2\exp\left(-\frac{\Gamma}{\sigma^2_m} + \exp\left(-\frac{2\Gamma}{\sigma^2_m}\right)\right)\right)^{\left|\Delta_n\right|}. \end{aligned} \tag{53}$$

Therefore, upon substituting (48)–(53) for (46), we can formulate the closed-form outage probability expression of our proposed model in the following equation:

$$\begin{aligned} P^{\mathrm{DF}}_{\mathrm{out}} &= \left[1 - 2\exp - \left(\frac{\Gamma}{\sigma^2_m}\right) + \exp - \left(\frac{2\Gamma}{\sigma^2_m}\right)\right]^M \left[1 \right. \\ &\quad \left. - \exp - \left(\frac{\Gamma}{\sigma^2_m}\right)\right] + \sum_{n=1}^{2^M - 1}\left[\left[1 - 1\exp - \left(\frac{\Gamma}{\sigma^2_m}\right)\right]\right. \\ &\quad \left. \cdot \left[1 - 2\exp - \left(\frac{\Gamma}{\sigma^2_m}\right) + \exp - \left(\frac{2\Gamma}{\sigma^2_m}\right)\right]^{\left|\Delta_n\right|}\right. \\ &\quad \left. \cdot \left[\exp\left(-\frac{2\Gamma\left|\Delta_n\right|}{\sigma^2_m}\right)\right]\right. \\ &\quad \left. \cdot \left[1 - 2\exp - \left(\frac{\Gamma}{\sigma^2_m}\right) + \exp - \left(\frac{2\Gamma}{\sigma^2_m}\right)\right]^{\left|\Delta_n\right|}\right]. \end{aligned} \tag{54}$$

The simplified closed form of the outage probability expression can be obtained as follows:

$$\begin{aligned} P^{\mathrm{DF}}_{\mathrm{out}} &= \left[1 - \exp\left(-\frac{\Gamma}{\sigma^2_m}\right)\right] \\ &\quad \cdot \left[1 - 2\exp - \left(\frac{\Gamma}{\sigma^2_m}\right) + 2\exp - \left(\frac{2\Gamma}{\sigma^2_m}\right)\right]^M. \end{aligned} \tag{55}$$

From (55), it is obvious that the outage probability increases as the number of the vehicular relays increases.

## 4. Numerical Calculation Study

This section shows the numerical study of the channel-secrecy capacity of DF cooperative vehicle schemes. Simulation results show that channel-secrecy capacity of the proposed system model is higher than the traditional system (i.e., without existing direct link).

Moreover, simulation results showed that the channel secrecy of the proposed system model significantly increases when the number of the vehicle relays increases. Therefore, the simulation results show an improvement in the physical layer security when exploiting cooperative relays.

Additionally, the simulation showed the effect of increasing the relays gain ($G$), assuming that all relays are identical and independently distributed (i.i.d).

The following simulation parameters were considered for all tests:

(i) $G_{srd}$ (dB) = 0; $G_{sre}$ (dB) = 0. $\sigma^2_{sd} = 0.5$.

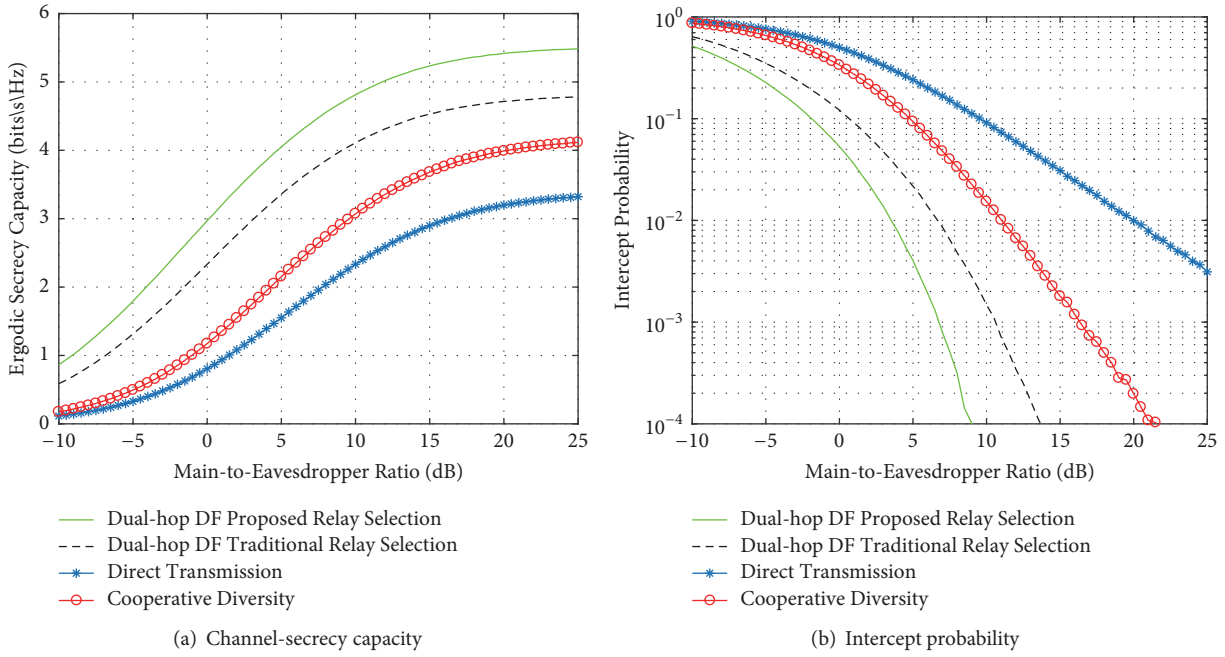
(ii) $\sigma^2_{si} = \sigma^2_{id} = \sigma^2_{ie} = 1$.

(iii) $N_t = 9$. SNR = 12 dB.

Figure 5 depicts the ergodic channel-secrecy capacity and intercepts probability comparison between traditional direct transmission and DF cooperative vehicle protocol for both the proposed system model and the traditional system model. Figure 5 shows that the traditional direct transmission is worse than the DF cooperative vehicle protocol regardless of the system model (traditional or proposed) used.

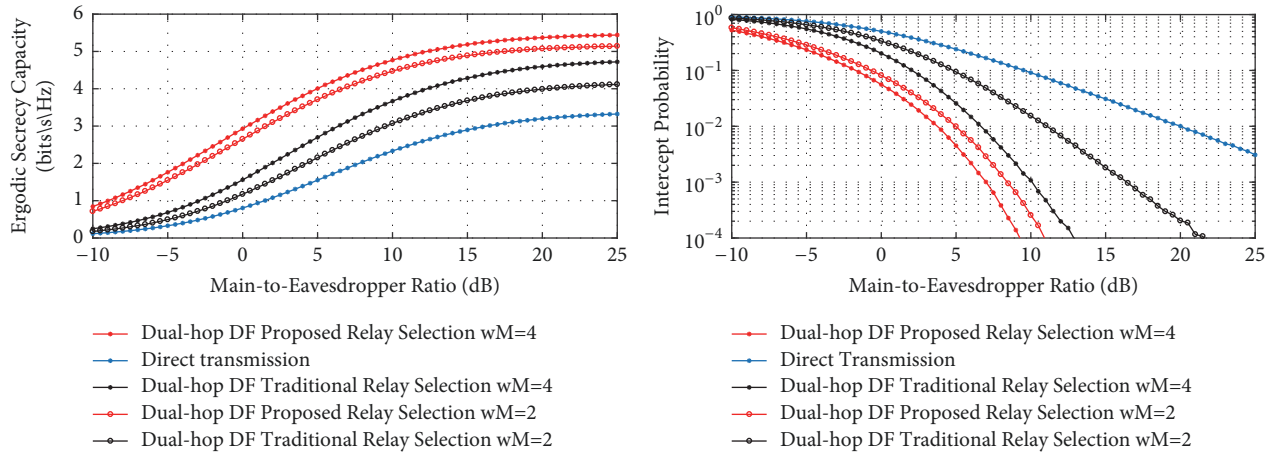
Moreover, when $M \geq 1$, the optimal system model always outperforms the traditional system model. Therefore, regardless of the DF relaying mechanism, whether it was optimal or traditional, the direct transmission and cooperative diversity relay selection constantly performs worse than the traditional and optimal relay selections in terms of both ergodic secrecy capacity and intercept probability.

Figure 5(a) presents ergodic channel-secrecy capacity comparison between direct transmission and DF cooperative vehicle schemes with the traditional and the proposed system models. As shown in Figure 5(a), the proposed system model gives better channel-secrecy capacity




(a) Channel-secrecy capacity (b) Intercept probability

FIGURE 5: $C_S$ and $P_{\text{intercept}}$ probability versus MER for dual-hop DF cooperative vehicles schemes.




(a) Channel-secrecy capacity (b) Intercept probability

FIGURE 6: $C_S$ and $p_{\text{intercept}}$ versus MER of dual-hop DF cooperative vehicles scheme (proposed and traditional relay selection mechanisms) and direct transmission system models with different number of transmitted relays.

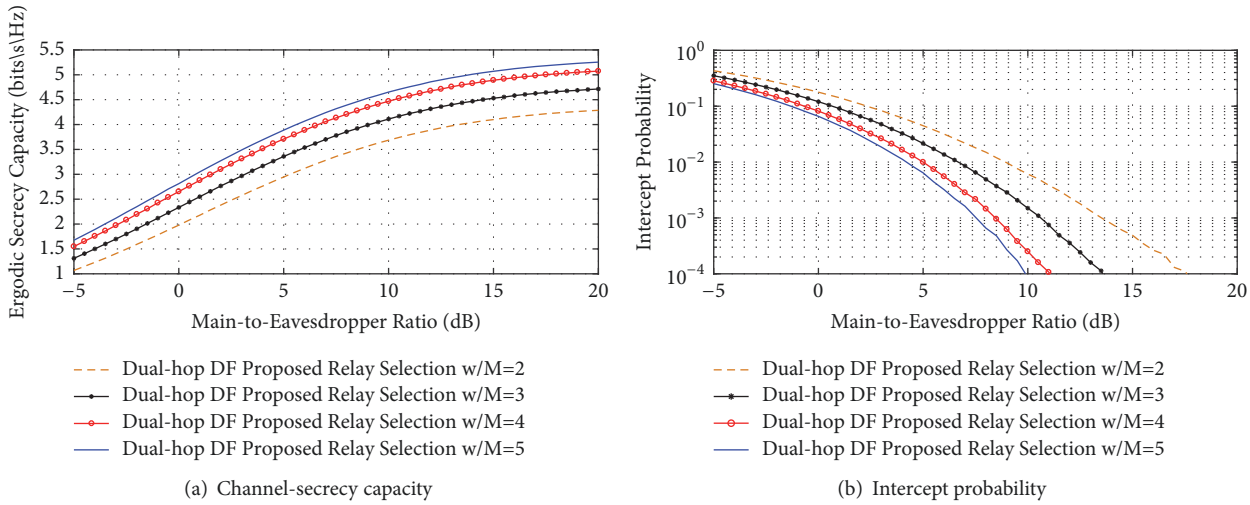
than the traditional system model and the conventional direct transmission. Increasing channel capacity implies that using cooperative relays enhances the overall system security.

Figure 5(b) shows that the best intercept probability performance is given by DF cooperative vehicle scheme using either the proposed or the traditional system model when compared to conventional direct transmission. Moreover, the proposed system model is better than the traditional system model with respect to intercept probability.

Figure 6 shows that as the number of relays between a transmitter and receiver increases ($M = 2$ and 4), the physical layer security is improving using either our proposed system model or the cooperative system model. Additionally, Figure 6 shows that the proposed system model is strictly higher than that of either the cooperative system model or the conventional transmission.

Figure 6(a) shows that as the number of relays increases, the ergodic channel-secrecy capacity improves. It is obvious that the channel-secrecy capacity of the dual-hop DF proposed and traditional system models with $M = 4$ is higher than the capacity of $M = 2$.

Figure 6(b) shows that the probability of the eavesdropper to listen the transmitted data is decreased in our proposed




(a) Channel-secrecy capacity

(b) Intercept probability

FIGURE 7: $C_S$ and $p_{\text{intercept}}$ versus MER of dual-hop DF cooperative vehicles scheme: comparison of proposed relay selection mechanism with different number of transmitted relays.

system model. Moreover, the intercept probability of the dual-hop DF proposed and traditional system models with $M = 4$ is lower than the intercept probability of $M = 2$. Therefore, the overall physical layer security in the proposed system model is the highest one.

Figure 7 characterizes the effect of varying number of relays when relay's gain is constant for DF cooperative vehicle algorithm. Moreover, Figure 7 presents the channel-secrecy capacity and the intercept probability of the proposed system model for a different number of relays $M = 2, 3, 4, 5$. The channel-secrecy capacity of the proposed dual-hop DF cooperative diversity with $M = 5$ is the highest one.

Figure 7(a) shows significant increase in ergodic-secrecy capacity as the number of relays ($M$) increases. Therefore, channel-secrecy capacity of $M = 5$ has the highest channel secrecy and the lowest capacity is for $M = 2$.

Moreover, Figure 7(b) proves that the intercept probability of DF cooperative vehicle protocol with our proposed system model is improved by increasing the number of relays between transmitter and receiver. Therefore, DF cooperative vehicle protocol using the proposed system model has the best intercept probability.

Figure 8 depicts the effect of changing the relays locations with a constant number of relays $M = 2$ and constant geometric relays gain for DF cooperative vehicle algorithms.

Figure 8(a) presents the channel-secrecy capacity of DF using the proposed system model. Figure 8(a) shows that channel-secrecy capacity is significantly improved as the relays are closer to the source node. As per the aforementioned figure, the relays are closer to destination node, in which case an active/passive eavesdropper is able to attack the legitimate user data during the broadcast phase.

Figure 8(b) shows the improvement of the intercept probability when relays are closer to the source node. Therefore, by exploiting cooperative relays closer to the source node, the physical layer security will be improved.

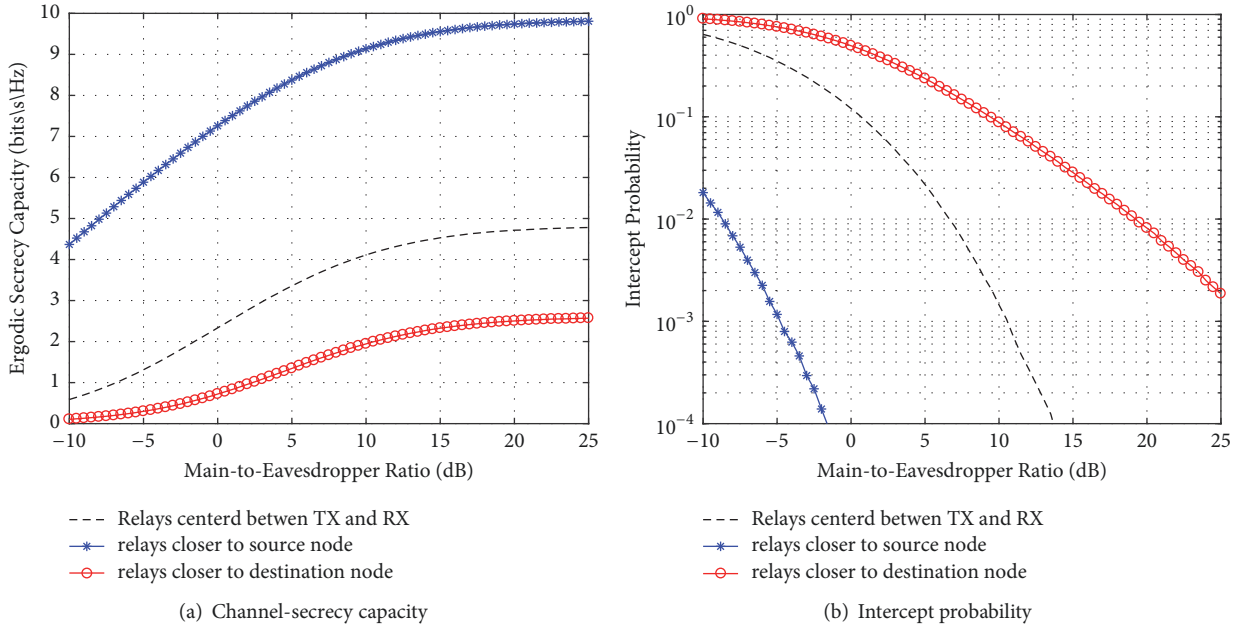
Figure 9 presents a comparison of the outage probability in our proposed system model and the traditional cooperative diversity with the direct transmission. It is clearly obvious from Figure 9 that the outage probability increases as MER increases, which is proved in (55). Moreover, Figure 9 shows that the outage probability of our proposed system model is strictly higher than the traditional cooperative diversity and direct transmission.

Figure 10 presents our numerical outage probability results for direct transmission, cooperative diversity relays, and the proposed cooperative vehicle scheme for different data rates. As shown from Figure 10, when the data rate increases from $R_d = 1.5$ to $R_d = 2.5$, the outage probability of our proposed model is strictly lower than the direct transmission and the traditional cooperative diversity at certain MER.

Figure 11 presents the relation between the outage probability and the used data rate $R_d$ from the source node with respect to the number of vehicular relays between the source and destination. As shown in Figure 11, when the data rate $R_d$ increases from $R_d = 1$ to $R_d = 4.5$, the outage probability is significantly reduced. It is also observed in Figure 11 that, for $R_d = 1$ to $R_d = 4.5$, the outage probability of our proposed system model tends to zero, as the number of relays increases from $M = 1$ to $M = 10^3$. This demonstrates that reliability of dual-hop vehicular cooperative model improves upon increasing the number of relays.

## 5. Conclusion

This paper proposed a novel technique to improve vehicular wireless channel secrecy by enabling precoded cooperative vehicular relaying to contribute towards the formation of an advanced telecommunication network. The goal is to increase network security by enhancing the channel secrecy and reducing the intercept probability. Best relay selection




(a) Channel-secrecy capacity

(b) Intercept probability

FIGURE 8: $C_S$ and $P_{\text{intercept}}$ versus MER of DF cooperative vehicles scheme: comparison of proposed system model with different relays locations.

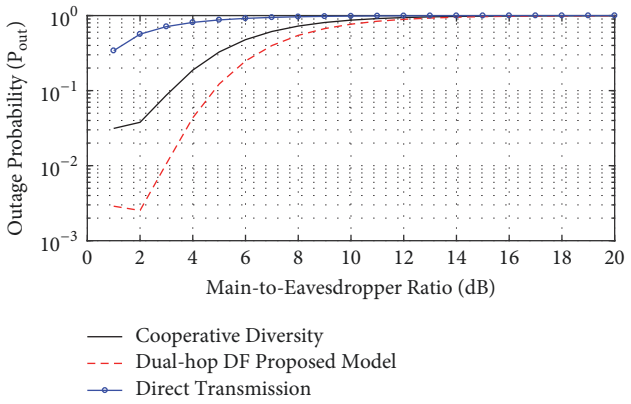



FIGURE 9: Outage probability of the direct transmission, cooperative diversity, and dual-hop DF cooperative vehicular relays versus the MER.

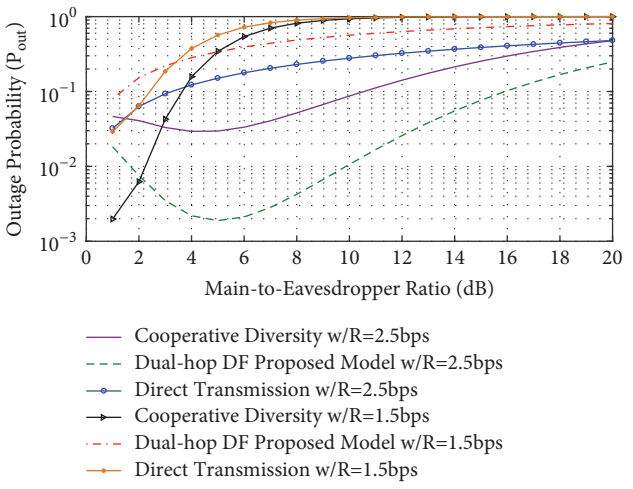



FIGURE 10: Outage probability of the direct transmission, cooperative diversity, and dual-hop DF cooperative vehicular relays versus the MER for different data rates $R_d$.

mechanism is presented as a base to realize security-through-diversity concepts for cooperative wireless vehicular networks.

This paper demonstrated that using vehicles to construct cooperative relaying in broadband networks not only potentiates reduced levels of power consumption but also provides lower error rates, increases channel security, and promises lower intercept probabilities. We employed a precoded cooperative transmission technique to extract the underlying rich multipath-Doppler-spatial diversity. Analytical and simulation results demonstrated significant increase in the physical layer security with a clear reduction in the required transmitting power compared with traditional transmission schemes. Our proposed scheme can be particularly useful in heavily populated urban areas.

Our future work will consider vehicle speed among other communication characteristics in various communication scenarios.

## Conflicts of Interest

The authors declare that there are no conflicts of interest.

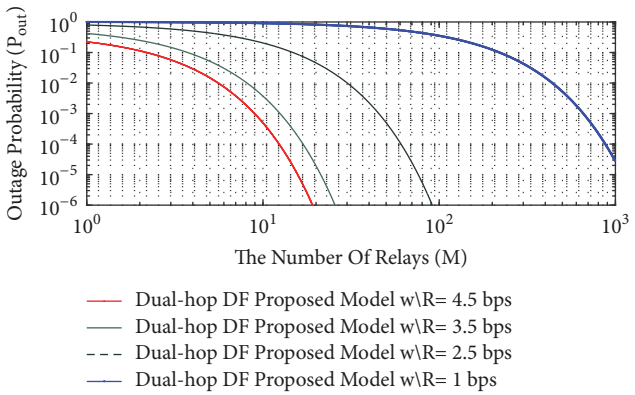



FIGURE 11: Outage probability of direct transmission, cooperative diversity, and dual-hop DF cooperative vehicular relays versus different number of relay nodes associated for different data rates $R_d$.

## Acknowledgments

This research was partially supported by the Roadway, Transportation, and Traffic Safety Research Center (RTTSRC) of the United Arab Emirates University (Grant no. 31R058). The authors would like to express their appreciation for the "IoT and Cyber Security Lab," SmartCI, Alexandria University, Egypt, for supporting and hosting the activities related to this manuscript.

## References

[1] E. M. Ghourab, M. Azab, M. Rizk, and A. Mokhtar, "Security versus reliability study for power-limited mobile IoT devices," in *Proceedings of the 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 430–438, Vancouver, BC, October 2017.

[2] E. M. Ghourab, A. Mansour, M. Azab, M. Rizk, and A. Mokhtar, "Towards physical layer security in Internet of Things based on reconfigurable multiband diversification," in *Proceedings of the 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 446–450, Vancouver, BC, October 2017.

[3] A. Tulino, A. Lozano, and S. Verdu, "MIMO capacity with channel state information at the transmitter," in *Proceedings of the Eighth IEEE International Symposium on Spread Spectrum Techniques and Applications - Programme and Book of Abstracts*, pp. 22–26, Sydney, NSW, Australia.

[4] Y. Zhou and T.-S. Ng, "Performance analysis on MIMO-OFCDM systems with multi-code transmission," *IEEE Transactions on Wireless Communications*, vol. 8, no. 9, pp. 4426–4433, 2009.

[5] J. Hu and N. C. Beaulieu, "Performance analysis of decode-and-forward relaying with selection combining," *IEEE Communications Letters*, vol. 11, no. 6, pp. 489–491, 2007.

[6] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[7] S. V. Kartalopoulos, "A primer on cryptography in communications," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 146–151, 2006.

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

[9] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[10] J. N. Laneman, D. N. Tse, and G. . Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[11] E. R. Alotaibi and K. A. Hamdi, "Ergodic secrecy capacity analysis for cooperative communication with relay selection under non-identical distribution," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, Malaysia, May 2016.

[12] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *Proceedings of the ICC 2013 - 2013 IEEE International Conference on Communications*, pp. 2183–2187, Budapest, Hungary, June 2013.

[13] M. F. Feteiha and M. H. Ahmed, "Best-Relay Selection for Multi-Hop Vehicular Communication in Highways," in *Proceedings of the GLOBECOM 2015 - 2015 IEEE Global Communications Conference*, pp. 1–7, San Diego, CA, USA, December 2015.

[14] M. Feteiha and H. S. Hassanein, "Decode-and-Forward cooperative vehicular relaying for LTE-A MIMO-downlink," *Vehicular Communications*, vol. 3, pp. 12–20, 2016.

[15] M. F. Feteiha and M. Uysal, "On the Performance of MIMO Cooperative Transmission for Broadband Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2297–2305, 2015.

[16] M. F. Feteiha and M. Uysal, "Multipath-Doppler Diversity for Broadband Cooperative Vehicular Communications," in *Proceedings of the ICC 2011 - 2011 IEEE International Conference on Communications*, pp. 1–6, Kyoto, Japan, June 2011.

[17] T. Chrysikos, T. Dagiuklas, and S. Kotsopoulos, "Wireless Information-Theoretic Security in MANETs," in *Proceedings of the 2013 IEEE International Conference on Communications (ICC). Workshops*, pp. 692–696, Budapest, June 2013.

[18] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, 2006.

[19] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[20] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073–1096, 2003.

[21] C. E. Shannon, "A mathematical theory of communication," *Bibliometrics*, vol. 5, no. 1, pp. 3–55, 2001.

[22] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 58, no. 10, pp. 5438–5455, 2010.