Secrecy Capacity Analysis of Reconfigurable Intelligent Surface Based Vehicular Networks

Ashokraj Murugesan
Department of Electronics and Communication Engineering, Oxford Engineering College, India
ashokrajom@gmail.com

Ananthi Govindasamay
Department of Electronics and Communication Engineering, Thiagarajar College of Engineering College, India
gananthi@tce.edu

Abstract: *As Vehicular Networks based technologies are in the close proximity of deployment for various wireless applications under proposal worldwide, this research paper proposes secrecy capacity analysis for Reconfigurable Intelligent Surface (RIS) based Vehicular Network. The proposed network model has a fixed infrastructure comprising of source node, destination node incorporated with single antenna and passive eavesdropper forming the scenario. RIS based Vehicular communication links are modelled by Rayleigh fading for source-to RIS link and RIS to destination Vehicle, whereas Eavesdropper channel links are Double-Rayleigh amplitude distribution, induced by double scattering in the channel. For this scenario, we derive the closed-form expressions for the average Secrecy Capacity and Secrecy Outage Probability (SOP) of the considered system. Though, Secrecy Capacity analysis is an excellent performance metric for assessing eavesdropper based system, it has been reported by various research works, this research paper differentiates from other research papers by considering different secrecy rates and different distances of eavesdropper as presented in simulation. Further, to validate the obtained simulation results, theoretical results are also derived for assessing performance of SOP for various secrecy rates which is the highlight of this research paper and it can be used as benchmark for various research works to proceed further.*

Keywords: *Channel capacity, rayleigh fading channel, vehicular network, secrecy outage probability*.

Received February 8, 2021; accepted October 10, 2021
https://doi.org/10.34028/iajit/19/3/7

1. Introduction

Vehicular communication concatenated with relay based techniques [1] are considered to be the frontrunners to meet requirements of 5G wireless network standards where it contributes to an improvement in capacity, coverage and reliability aspects in comparison to existing standards where they are deemed to be vital for evolving wireless products. Key achievement and challenges of relay communication techniques are deployment of multiple relay based cells, which contribute an improvement in capacity, coverage, and bandwidth and data rate. Such performance metrics of various types of vehicular relay oriented communication systems are studied and analysed under various channel fading conditions as in the research work [15]. Though a number of performance metrics are prevalent for vehicular networks, whenever in the context of presence of a passive eavesdropper in relay based vehicular systems an important such metric which attains prime importance is secrecy capacity [20].

Secrecy capacity is information related metric which accounts for the amount of information rate when information is transmitted from an intended source node to the intended destination node with the constraint that the passive eavesdropper in the communication scenario is not able to access the information which is the universally recognized concept. Analysis of secrecy capacity and Physical layer security for Amplify and Forward (AF) relay network are analysed and studied in the research literatures from [9, 19, 20]. Moreover, in the presence of Eavesdroppers, secrecy capacity is obtained with the assumption that Channel State Information (CSI) is known at the transmitting end [9]. In addition optimal relay selection also needs to be considered if there is a possibility of multihop relay based scenario where it can be addressed based on channel quality or by jamming procedure which is used in decode-and-forward relay networks [11, 19] where intelligent transmission is done.

However, there are challenges and drawback of 5G wireless network discussed which are portrayed in [18] and also the key contribution of [18] is 6G systems which provides a vision that identifies, the applications, trends, performance metrics, and enabling technologies to impel the 6G revolution. Also irrespective of the fact generations in wireless networks for vehicular based networks utilization of relays can adequately turn a Non-Line Of Sight (NLOS) interface into numerous Line Of Sight (LOS) links. This methodology requires each relay to be employed in vehicular networks with a committed power source and a fundamental front-end hardware for gathering, processing, and retransmission of information in reconfigurable intelligent surface

networks. Reconfigurable Intelligent Surface (RIS) are an upcoming new technology and information analysis of such networks are presented in the research papers from [3, 6, 17, 21, 22].

Reconfigurable Intelligent Surface based 6G wireless communication systems developed are proficient of considerably reducing the power consumption in comparison to Cooperative communication systems [21]. In the security enhancements of Mobile Ad hoc Network (MANET) improved by position and energy based monitoring under various attack in [5]. Challenges and opportunities of a new brand technology Reconfigurable Intelligent Surface [6, 22] and reflecting intelligent surface of 6G wireless communications are dealt in the literature of [17]. The performance of Reconfigurable Intelligent Surface for wireless communications is analysed for various Signal to Noise Ratio (SNR) values in [3]. The RIS use Electro Magnetic (EM) material based artificial manmade surfaces that electronically are controlled with integrated electronics and RIS have unique wireless communication capabilities.

Further another aspect of RIS are that it refrains wireless location to increase spectrum and energy efficiencies. In research literature of [22] the following concepts and challenges are discussed with that of RIS aided communications and comparison of RIS with massive Multiple Input Multiple Output (MIMO) and other related terminologies such as reliability, capacity analysis, implementation of RIS for secure communications is done. The performance analysis of RIS aided Vehicle to Vehicle (V2V) network is discussed under various criteria and distance between source vehicle and destination vehicle is considered in [10].

The objective of RIS concepts in 6G wireless networks is to secure communications over a wiretap channel and further increase the data rate by using RIS at a legitimate receiver and decreasing the data rate at an eavesdropper [4]. The RIS assisted mobile and vehicular network are analysed and studied under various channel model as in [8] using fox H distribution and fisher snedecor fading [14]. Optimization and analysis of channel capacity is studied in [16] where RIS aided millimetre wave indoor communication without Line Of Sight (LOS). To assess capacity oriented metric for physical layer security, [2] derives an expression for secrecy capacity and secrecy outage probability for a Single Input Single Output (SISO) system under various fading channel scenarios. Also, Secrecy Capacity and SOP analysis of SISO system is analysed in [7] the presence of eavesdropper under Nagakami-m fading channel to send the confidential message between two legitimate vehicles. The performance of RIS assisted wireless powered interference link network is discussed in [13] under channel model ask fading distribution and Nagakami m fading and channel link between the access point and destination point are not in direct link.

Intuitively, in literature in existing system, none of the works studied the concept of Physical layer security of RIS enabled vehicular relay networks. In the proposed system it is a novel research paper, we describe the importance of security for realization of future autonomous RIS assisted vehicular relay networks for better connectivity under passive eavesdropping which is the justification. We consider that infrastructure node sends confidential information to a destination vehicle through RIS in an intelligent transport infrastructure. The RIS is engaged as relay or reflector. Eavesdropper is considered in the proposed system model. The closed form expression for secrecy capacity is derived and analysed for the proposed model. But in literature, the authors provided approximate secrecy capacity results.

Though all the research dealt above gives a good analysis of secrecy capacity analysis, this research paper considers different secrecy rates and different distances of eavesdropper which makes it a different research paper contribution for RIS based Vehicular Networks in comparison to other different model as given in the literature [2, 4, 7, 8, 10, 14, 16]. From a physical layer security perspective we consider a RIS based vehicular network system to transmit a confidential message from infrastructure node to destination vehicle through RIS in the presence of an eavesdropper. In addition we assume that the infrastructure node (T)-RIS channel link and RIS-destination vehicle channel link are Rayleigh fading channel and the infrastructure node (T)-eavesdropper channel link and RIS- eavesdropper channel link are double rayleigh fading channel. We derive the secrecy capacity and SOP for RIS based vehicular network under various secrecy rates and distances.

The rest of this paper is structured as track. Section 1 is introduction. In section 2 we have three sub sections, which illustrate our system model, secrecy capacity analysis for the proposed RIS based vehicular network and we derive a tight closed form expression of SOP for considered system in presence of a passive eavesdropper. The performance of SOP and Secrecy Capacity are discussed and validated with analytical results compared with simulation in section 3. Finally conclusion is presented in section 4.

Notations: We denote vectors, scalar, and matrices by boldface small, small letter and boldface capital letter. The transpose, complex conjugate, Hermitian, Norm of matrix and inverse of the matrix A are denoted by A^T, A^*, A^H, $\|h_{rk}\|$ and A^{-1}, respectively. $W_{a,b}(z)$ is Whittaker function. $K_v(x)$ is modified Bessel function.

2. RIS Based Vehicular Network System

2.1. System Model

The infrastructure node (T) sends confidential information to a destination Vehicle Equipment (VE) through RIS. The RIS is engaged as relay or reflector for this system in Figure 1. There is no direct link between The Infrastructure node (T) and destination VE. The channel link between T to RIS and RIS to destination VE are Rayleigh fading channel g_{tr} and h_{rd} respectively. In this RIS based system model, we assume a passive Eavesdropper where channel link is modelled as double rayleigh fading channel. Reconfigurable Intelligent Surface is defined as a structure a reflect exhibit integrate N reconfigurable reflector components, capable of being constrained by a correspondence situated programming for insightful transmission. y_{VE} and y_{VE} are received signals at destination VE and Eavesdropper EV respectively.

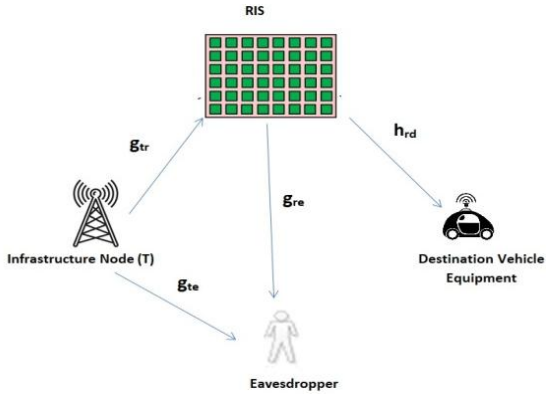

Figure 1. RIS based vehicular network.

$$y_{VE} = \left(\sum_{n=0}^{N} h_{rd,n} e^{-j\Phi_n}\right) x + \omega_{VE} \quad (1)$$

$$y_{EV} = \left(\sum_{n=0}^{N} g_{re,n} e^{-j\Phi_n}\right) x + \omega_{EV} \quad (2)$$

Where x represents transmitted signal by T with transmitting power Ps, ω_{EV}, ω_{EV} are Additive White Gaussian Noise (AWGN) at EV and VE, CN (0, N_0)

In our analysis, we assume perfect knowledge of channel phases of $h_{rv,n}$ and $g_{rt,n}$ for n=0, 1, 2, 3,….. N. Where Φ_n is phase induced by the n[th] reflecting surface of RIS.

$$h_{rv,n} = \alpha_n e^{-j\Phi_n} \text{ and } g_{rv,n} = \beta_n e^{-j\Phi_n}$$

In matrix form Equations (1) and (2) can be written as

$$r_{VE} = h^T \Phi g x + n_r \quad (3)$$

$$r_{EV} = g_{re}^T \Phi g_{te} x + n_e \quad (4)$$

Where $h=[h_1,h_2,,.....h_N]^T$,

$g=[g_1,g_2,,.....g_N]^T$ and $\Phi=e^{j\Phi}{}_1$, $e^{j\Phi 2}$,....., $e^{j\Phi}{}_N$ is a diagonal matrix that contains the phase shift applied by reflecting surface of RIS.

The received signal at EV from infrastructure node T

$$y_{TV} = g_{TE} x + \omega_{te} \quad (5)$$

SNR at VE and EV can be written from Equations (1) and (2)

$$\gamma_{VE} = \frac{\sum_{n=1}^{N} P_s |h_{RV,n}|^2}{N_0} \quad (6)$$

And

$$\gamma_{EV} = \frac{\sum_{n=1}^{N} P_s |g_{RE,n}|^2}{N_0} \quad (7)$$

2.2. Secrecy Capacity Analysis

The Capacity of destination VE is derived as

$$C_{VE} = \frac{1}{2}\log_2(1+\gamma_{VE}) \quad (8)$$

$$C_{VE} = \frac{1}{2}\log_2\left(1+\frac{\sum_{n=1}^{N} P_s |h_{RV,n}|^2}{N_0}\right) \quad (9)$$

From Equation (5), SNR of eavesdropper link between from T to EV is expressed as

$$\gamma_{EVT} = \frac{P_s |g_{TE}|^2}{N_0} \quad (10)$$

For the Eavesdropper, the transmission rate

$$C_{EV} = \frac{1}{2}\log_2(1+\gamma_{EVR}+\gamma_{EVT}) \quad (11)$$

$$C_{EV} = \frac{1}{2}\log_2\left(1+\frac{\sum_{n=1}^{N} P_s |g_{RE,n}|^2}{N_0}+\frac{P_s |g_{TE}|^2}{N_0}\right) \quad (12)$$

Therefore, the secrecy rate of VE is

$$R_{sec} = [C_{VE} - C_{EV}]^+ \quad (13)$$

Where, $(x)^+=\max(0,a)$, the maximum achievable secrecy capacity

$$C_s = \begin{cases} \log_2(1+\gamma_{VE}) - \log_2(1+\gamma_{EV}), & \gamma_{VE} > \gamma_{EV} \\ 0, & \gamma_{VE} < \gamma_{EV} \end{cases} \quad (14)$$

2.3. Secrecy Outage Probability (SOP) Analysis

For the considered system model SOP can be written as

$$\begin{aligned} P_{SOP} &= P_r\left[(C_{VE} - C_{EV}) < R_s\right] \\ &= P_r\left[\left(\frac{1}{2}\log_2(1+\gamma_{VE}) - \frac{1}{2}\log_2(1+\gamma_{EV})\right) < R_s\right] \\ &= P_r\left[\left(\log_2\frac{(1+\gamma_{VE})}{(1+\gamma_{EV})}\right) < 2R_s\right] \\ &= P_r\left[\left(\log_2\frac{(1+\gamma_{VE})}{(1+\gamma_{EV})}\right) < 2R_s\right] \end{aligned} \quad (15)$$

$$P_{SOP} = P_r\left[\left(\frac{(1+\gamma_{VE})}{(1+\gamma_{EV})}\right) < 2^{2R_s}\right] \quad (16)$$

Where, γ_{EV} is total SNR of eavesdropper and $\eta = 2^{2R_S}$

denoted as Secrecy SNR threshold.

SOP can be expressed as

$$P_{SOP} = P_r\left[\left((1+\gamma_{VE})\right) < \eta(1+\gamma_{EV})\right] \quad (17)$$

$$= P_r\left[\gamma_{VE} < \eta(1+\gamma_{EV})-1\right]$$

$$P_{SOP} = \int_0^{\infty} F_{\gamma_{VE}}\left(\eta(1+\gamma_{EV})-1\right) f_{\gamma_{EV}}(\gamma_{EV})\, d\gamma_{EV} \quad (18)$$

The CDF of vehicular equipment SNR γ_{VE} and

$$F_{\gamma_{VE}}(x) = 1-\exp(-\alpha_{VE}x) \quad (19)$$

The pdf of Eavesdropper SNR γ_{VE}

$$f_{\gamma_{EV}}(x) = \frac{2}{\Omega_{EV}^2}\kappa_0\left((2\alpha_{EV})\sqrt{x}\right) \quad (20)$$

Where the parameters α_{VE} and α_{VE} are written as

$$\alpha_{VE} = \frac{N_0}{P_s\Omega_{tr}} + \frac{N_0}{P_s\Omega_{rd}} \text{ and } \alpha_{EV} = \frac{N_0}{P_s\Omega_{re}} \quad (21)$$

Where Ω_{tr}, Ω_{re}, and Ω_{rd} are average channel gain of infrastructure node T to RIS channel link, RIS-EV channel link , and RIS-VE Channel link .

Substitute Equations (19) and (20) in Equation (18), we can written expression of SOP as

$$P_{SOP} = \int_0^{\infty} 1-e^{-\left(\alpha_{VE}\eta(1+\gamma_{EV})-1\right)} \frac{2}{\Omega_{EV}^2}\kappa_0\left((2\alpha_{EV})\sqrt{\gamma_{EV}}\right) d\gamma_{EV}$$

Further simplification above equation can be written as

$$P_{SOP} = 1-\frac{2e^{-\alpha_{VE}(\eta-1)}}{\Omega_{EV}^2}\int_0^{\infty} e^{-\alpha_{VE}\eta\gamma_{EV}}\kappa_0\left((2\alpha_{EV})\sqrt{\gamma_{EV}}\right) d\gamma_{EV} \quad (22)$$

Equation (22) required integral by using the transformation of variable and taking differential with respect to γ_{EV}. Let $y^2 = \gamma_{EV}$

$$2ydy = d\gamma_{EV}$$

And taking square root of y^2

$$y = \sqrt{\gamma_{EV}} \quad (23)$$

Let the parameters α and β are denoted as,

$$\alpha = \eta\alpha_{VE} \text{ and } \beta = 2\alpha_{EV} \quad (24)$$

Substitute Equations (23) and (24) in (22), the SOP can be written as

$$P_{SOP} = 1-\frac{2e^{-\alpha_{VE}(\eta-1)}}{\Omega_{EV}^2}\int_0^{\infty} e^{-\alpha y}\kappa_0(\beta y)dy \quad (25)$$

Using [7,. Equation 6.631.3] $\int_0^{\infty} y^{\mu}e^{-\alpha y}\kappa_{\nu}(\beta y)dy$

$$= \frac{1}{2}\alpha^{-\frac{1}{2}\mu}\beta^{-1}\Gamma\left(\frac{1+\mu+\nu}{2}\right)\Gamma\left(\frac{1+\mu-\nu}{2}\right)\exp\left(\frac{\beta^2}{8\alpha}\right)W_{\frac{1}{2}\mu,\frac{1}{2}\nu}\left(\frac{\beta^2}{4\alpha}\right) \quad (26)$$

Where $W_{a,b}(z)$ is Whittaker function.

The closed form expression of Secrecy Outage Probability for RIS based Vehicular network is

$$P_{SOP} = 1-\frac{2e^{-\alpha_{VE}(\eta-1)}}{\Omega_{EV}^2}\left\{\alpha^{-\frac{1}{2}}\beta^{-1}\exp\left(\frac{\beta^2}{8\alpha}\right)W_{\frac{1}{2}\mu,0}\left(\frac{\beta^2}{4\varepsilon}\right)\right. \quad (27)$$

Where, Ω_{EV} is average Eavesdropper link channel gain.

3. Results and Discussions

In this section, we validate and discuss the simulation result of secrecy capacity and secrecy outage probability for the proposed system model which is novel for RIS based vehicular network. We assume that the channel link between Infrastructure node (T) to RIS and RIS to Destination Vehicle Equipment (EV) are Rayleigh fading and Eavesdropper link is Double Rayleigh fading and path loss exponent parameter β_L=2.9 and the average channel gain is $\Omega_{i,j} = r_{i,j}^{-\beta_L}\lambda_{i,j}$. r_{ij} is denoted as the distance between the node i and j where $i \in T, RIS$ and $j \in VE, EV$ and $\lambda_{i,j}$ is mean values of average channel gain of respective nodes. For analytical discussion, we consider two dimensional plane, the coordinate points of RIS, Destination VE, EV are (0,0), (x_{RIS},0),(0,1) and (x_E,y_E) respectively. Accordingly the distance of the link $r_{T,RIS}$ = x_{RIS}, $r_{T,EV} = \sqrt{x_{EV}^2 + y_{EV}^2}$, $r_{RIS,EV}$=1-x_{RIS} and. $r_{RIS,EV} = \sqrt{(x_{RIS}-x_{EV})^2 + y_{EV}^2}$ and let the average channel gain of link T to RIS , RIS to VE and RIS to EV and T to EV are $\Omega_{T,RIS} = r_{T,RIS}^{-\beta_L}\lambda_{T,RIS} = x_{RIS}^{-\beta_L}\lambda_{T,RIS}$, $\Omega_{T,RIS} = (1-x_{RIS})^{-\beta_L}\lambda_{T,RIS}$ $\Omega_{T,EV} = \left(\sqrt{x_{EV}^2 + y_{EV}^2}\right)^{-\beta_L}\lambda_{T,EV}$ and $\Omega_{RIS,EV} = \left(\sqrt{(x_{RIS}-x_{EV})^2 + y_{EV}^2}\right)^{-\beta_L}\lambda_{RIS,EV}$ and we define the $\lambda_2 = \frac{\lambda_{RIS,VE}}{\lambda_{RIS,EV}}$ and $\lambda_1 = \frac{1}{\lambda_{T,EV}}$ as for Main To Eavesdropper Ratio (MER) RIS links.

In Figure 2 We plot the average secrecy capacity Vs source transmitted power. We assume that distance between RIS to Destination VE rVE=5m, Infrastructure node (T) to RIS distance rtr=10m, path loss exponent parameter β=2.9 and Infrastructure node (T) to eavesdropper distance rte=12m and number of RIS element is 32 the 12m and 16m distance of RIS to EV link. It is observed that the secrecy capacity increases by increasing the values of transmit powers.

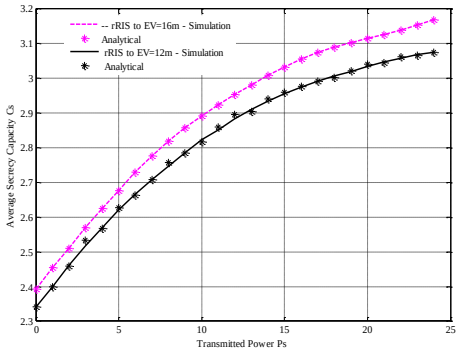

Figure 2. Average secrecy capacity VS transmitted power.

Figure 3 shows SOP versus transmitted power with various Secrecy Rate (Rs).

The performance of SOP is analysed with various Secrecy rate Rs. Secrecy rate Rs=0.2 bps/Hz and Rs=0.5 bps/Hz and various RIS to EV link distance by set y_{EV}=0.5 and y_{EV}=1.

We set x_{RIS}=0.5, x_{EV}=0.5, x_{RIS}=0.5. $\lambda_{T,RIS}=\lambda_{RIS,\ VE}=1$. For better performance of SOP likely for the higher value of Rs, more power is needed to support higher secrecy rate.

In Figure 4 the performance of SOP in different location of eavesdropper from RIS for various λ_1 and λ_2. The performance of Secrecy Outage Probability is analysed with Secrecy rate Rs=0.5 bps/Hz and transmitted power Ps=5dB

$$y_{EV}=0.2 \text{ to } y_{EV}=2 \cdot \text{ We set } x_{RIS}=0.5,\ x_{EV}=0.5 \cdot$$

Moreover in Figure 4 shows SOP performance increases when EV moves away from RIS because of links wiretap linkdegrade. From Figure 4 also it can be observed that SOP performance increases when λ_1 or λ_2 increases. For instance, when y_{EV}=0.6 the SOP performance is portrayed in Table 1. Various λ_1 and λ_2. Further, the SOP performance can be significantly improved if λ_1 and λ_2 increased jointly.

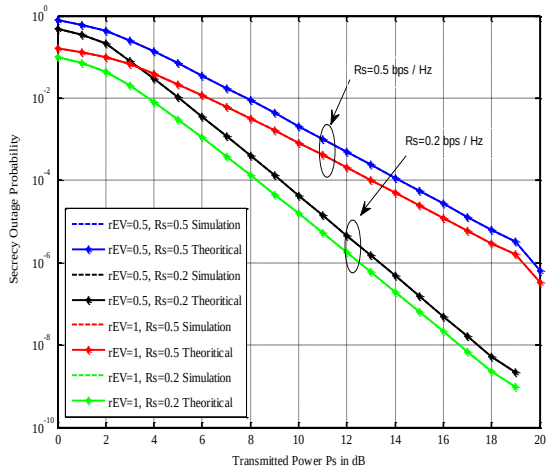

Figure 3. SOP Vs transmitted power Ps.

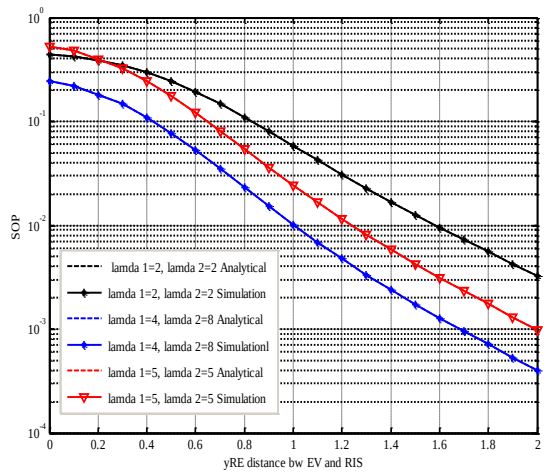

Figure 4. Secrecy outage probability Vs different position of eavesdropper from RIS.

Table 1. SOP performance various λ_1 and λ_2 from Figure 4.

S.No	λ_1	λ_2	SOP when y_{EV}=0.6
1	2 dB	2 dB	0.194
2	4 dB	8 dB	0.121
3	5 dB	5 dB	0.05267

4. Conclusions

This research paper derives closed form expressions of secrecy capacity and secrecy outage probability for RIS based vehicular communication networks over Rayleigh fading in the presence of a passive eavesdropper. It is observed that the theoretical and simulation results aid each other and are thus validated to show the outcome of the results presented for RIS vehicular networks. The results obtained can provide significant outcome for developing applications for 5G wireless and further for the road to 6G systems for developing new wireless applications as the future scope. Further as future work simultaneous information and power transfer enabled Physical Layer security in RIS based Vehicular relay networks can also be proposed for energy harvesting where vehicles charge their battery power by means of RF Signals through energy harvesting applications.

References

[1] Alghorani Y., Kaddoum G., Muhaidat S., Pierre S., and Al-Dhahir N., "On the Performance of Multihop-Intervehicular Communications Systems Over n∗ Rayleigh Fading Channels," *IEEE Wireless Communication Letters*, vol. 5, no. 2, pp. 116-119, 2016.

[2] Al-Hmood H. and Al-Raweshidy H., "Performance Analysis of Physical Layer Security over Fluctuating Beckmann Fading Channels," *IEEE Access*, vol. 7, pp. 119541-119556, 2019.

[3] Basar E., Di Renzo M., De Rosny J., Debbah M., Alouini M., and Zhang R., "Wireless Communications through Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 7, pp. 116753-116773, 2019.

[4] Chen J., Liang Y., Pei Y., and Guo H., "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security," *IEEE Access*, vol. 7, pp. 82599-82612, 2019.

[5] Dheepan K., "Security Enhancement and Certificate Revocation in MANET Using Position and Energy Based Monitoring," *The International Arab Journal of Information Technology*, vol. 16, no. 1, pp. 88-97, 2019.

[6] Elmossallamy M., Zhang H., Song L., Seddik K., Han Z., and Li G., "Reconfigurable Intelligent Surfaces for Wireless Communications: Principles, Challenges, and Opportunities," *IEEE Transactions on Cognitive Communications and*

Networking, vol. 6, no. 3, pp. 990-1002, 2020.
[7] Jerrey A. and Zwillinger D., *Table of Integrals, Series, and Products, Seventh Edition*, Elsevier, 2007.
[8] Karas D., Boulogeorgos A., and Karagiannidis G., "Physical Layer Security with Uncertainty on the Location of the Eavesdropper," *I IEEE Wireless Communications Letters*, vol. 5, no. 5, pp. 540-543, 2016.
[9] Kobayashi M and Debbah M., "On The Secrecy Capacity of Frequency-Selective Fading Channels : A practical vandermonde precoding," *in Proceedings of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, Cannes, pp. 1-5, 2008.
[10] Kong L., He J., Ai Y., Chatzinotas S., and Ottersten B., "Channel Modeling and Analysis of Reconfigurable Intelligent Surfaces Assisted Vehicular Networks," *in Proceedings of IEEE International Conference on Communications Workshops*, Montreal, pp. 1-6, 2021.
[11] Makarfi A., Rabie K., Kaiwartya O., Adhikari K., Li X., Quiroz-Castellanos M., and Kharel P., "Reconfigurable Intelligent Surfaces-Enabled Vehicular Networks: A Physical Layer Security Perspective," *arXiv preprint arXiv:2004.11288* 2020.
[12] Nessa A., Yang Q., and Kwak K., "Performance Analysis of Two-Hop Cooperative MIMO Transmission with Best Relay Selection in Rayleigh Fading Channel," *The International Arab Journal of Information Technology*, vol. 8, no. 1, pp. 9-15, 2011.
[13] Odeyemi K., Owolawi P., and Olakanmi O., "Reconfigurable Intelligent Surface in Wireless-Powered Interference Limited Communication Networks," *Symmetry*, vol. 13, no. 6, pp. 960, 2021.
[14] Odeyemi K., Owolawi P., and Olakanmi O., "Reconfigurable Intelligent Surface Assisted Mobile Network with Randomly Moving User over Fisher-Snedecor Fading Channel," *Physical Communication*, vol. 43, pp. 101186, 2020,
[15] Pandey A. and Yadav S., "Physical Layer Security in Cooperative AF Relaying Networks With Direct Links Over Mixed Rayleigh and Double-Rayleigh Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10615-10630, 2018.
[16] Perovic N., Renzo M., and Flanagan M., "Channel Capacity Optimization Using Reconfigurable Intelligent Surfaces in Indoor mmWave Environments," *in Proceedings of IEEE International Conference on Communications*, Dublin, pp. 1-7, 2020.
[17] Renzo M., Ntontin K., Song J., Danufane S., Qian X., Lazarakis F., Rosny J., Phan-Huy D., Simeone O., Zhang R., Debbah M., Lerosey G., Fink M., Tretyakov S., and Shamai S., "Reconfigurable Intelligent Surfaces Vs. Relaying: Differences, Similarities, and Performance Comparison," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 798-807, 2020.
[18] Saad W., Bennis M., and Chen M., "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134-142, 2020.
[19] Yang L., Chen J., Jiang H., Vorobyov S., and Zhang H., "Optimal Relay Selection for Secure Cooperative Communications with an Adaptive Eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 26-42, 2017.
[20] Yang N., Wang L., Geraci G., Elkashlan M., Yuan J., and Di Renzo M., "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20-27, 2015.
[21] Yuan X., Zhang Y., Shi Y., Yan W., and Liu H., "Reconfigurable-Intelligent-Surface Empowered 6G Wireless Communications: Challenges and Opportunities," *arXiv*, pp. 1-7, 2020.
[22] Zhao J., "A Survey of Intelligent Reflecting Surfaces (IRSs): Towards 6G Wireless Communication Networks with Massive MIMO 2.0," *arXiv*, pp. 1-7, 2019.

Ashokraj Murugesan received the ME degree in Communication System from the Anna University, Tirunelveli, India. He works as an Assistant Professor at the Oxford Engineering College, Department of Electronics and Communication Trichy, Tamil Nadu, India. His current research interest includes the Signal Processing, Vehicular Relay Network, Adhoc network and Mobile network.

Ananthi Govindasamay received the PhD Degree from Anna University, Chennai, India. She is working an Assistant Professor with a Department of Electronics and Communication Engineering, Thiagarajar College of Engineering, Madurai, India. Research interests include in physical layer aspects of wireless communication systems, Deep learning algorithms and Vehicular Networks. She is a reviewer in IET Communications, IET Signal Processing, IET Networks, IET Science, Measurements and Technology, IET Microwaves, Antennas and Propagation, Springer Wireless Personal Communications.