Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces

Abubakar U. Makarfi[1], Khaled M. Rabie[2], Omprakash Kaiwartya[3], Xingwang Li[4], Rupak Kharel[1]
[1]Department of Computing and Mathematics, Manchester Metropolitan University, UK
[2]Department of Engineering, Manchester Metropolitan University, UK
[3]School of Science and Technology, Nottingham Trent University, UK
[4]School of Physics and Electronic Information Engineering, Henan Polytechnic University, China
Emails:{a.makarfi, r.kharel, k.rabie}@mmu.ac.uk; omprakash.kaiwartya@ntu.ac.uk; lixingwang@hpu.edu.cn.

***Abstract*—This paper studies the physical layer security (PLS) of a vehicular network employing a reconfigurable intelligent surface (RIS). RIS technologies are emerging as an important paradigm for the realisation of smart radio environments, where large numbers of small, low-cost and passive elements, reflect the incident signal with an adjustable phase shift without requiring a dedicated energy source. Inspired by the promising potential of RIS-based transmission, we investigate two vehicular network system models: One with vehicle-to-vehicle communication with the source employing a RIS-based access point, and the other model in the form of a vehicular adhoc network (VANET), with a RIS-based relay deployed on a building. Both models assume the presence of an eavesdropper to investigate the average secrecy capacity of the considered systems. Monte-Carlo simulations are provided throughout to validate the results. The results show that performance of the system in terms of the secrecy capacity is affected by the location of the RIS-relay and the number of RIS cells. The effect of other system parameters such as source power and eavesdropper distances are also studied.**

***Index Terms*—Double-Rayleigh fading channels, physical layer security, reconfigurable intelligent surfaces, secrecy capacity, vehicular communications.**

I. INTRODUCTION

Recent research in beyond 5G technologies has brought about new communication paradigms, especially at the physical layer. One of such emerging paradigms is the concept of “smart radio environments”, enabled by technologies to control the propagation environment in order to improve signal quality and coverage, such as reflector-arrays/intelligent walls and reconfigurable intelligent surfaces (RIS) [1], [2]. RISs are man-made surfaces of electromagnetic material that are electronically controlled with integrated electronics and have unique wireless communication capabilities [3].

RIS-based transmission concepts have been shown to be completely different from existing MIMO, beamforming and amplify-and-forward/decode-and-forward relaying paradigms, where the large number of small, low-cost and passive elements on a RIS only reflect the incident signal with an adjustable phase shift without requiring a dedicated energy source for RF processing or retransmission [4]. Applications of RIS have recently been investigated with respect to signal-to-noise ratio (SNR) maximisation [4], improving signal coverage [5], improving massive MIMO systems [6], beamforming optimisation [7]–[9], as well as multi-user networks [10].

On the other hand, physical layer security (PLS) in vehicular networks is important due to rapid advancements towards autonomous vehicles and smart/cognitive transportation networks to minimise the risk from compromise. Significant research efforts have been expended in studying vehicular networks with [11] or without PLS [12]–[15]. Given that PLS employs the inherent characteristics of the propagation channels, such as interference, fading and noise to realise keyless secure transmission through signal processing approaches [2], then RIS-based systems are well positioned for such applications. Initial results have been reported for PLS studies for systems employing RIS technologies [16], [17]. However, no such studies have been conducted for vehicular adhoc networks (VANETs).

From the aforementioned, this study presents the following contributions. We study the PLS of two possible vehicular network models, by analysing and deriving expressions for the average secrecy capacity. The first model considers a vehicle-to-vehicle (V2V) network with the source vehicle employing a RIS-based access point (AP) for transmission. In the second model, we consider a VANET with a source station transmission via a RIS-based relay. Such a RIS-relay could be deployed on a building as part of a smart infrastructure within a city. To the best of our knowledge, this is the first analysis of a RIS-based technology employed within a VANET. Moreover, the distances of the legitimate and eavesdropper nodes are taking into account along with realistic fading scenarios considered for the base stations and the mobile nodes. Monte Carlo simulations are provided throughout to verify the accuracy of our analysis. The results show that the performance of the system in terms of the secrecy capacity is improved with the use of the RIS. Furthermore, the effect of the system parameters such as source power, eavesdropper distance and number of RIS cells on the system performance are investigated.

The paper is organised as follows. In Sections II and III, we describe the two system models under study and analyse the secrecy performance by deriving accurate analytical expressions for efficient computation of the secrecy capacity of the networks. Finally, in Sections IV and V, we present the results with discussions and outline the main conclusions, respectively.

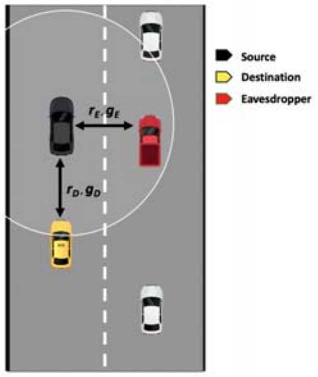

Figure 1: System model for V2V scenario with the source vehicle using RIS as AP.

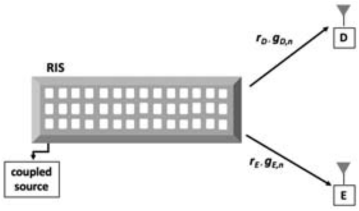

Figure 2: Vehicle RIS configuration as an AP.

II. V2V WITH RIS AS ACCESS POINT

In this section, we describe the V2V network with RIS as AP and derive expressions for the average secrecy capacity of the system.

A. System Description

We consider a system of vehicles operating in a network as shown in Fig. 1. We assume a classic Wyner's wiretap model in our analysis [18], such that an information source vehicle (S), sends confidential information to a destination vehicle (D), while a passive eavesdropper[1] vehicle (E) attempts to receive and decode the confidential information. The vehicles D and E are known to lie within a certain radius from S, the precise relative distances of the V2V links are unknown during transmission, which is a realistic assumption for a network of this nature [11], [19]. Moreover, S is assumed to employ a RIS-based scheme in the form of an AP to communicate over the network[2]. As shown in the block diagram of Fig. 2, the RIS can be connected over a wired link or optical fiber for direct transmission from S, and can support transmission without RF processing. For the system considered, we assume an intelligent AP with the RIS having knowledge of channel phase terms, such that the RIS-induced phases can be adjusted to maximise the received SNR through appropriate phase cancellations and proper alignment of reflected signals from the intelligent surface.

[1]Passive eavesdropper in the sense that the node only intercepts the information, but makes no attempt to actively disrupt, such as through jamming.

[2]Initial proposal and results for such a configuration of intelligent surfaces were reported in [4].

For a RIS configuration with N cells, the received signals at D and E are respectively represented as

$$y_D = \left[\sum_{n=1}^{N} h_{D,n} e^{-j\phi_n}\right] x + w_D, \tag{1}$$

$$y_E = \left[\sum_{n=1}^{N} h_{E,n} e^{-j\phi_n}\right] x + w_E, \tag{2}$$

where x represents the transmitted signal by S with power P_s, while the terms w_D and w_E are the respective additive white Gaussian noise (AWGN) at D and E. Without loss of generality, we denote the power spectral density of the AWGN as N_0 and equal at both links. The terms $h_{i,n} = \sqrt{g_{i,n} r_i^{-\beta}}, \quad i \in \{D, E\}$, is the channel coefficient from S to the receiving vehicles D and E, where r_i is the V2V link distance, β is the path-loss exponent and $g_{i,n}$ is the channel gain from the RIS to the receiver, following independent double Rayleigh fading [11]. The term ϕ_n is the reconfigurable phase induced by the nth reflector of the RIS, which through phase matching, the SNR of the received signals can be maximised[3].

Based on (1) and (2), the instanstaneous SNRs at D and E are given by

$$\gamma_D = \frac{\sum_{n=1}^{N} P_s \mid h_{D,n} \mid^2}{N_0}, \tag{3}$$

and

$$\gamma_E = \frac{\sum_{n=1}^{N} P_s \mid h_{E,n} \mid^2}{N_0}. \tag{4}$$

B. Average Secrecy Capacity Analysis

In this section, we derive analytical expressions for the secrecy capacity of the system. The maximum achievable secrecy capacity is defined by [20]

$$C_s = \max\left\{C_D - C_E, 0\right\}, \tag{5}$$

where $C_D = \log_2(1+\gamma_D)$ and $C_E = \log_2(1+\gamma_E)$ are the instantaneous capacities of the main and eavesdropping links, respectively. The secrecy capacity in (5) can therefore be expressed as [20]

$$C_s = \begin{cases} \log_2(1+\gamma_D) - \log_2(1+\gamma_E), & \gamma_D > \gamma_E, \\ 0, & \gamma_D < \gamma_E. \end{cases} \tag{6}$$

The average secrecy capacity $\overline{C_s}$ is given by [21]

$$\begin{aligned} \overline{C_s} &= \mathbb{E}\left[C_s(\gamma_D, \gamma_E)\right] \\ &= \int_0^\infty \int_0^\infty C_s(\gamma_D, \gamma_E) f(\gamma_D, \gamma_E) \, \mathrm{d}\gamma_D \mathrm{d}\gamma_E, \end{aligned} \tag{7}$$

where $\mathbb{E}[\cdot]$ is the expectation operator and $f(\gamma_D, \gamma_E)$ is the joint PDF of γ_D and γ_E. In order to simplify the analysis, we

[3]For the sake of brevity, the reader is referred to [4], for details of phase cancellation techniques.

express the logarithmic function in (5) in an alternate form. Recalling the identity [22, Eq. (6)]

$$\ln(1+\zeta) = \int_0^\infty \frac{1}{s}\left(1-e^{-\zeta s}\right)e^{-s}\mathrm{d}s, \tag{8}$$

and by substituting $\zeta = \gamma_D$ in (8), we can express the instantaneous capacity of the main link as

$$\overline{C}_D = \frac{1}{\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\mathcal{M}_D(z)\right)e^{-z}\mathrm{d}z, \tag{9}$$

where $\mathcal{M}_D(z) = \mathbb{E}\left[e^{-z\frac{P_s r_D^{-\beta}}{N_0}\sum_{n=1}^N g_{D,n}}\right]$ is the moment generating function (MGF) of the SNR at D.

Next, we compute the MGF $\mathcal{M}_D(z)$, defined by

$$\begin{aligned}\mathcal{M}_D(z) =& \mathbb{E}\left[e^{-z\frac{P_s r_D^{-\beta}}{N_0}\sum_{n=1}^N g_{D,n}}\right] \\ =& \prod_{n=1}^N \mathbb{E}\left[e^{-z\frac{P_s r_D^{-\beta}}{N_0} g_{D,n}}\right] \\ =& \prod_{n=1}^N \int_g e^{-z\xi_D g_{D,n}} f_{g_D}(g)\mathrm{d}g_D, \end{aligned}\tag{10}$$

then from the generalized cascaded Rayleigh distribution, we can obtain the PDF of the double Rayleigh channel for $n=2$ in [23, Eq. (8)] as $f(g) = \mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g^2\middle|\begin{matrix}-\\ \frac{1}{2},\frac{1}{2}\end{matrix}\right)$. By invoking [24, Eq. (9.34.3)], we can express the PDF by re-writing the Meijer G-function in an alternate form. Thus, we get

$$f(g) = \mathrm{G}_{0,2}^{2,0}\left(\frac{1}{4}g^2\middle|\begin{matrix}-\\ \frac{1}{2},\frac{1}{2}\end{matrix}\right) = gK_0(g). \tag{11}$$

Using (11) and [24, Eq. (6.621.3)] along with some basic algebraic manipulations, we can obtain the desired result as

$$\mathcal{M}_D(z) = \prod_{n=1}^N \frac{4}{3(1+z\frac{P_s r_D^{-\beta}}{N_0})^2}\,{}_2F_1\left(2,\frac{1}{2},\frac{5}{2},\frac{z\frac{P_s r_D^{-\beta}}{N_0}-1}{z\frac{P_s r_D^{-\beta}}{N_0}+1}\right), \tag{12}$$

where ${}_2F_1(\alpha;\beta;\gamma;z)$ is the Gauss hypergeometric function [24, Eq. (9.111)].

Using similar analysis, the average capacity of the eavesdropper link can be represented as

$$\overline{C}_E = \frac{1}{\ln(2)}\int_0^\infty \frac{1}{z}\left(1-\mathcal{M}_E(z)\right)e^{-z}\mathrm{d}z, \tag{13}$$

where the MGF $\mathcal{M}_E(z) = \mathbb{E}\left[e^{-z\frac{P_s r_E^{-\beta}}{N_0}\sum_{n=1}^N g_E}\right]$ and can be similarly evaluated as

$$\mathcal{M}_E(z) = \prod_{n=1}^N \frac{4}{3(1+z\frac{P_s r_E^{-\beta}}{N_0})^2}\,{}_2F_1\left(2,\frac{1}{2},\frac{5}{2},\frac{z\frac{P_s r_E^{-\beta}}{N_0}-1}{z\frac{P_s r_D^{-\beta}}{N_0}+1}\right). \tag{14}$$

From (6), (9), (12) - (14), the average secrecy capacity can be represented as (15), shown at the top of the next page.

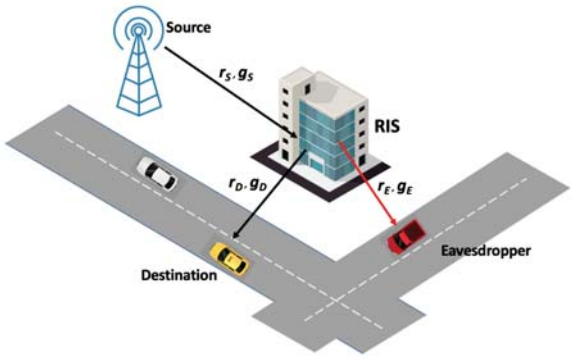

Figure 3: System model for a vehicular network scenario. Source station using building-mounted-RIS as relay for vehicular communication.

III. VANET Transmission Through RIS Relay

In this section, we describe the VANET system transmitting through a RIS relay and derive expressions for the average secrecy capacity of the system.

A. System Description

In this section, we consider an RIS-based scheme with the RIS employed as a relay or reflector for vehicular nodes in the network. Fig. 3 illustrates the RIS-based system under consideration. The RIS is deployed on a building and used as a relay for the signal from stationary source S, while D and E are assumed to be highly mobile vehicular nodes. Under this assumption, the source-to-RIS channel g_s is assumed to be Rayleigh faded, while the RIS-to-destination and RIS-to-eavesdropper fading channels, g_D and g_E are assumed to be double-Rayleigh distributed. The RIS is in the form of a reflect-array comprising N reconfigurable reflector elements, capable of being controlled by a communication oriented software for intelligent transmission. With this in mind, the received signals at D and E are

$$y_i = \left[\sum_{n=1}^N h_s h_{i,n} e^{-j\phi_n}\right]x + w_i, \tag{16}$$

where $h_{s,n} = \sqrt{g_{s,n} r_s^{-\beta} e^{-j\theta_n}}$ is the source-to-RIS channel with distance r_s, phase component θ_n and g_s following a Rayleigh fading distribution. The term $h_{i,n} = \sqrt{g_{i,n} r_i^{-\beta} e^{-j\psi_n}}$, $i \in \{D,E\}$, is the channel coefficient from RIS-to-vehicle node, with distance r_i, path-loss exponent β, phase component ψ_n and $g_{i,n}$ following a double-Rayleigh distribution to model the mobility of the nodes. [11]. The instanstaneous SNRs at D and E are given respectively by

$$\gamma_D^r = \frac{\sum_{n=1}^N P_s \mid h_{s,n} \mid^2 \mid h_{D,n} \mid^2}{N_0} \tag{17}$$

and

$$\gamma_E^r = \frac{\sum_{n=1}^N P_s \mid h_{s,n} \mid^2 \mid h_{E,n} \mid^2}{N_0} \tag{18}$$

$$\overline{C}_s = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} e^{-z} \left[\left(\left(1 - \left\{ \frac{4}{3\left(N_0 + zP_s r_D^{-\beta}\right)^2} {}_2F_1\left(2, \frac{1}{2}, \frac{5}{2}, \frac{zP_s r_D^{-\beta} - N_0}{zP_s r_D^{-\beta} + N_0}\right) \right\} \right)^N \right. \right.$$
$$\left. \left. - \left(1 - \left\{ \frac{4}{3\left(N_0 + zP_s r_E^{-\beta}\right)^2} {}_2F_1\left(2, \frac{1}{2}, \frac{5}{2}, \frac{zP_s r_E^{-\beta} - N_0}{zP_s r_E^{-\beta} + N_0}\right) \right\} \right)^N \right] \mathrm{d}z. \quad (15)$$

B. Average Secrecy Capacity Analysis

From (9), we obtain the average capacity for the destination V2V link as

$$\overline{C}_{D,r} = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_{D,r}(z)\right) e^{-z} \mathrm{d}z, \quad (19)$$

where $\mathcal{M}_{D,r}(z) = \mathbb{E}\left[e^{-z\frac{P_s r_s^{-\beta} r_D^{-\beta}}{N_0} \sum_{n=1}^{N} g_{s,n} g_{D,n}}\right]$ is the MGF of the SNR at D. As for the joint distribution of g_s and g_D, given that g_s is a Rayleigh RV and g_D is a double-Rayleigh RV, we can define the RV $g = g_s g_D$, which follows the cascaded Rayleigh distribution with $n = 3$. From the generalized cascaded Rayleigh distribution [23], we can evaluate the PDF of g as

$$f(g) = \frac{1}{\sqrt{2}} \mathrm{G}_{0,3}^{3,0}\left(\frac{1}{8} g^2 \middle| \begin{matrix} - \\ \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \end{matrix} \right). \quad (20)$$

Thus, the $\mathcal{M}_{D,r}(z)$ is given by

$$\begin{aligned} \mathcal{M}_{D,r}(z) =& \mathbb{E}\left[e^{-z\frac{P_s r_s^{-\beta} r_D^{-\beta}}{N_0} \sum_{n=1}^{N} g_{s,n} g_{D,n}}\right] \\ =& \prod_{n=1}^{N} \int_0^\infty e^{-zg\frac{P_s r_s^{-\beta} r_D^{-\beta}}{N_0}} f_g(g) \mathrm{d}g \\ =& \prod_{n=1}^{N} \int_0^\infty \frac{1}{\sqrt{2}} e^{-zg\frac{P_s r_s^{-\beta} r_D^{-\beta}}{N_0}} \mathrm{G}_{0,3}^{3,0}\left(\frac{1}{8} g^2 \middle| \begin{matrix} - \\ \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \end{matrix} \right) \mathrm{d}g. \end{aligned} \quad (21)$$

Using (20) and [24, Eq. (7.813.2)] along with some basic algebraic manipulations, we can obtain the MGF as

$$\mathcal{M}_{D,r}(z) = \prod_{n=1}^{N} \frac{1}{z\mu_d\sqrt{2\pi}} \mathrm{G}_{2,3}^{3,2}\left(\frac{1}{2(z\mu_d)^2} \middle| \begin{matrix} 0, \frac{1}{2} \\ \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \end{matrix} \right), \quad (22)$$

where $\mu_d = \frac{P_s r_s^{-\beta} r_D^{-\beta}}{N_0}$. Using similar analysis, the average capacity of the eavesdropper link can be represented as

$$\overline{C}_{E,r} = \frac{1}{\ln(2)} \int_0^\infty \frac{1}{z} \left(1 - \mathcal{M}_{E,r}(z)\right) e^{-z} \mathrm{d}z, \quad (23)$$

where the MGF $\mathcal{M}_{E,r}(z) = \mathbb{E}\left[e^{-z\frac{P_s r_s^{-\beta} r_E^{-\beta}}{N_0} \sum_{n=1}^{N} g_{s,n} g_{E,n}}\right]$ and can be similarly evaluated as

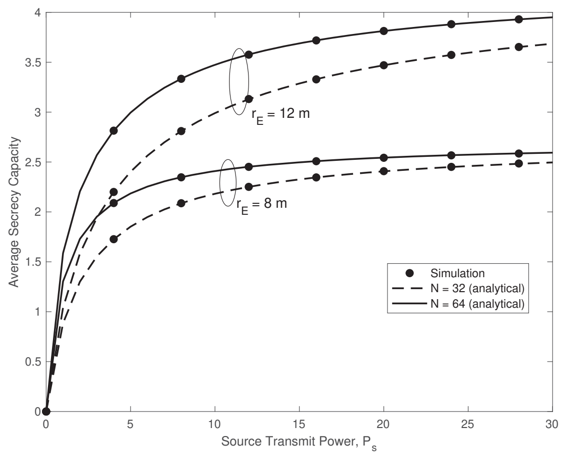

Figure 4: Average secrecy capacity versus source transmit power P_s for the V2V network with RIS as AP. Parameters considered with varying eavesdropper distance r_E and number of RIS cells N.

$$\mathcal{M}_{E,r}(z) = \prod_{n=1}^{N} \frac{1}{z\mu_e\sqrt{2\pi}} \mathrm{G}_{2,3}^{3,2}\left(\frac{1}{2(z\mu_e)^2} \middle| \begin{matrix} 0, \frac{1}{2} \\ \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \end{matrix} \right), \quad (24)$$

where $\mu_e = \frac{P_s r_s^{-\beta} r_e^{-\beta}}{N_0}$.

From (6), (19), (22) - (24), the average secrecy capacity can be represented as (25), shown at the top of the next page.

IV. Numerical Results and Discussions

In this section, we present and discuss some results from the mathematical expressions derived in the paper. We then investigate the effect of key parameters on the secrecy capacity of the system. The results are then verified using Monte Carlo simulations with at least 10^6 iterations. Unless otherwise stated, we have assumed source power $P_s = 10$W, RIS-to-D distance $r_D = 4$m, RIS-to-E distance $r_E = 8$m, source-to-RIS distance $r_s = 10$m and pathloss exponent $\beta = 2.7$.

In Fig. 4, we commence analysis for the V2V network model, with the average secrecy capacity against source power for different numbers of RIS cells and eavesdropper distances. It can be observed that the secrecy capacity increases with an increase in P_s, r_E or N. It can be further noted that within the region considered, the eavesdropper distance has a greater effect on the secrecy capacity than doubling the number of RIS cells. Also, the effect of increased RIS cells, is more pronounced when the eavesdropper is further away. A similar analysis can be made for the average secrecy capacity of

$$
\overline{C}_{s,r} = \frac{1}{\ln(2)} \int_{0}^{\infty} \frac{1}{z} e^{-z} \left[\left(1 - \left\{ \frac{N_0}{\sqrt{2\pi} z P_s r_s^{-\beta} r_D^{-\beta}} \mathrm{G}_{2,3}^{3,2} \left(\frac{1}{2} \left(\frac{N_0}{z P_s r_s^{-\beta} r_D^{-\beta}} \right)^2 \middle| \begin{matrix} 0, \frac{1}{2} \\ \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \end{matrix} \right) \right\}^N \right) \right.
$$

$$
\left. - \left(1 - \left\{ \frac{N_0}{z P_s r_s^{-\beta} r_E^{-\beta} \sqrt{2\pi}} \mathrm{G}_{2,3}^{3,2} \left(\frac{1}{2} \left(\frac{N_0}{z P_s r_s^{-\beta} r_E^{-\beta}} \right)^2 \middle| \begin{matrix} 0, \frac{1}{2} \\ \frac{1}{2}, \frac{1}{2}, \frac{1}{2} \end{matrix} \right) \right\}^N \right) \right] \mathrm{d}z. \quad (25)
$$

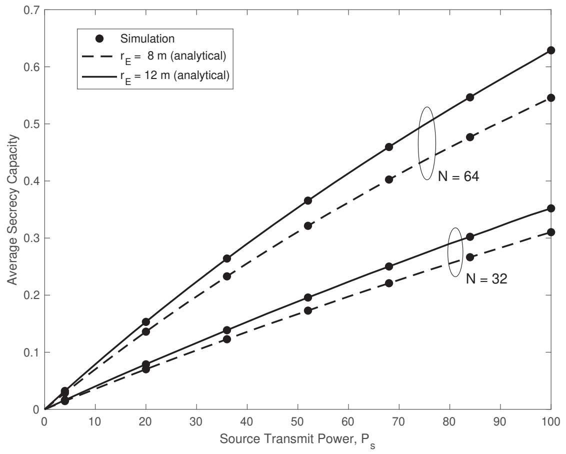

Figure 5: Average secrecy capacity versus source transmit power P_s for the VANET with RIS as relay. Parameters considered with varying eavesdropper distance r_E and number of RIS cells N.

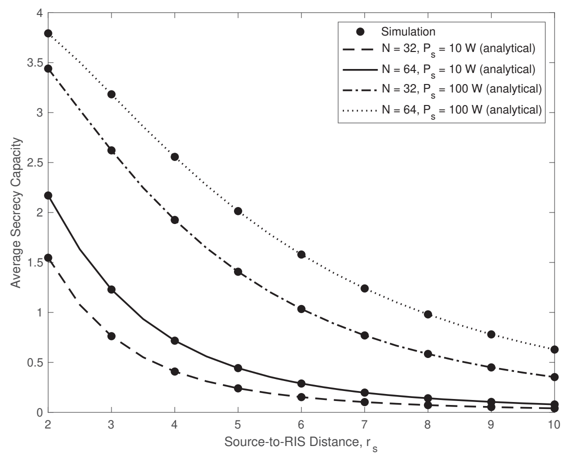

Figure 6: Average secrecy capacity versus source-to-RIS distance for the VANET with RIS as relay. Parameters considered with varying source transmit power P_s and number of RIS cells N.

the VANET RIS-relay model considered, as observed in Fig. 5. However, the effect of increased source power produces an almost linear response for the secrecy capacity, while the effective value of the secrecy capacity is much lower than the V2V RIS model for similar P_s.

Fig. 6, shows a plot of the average secrecy capacity against r_s with different values of P_s and N, for the VANET RIS-relay system. We assume the RIS-to-eavesdropper distance $r_E = 12$m. First, we observe that the average secrecy capacity decreases as the source distance increases, demonstrating the effect of fading and pathloss on the link, before the RIS relay. The result also demonstrates that doubling the number of RIS cells has less influence on the average secrecy capacity, as compared to the impact of the source power, within the observed region.

V. Conclusions

In this paper, we examined the secrecy capacity as a key metric for PLS of a wireless vehicular communication network. Two scenarios of a RIS-based vehicular network were considered. The results demonstrate how the secrecy capacity of a vehicular network can be improved with respect to the source power, eavesdropper distance and the number of RIS cells. The results further showed how the location and size of RIS (in terms of number of RIS cells) can be employed to improve a RIS relay-based VANET.

References

[1] M. D. Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. C. Alexandropoulos, J. Hoydis, H. Gacanin, J. d. Rosny, A. Bounceur, G. Lerosey, and M. Fink, "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 129, May 2019. [Online]. Available: https://doi.org/10.1186/s13638-019-1438-9

[2] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.

[3] E. Basar, M. D. Renzo, J. D. Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[4] E. Basar, "Transmission Through Large Intelligent Surfaces: A New Frontier in Wireless Communications," in *2019 European Conf. Netw. Commun. (EuCNC)*, Jun. 2019, pp. 112–117.

[5] L. Subrt and P. Pechac, "Controlling propagation environments using intelligent walls," in *6th European Conf. Antennas Propag. (EUCAP)*, Mar. 2012, pp. 1–5.

[6] S. Hu, F. Rusek, and O. Edfors, "Beyond Massive MIMO: The Potential of Data Transmission With Large Intelligent Surfaces," *IEEE Trans. Sig. Process.*, vol. 66, no. 10, pp. 2746–2758, May 2018.

[7] Q. Wu and R. Zhang, "Beamforming optimization for intelligent reflecting surface with discrete phase shifts," in *IEEE Int. Conf. Acoust., Speech and Sig. Process. (ICASSP)*, May 2019, pp. 7830–7833.

[8] ——, "Intelligent reflecting surface enhanced wireless network: Joint active and passive beamforming design," in *IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[9] X. Tan, Z. Sun, J. M. Jornet, and D. Pados, "Increasing indoor spectrum sharing capacity using smart reflect-array," in *IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[10] C. Huang, A. Zappone, M. Debbah, and C. Yuen, "Achievable Rate Maximization by Passive Intelligent Mirrors," in *IEEE Int. Conf. Acoust. Speech Sig. Process. (ICASSP)*, Apr. 2018, pp. 3714–3718.

[11] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On Physical Layer Security of Double Rayleigh Fading Channels for Vehicular Communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

[12] I. Dey, R. Nagraj, G. G. Messier, and S. Magierowski, "Performance analysis of relay-assisted mobile-to-mobile communication in double or cascaded Rayleigh fading," in *IEEE Pacific Rim Conf. Commun. Comput. Sign. Process.*, Aug. 2011, pp. 631–636.

[13] R. Kasana, S. Kumar, O. Kaiwartya, R. Kharel, J. Lloret, N. Aslam, and T. Wang, "Fuzzy-based channel selection for location oriented services in multichannel VCPS environments," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4642–4651, Dec 2018.

[14] O. Kaiwartya, Y. Cao, J. Lloret, S. Kumar, N. Aslam, R. Kharel, A. H. Abdullah, and R. R. Shah, "Geometry-Based Localization for GPS Outage in Vehicular Cyber Physical Systems," *IEEE Trans. Veh. Tech.*, vol. 67, no. 5, pp. 3800–3812, May 2018.

[15] S. Kumar, U. Dohare, K. Kumar, D. Prasad, K. N. Qureshi, and R. Kharel, "Cybersecurity measures for geocasting in vehicular cyber physical system environments," *IEEE Internet Things J.*, pp. 1–1, 2019.

[16] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, pp. 1–1, 2019.

[17] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[18] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M. Alouini, "Secrecy Capacity Analysis Over α-μ Fading Channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[19] D. S. Karas, A. A. Boulogeorgos, and G. K. Karagiannidis, "Physical layer security with uncertainty on the location of the eavesdropper," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 540–543, Oct. 2016.

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

[21] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. Rabie, and N. Al-Dhahir, "On the secrecy capacity of Fisher-Snedecor $\mathcal{F}$ fading channels," in *14th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2018, pp. 102–107.

[22] K. A. Hamdi, "Capacity of MRC on correlated Rician fading channels," *IEEE Trans. Commun.*, vol. 56, no. 5, pp. 708–711, May 2008.

[23] J. Salo, H. M. El-Sallabi, and P. Vainikainen, "The distribution of the product of independent Rayleigh random variables," *IEEE Trans. Antennas Propag.*, vol. 54, no. 2, pp. 639–643, Feb. 2006.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Califonia: Academic Press, 7th ed., 2007.