Journal of Intelligent Communication (2022) Volume 2 Issue 2, *7 pages*.
doi: 10.54963/jic.v2i2.125

ORIGINAL RESEARCH ARTICLE

Improved Rate of Intelligent Surfaces for Vehicular Networks

Zhening Liu [1,2,3*], Hongxing Sun [1,2], Qiang Liu [1]

*[*1] University of Bahrain, Zallaq 32038, Bahrain*

[2] Hankuk University of Foreign Studies, Yongin-si 17035, Republic of Korea

[3] Inha University, Incheon 22212, Republic of Korea. Email: ZnL@bzu.edu

ABSTRACT

An intelligent reflecting surface (IRS) is an array that consists of a large number of passive reflecting elements. Such a device possesses the potential to extend the coverage of transmission in future communication networks by overcoming the effects of non line-of-sight propagation. Accordingly, to present the case for utilizing IRS panels in future wireless networks, in this paper, we analyze a multi-user downlink network aided by IRS. In particular, by using a realistic 5G channel model, we compare the performance of the IRS-aided network with a decode and forward (DF) relay-aided scenario and a network without IRS or relay. Our analysis revealed the following: (i) At best, communication aided by a DF relay with perfect channel state information (CSI) could match the performance of the IRS-aided network with imperfect CSI when the channel estimation error was high and the number of users was large. (ii) IRS-aided communication outright outperformed the DF relay case when the transmit power was high or the number of users in the network was low. (iii) Increasing the number of elements in an IRS translated to greater quality of service for the users. (iv) IRS-aided communication showed better energy efficiency compared with the other two scenarios for higher quality of service requirements.

Keywords: intelligent reflecting surface; multi-users communications; energy-efficiency; power-minimization

1. Introduction

With the increasing number of vehicles equipped with computing technologies and wireless communication devices, vehicular communication is developing into a potential area for standardization, development, and research. Numerous applications are made possible by vehicle-to-vehicle (V2V) communications, including security, real-time traffic condition, blind crossing prevention, safety, dynamic route planning, and collision prevention[1]. Vehicular communications can be utilized for a wide variety of secure and non-secure applications, enabling value-added services like automated toll collection, vehicle well-being, improved route selection, area-based services like finding the nearest convenience store,

ARTICLE INFO

Received: July 7, 2021 | Accepted: July 17, 2022 | Available online: October 27, 2022

CITATION

Zhening Liu, Hongxing Sun, et al. Improved Rate of Intelligent Surfaces for Vehicular Networks, Journal of Intelligent Communication, 2022; 2(2): 1–7 pages.

restaurant, or travel destination, as well as a wide range of entertainment applications[2]. In the last decade, a wide range of applications have been developed to address different issues and problems that have surfaced as a result of smart automobiles[3–5]. With the introduction of new applications and the broadening of the domain, there arises security threats as well. The security threats in vehicular communications can be broadly categorized as confidentiality, non-repudiation, data integrity and availabilit. Different approaches have been highlighted to mitigate different types of security threats that arise in vehicular communication.

The traditional techniques of data encryption are not feasible for a dynamic environment where the receiver as well as the source both are in motion. Although these methods tend to provide the necessary security but are unable to meet the demands of a dynamic environmen. In addition, the traditional approaches tend to require a sophisticated end-system with the capability to decrypt the received message. Both the sender and the receiver are in need of considerable computational power to perform these sophisticated encryption-decryption techniques. The vehicular system tends to be a lot simpler with limited computational power. Thus, making the traditional approach to be much less undesirable, especially in terms of computational power and processing time[6–9].

Physical layer security (PLS), on the other hand, is introduced to mitigate the drawbacks associated with traditional security techniques. The PLS considers the random behavior and reciprocity of the channel to provide security. It does not require the need for either complex encryption or the computational ability of the transceivers. Nevertheless, security at the physical layer (PL) is largely provided by using either a key-less or a key-based approach. The key-less based PLS is better as it does not require any additional cost of computation at the receiver. However, we need to be aware of the exact location of the devices for information to be disseminated without any security concerns. Besides, it also requires perfect channel state information (CSI) to be effective. In the case of a key-based PLS technique, a secret key is generated to be exchanged between the source and the receiver before the actual information is sent.

Recently, reflecting intelligent surfaces (RIS) are playing an important role in the next generation of wireless communication. The RIS has passive reflecting elements (RE) that can scatter the incident signal in a particular direction in such a way as to increase the signal strength in one direction while lessening it in the other direction. The individual elements can be controlled by adjusting the phase shift angle using phase. In, the RIS is used in symbiotic radio (SR) for introducing channel diversity for secret key generation. The authors propose a heuristic, as well as a deep reinforcement learning-based, approach to controlling the switching of the RIS-assisted phase shift matrices.

The PL secrete key generation (SKG) is a reasonable alternative for accomplishing one-time-pad encryption in wireless communication systems. Nevertheless, due to the obvious lack of channel time-variation in a static environment, the secret key rate is low. The SKG scheme assisted by a reconfigurable intelligent surface (RIS) with discrete phase shifts can be used to overcome this limitation. In this method, the phases of the RIS are rapidly and randomly adjusted by the legitimate nodes to construct the dynamic time-varying channel. The channel coefficients generated as a result are used for the SKG. Furthermore, by modifying the RIS phase switching time, the secret key rate can be optimized.

The RIS, unlike the traditional relay base station (BS), has the dual capability, i.e., it acts as a signal booster as well as a signal diminisher. It has the capability to redirect the signal by adjustment of the RE called meta-surface element. This can be done by phase adjustment as well as the angle of incidence of the signal at the transmitter. These features allow a RIS to concentrate the signal in one direction while completely blocking the signal in the nearby vicinity. Thus, even if the eavesdropper is near the legit vehicle, the signal-diminishing property of the RIS will not allow the eavesdropper to receive the signal. The

vehicular environment is dynamic as well as time-constrained due to the mobile nature of the vehicle. The RIS is a potential candidate for exchanging secure information, without delays due to computation. The signal diminishing features minimizes the leakage of information to a potentially malicious user.

2. Related Work

The concept of key generation and KGR in vehicular ad-hoc networks (VANETs) based scenario, using PLS techniques has not been exploited. The security techniques are mostly based on the public key encryption mechanism or for a key-less based PLS. Most of the existing literature is focused on KGR for a static environment.

Secure communication in VANETs is mostly done by using public key encryption for authenticity and security. The authors in have highlighted the main factors that are a threat during the authentication process. They have proposed various methodologies in this regard to ensure authentication such as trusted parties and authentication of roadside units (RSUs), using cooperative key exchanges in VANETs.

The authors of have focused on the quantization of the secret key generation process, by reviewing the existing schemes in the public domain and associated performance metrics i.e., randomness and entropy of keys. Their preliminary findings show that received signal strength (RSS)-based algorithms do not perform efficiently for the proposed vehicular stochastic wireless model. Hence, they are not able to satisfy the typical low latency required in safety-related broadcasting messaging, resulting in a higher key mismatch.

The authors of have worked on a multi-layer cluster-wise key generation for securing communication for a highly dense VANET-based environment. They have divided the entire VANETs into clusters, where they have considered that every cluster will have its own separate RSU for key generation and distribution. The concept of public key encryption is used at the RSU to generate keys.

The authors of have proposed a batch authentication scheme to provide high-level security by evading communication with the eavesdropper vehicle. Along with this, the batch authentication scheme is also used at roadside units (RSUs) to lessen the authentication burden while performing the authentication process in congested areas, by producing a batch of keys at each RSU. The key exchange process is kept anonymous. The concept of public key encryption is used for generating the keys at the RSUs after the registration process. The authors have not taken into consideration the fact that an RSU can be used as a malicious RSU.

Authors have provided a discrete phase shift SKG approach. To introduce channel randomness of the wireless channel in a static environment and produce secret keys, the authors propose a higher SKR than that of SKG schemes based on the artificial random signal.

The problem of key generation in the IRS-assisted multiple-input single-output (MISO) system is addressed. The authors investigated the correlation between the CSI of eavesdroppers and legitimate users. After analysis, the expression of the upper bound of the secret key rate under a passive eavesdropping attack was derived.

The authors of also proposed a wireless key generation architecture using a RIS, which is based on randomized channel responses for a static environment, using a single sub-carrier, the IRS-assisted prototype system achieves a KGR of 97.39 bps with a 6.5% key disagreement rate (KDR) after quantization. The authors of have investigated secure communication in IRS-assisted networks having multiple passive eavesdroppers. The one-time password (OTP) secret keys were provided using random phase shifting of a RIS in an encrypted data transmission methodology. The KGR was calculated assuming that all eavesdroppers were located near the sender. In addition, they have proposed an optimal time slot allocation algorithm to maximize the rate of secure communication.

The authors of proposed an IRS-assisted key

generation methodology, against multiple correlated eavesdroppers. The system's secret key capacity is maximized by optimizing an IRS's reflection coefficient matrix. They devised and solved an optimization problem to find the best IRS configuration using semi-definite relaxation (SDR) and the convex-concave procedure (CCP). They concluded that the same secret key capacity can be obtained by reducing the number of transmitting antennas while increasing the number of IRS elements, resulting in lower antenna hardware costs. The numerical outcomes are compared to MRT and IRS with random phase shifts.

3. Our Contributions

From the literature, it can be observed that most of the existing research is considered a static environment, where the channel is mostly static. This characteristic limits the key generation rate. This is not the case for vehicular communications, where the mobility factor tends to change the distance constantly. Although mobility introduces diversity in the reciprocity of a channel, moving devices can almost share the same CSI. None of the existing literature has addressed the problem of a dynamic environment where there are multiple mobile eavesdroppers. To the best of our knowledge, the concept of using a set of RIS elements in directing the information signal has not been considered, especially for a dynamic environment for increasing the key generation rate. The main contributions of our research are summarized as follows.

- We introduced diversity in the SKGR, by taking a set of consecutive reflecting elements (RE) of a passive-RIS into consideration as a subset. These subsets constantly change with each successive communication introducing variations in the possible number of keys that can be generated for a VANET-based environment.

- A mobile environment for communicating vehicles is considered in the presence of multiple eavesdroppers.

- The proposed methodology is based on four different types of subsets. The first considered subset consists of 3 RE, then the second includes 4 RE, the third one incorporates 5 RE, and, finally, the last one comprises a random subset of REs.

- In the proposed method, DPS is executed for a dynamic scenario, as the system model is developed for VANETs that consist of moving vehicles. In the DPS methodology, all phases of the RE of an RIS are adjusted. In the proposed methodology, consecutive RE subsets of the RIS are partitioned into different subsets, for redirecting the information signal. (The proposed scheme is in contrast to the DPS of a static environment for KGR).

- An implementation of discrete phase shift methodology of a static environment is simulated for a vehicular environment for comparing it with the proposed methodology.

The rest of the paper is organized as follows. The next section represents the overall system model developed for the above-laid-out scenario, followed by the theoretical analysis. Finally, based on the theoretical analysis, simulations are conducted in the simulation section. The last section concludes the paper.

4. System Model

The basic steps involved in SKG using which the source and destination can secure their information are, channel probing (CP), Quantization scheme (QS), verification of Keys exchanged, and key exchange process.

- **Channel Probing:** In this step, the characteristics of a channel are gathered by the legitimate communicating vehicles. For our model, we are considering the received signal strength (RSI) as channel characteristics. Training signals are exchanged in this step to establish the channel conditions between the communicating vehicles based on

the received signals. The training symbols are exchanged as probing signals for a duration of Δt. The receiving vehicle instantly replies upon receiving the training signal. Since we are considering a dynamic environment, i.e., where the vehicles are in motion, Δt is kept very small, i.e., 1 s.

- **Quantization Scheme:** In this step, the communicating vehicles adopt the same quantization scheme. This is done to quantify the channel for obtaining the initial keys. The measured channel characteristics are quantized into bits.

- **Verification of Keys Exchanged:** In this step, the verification of the exchanged keys is done, as the communication is taking place in a wireless environment where factors, such as interference, may result in errors or bit inconsistency during the initial key exchange process. It is a form of error correction between the communicating vehicles to ensure that the generated keys are identical.

- **Key Exchange:** During this step, the keys are exchanged between the communicating vehicles. There are chances that the eavesdropper might be able to tap into the communication process, for which a universal hashing scheme can be utilized to minimize the chances of eavesdropping.

The basic concept of channel reciprocity for secret key generation is exploited for the key generation at the physical layer. We have assumed multiple eavesdroppers in the transmission range of the destination. Thus, as the vehicles are in motion for a specific time interval Δt, the signal values and channel conditions for the communicating vehicles remain unchanged for a single slot. The eavesdroppers in the vicinity of the receiving vehicles have full access to the channel and can intercept any kind of signal within receiving range. We have introduced the RIS as a passive relay for channel diversity and to generate different codes in the same time interval. For diversification in channel randomness, we exploit the different sets of meta-surface elements of the RIS. Thus, the signals that are incident on the different sets of meta-surfaces have different transmission paths and phase shifts due to the angle of incidence from the source.

The generic properties of the RIS state that if the signal is boosted in one direction, then it can diminish the signal in the opposite direction such that it will be received as a noise signal at the eavesdropper. Exploiting this nature of the RIS, even if the eavesdropper is aware of a key agreement taking place between the source and the legitimate receiver, it cannot acquire information about the actual keys being shared. The introduction of RIS further introduces randomness in the channel, making it more difficult to intercept the messages, communicated between the concerned parties. We consider time division duplex (TDD) as a mode of communication and ergodic block fading model to keep the channel gains constant for the duration of a slot.

We consider a vehicular-based scenario where there is a V2V-based communication. The model consists of multiple passive eavesdroppers, as depicted in **Figure 1**. Here, the RIS is considered as a passive relay denoted by *R*. The destination is represented by *D* and the eavesdropper is represented by *E*.

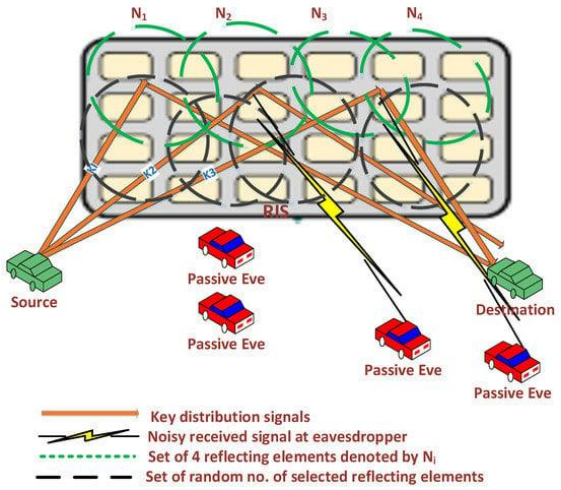

Figure 1. System model for an increase in secrete key generation using RIS as a passive relay.

Figure 2 represents a set of 4 reflectors among 16 for an RIS. The angular distance between the source and destination is kept different, i.e., a random value between 1–16 m, and the angle of incidence is also taken as a random value between 0–2π. The noise values here are kept minimum to see the effects on KGR for a constantly varying distance. It can be observed from **Figure 2**, the KGR constantly changes due to the fluctuation in distance between the source and destination. With a minimum noise value, the rate of key generation increases up to 2.5 bps, while at the lower distances, the KGR is minimum to 1.15 bps for a worst-case scenario. This is due to a number of factors. One of the major factors that result in an increase is the distance between the legitimate vehicle and the eavesdropper vehicle, i.e., the distance of the eavesdroppers both from the source and the destination. The larger the distance, the better the KGR. Similar to the distance are the noise values at the eavesdropper, which also improves the KGR at the legitimate vehicles. As the model incorporates an RIS, thus, the phase shift also plays a major role in increasing the KGR. The number of REs that are covered during the phase shift also has a significant effect on the KGR.

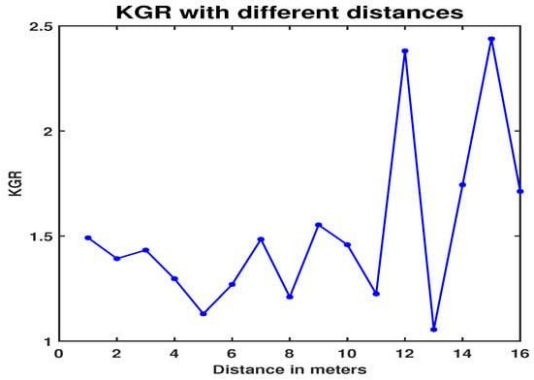

Figure 2. Considering a set of 4 reflectors per group, varying the distance between source and destination, while keeping noise constant.

Conflict of interest

The authors declare no conflict of interest.

Funding

No Fundings.

References

1. Brooks, R.R.; Yun, S.B.; Deng, J. Cyber-Physical Security of Automotive Information Technology; Morgan Kaufmann: Boston, MA, USA, 2012; pp. 655–676.
2. Han, B.; Peng, S.; Wu, C.; Wang, X.; Wang, B. LoRa-based physical layer key generation for secure V2V/V2I communications. Sensors 2020, 20, 682.
3. Pereira, J.; Ricardo, L.; Luís, M.; Senna, C.; Sargento, S. Assessing the reliability of fog computing for smart mobility applications in VANETs. Future Gener. Comput. Syst. 2019, 94, 317–332.
4. Arif, M.; Wang, G.; Bhuiyan, M.Z.A.; Wang, T.; Chen, J. A survey on security attacks in VANETs: Communication, applications and challenges. Veh. Commun. 2019, 19, 100179.
5. Tanwar, S.; Vora, J.; Tyagi, S.; Kumar, N.; Obaidat, M.S. A systematic review on security issues in vehicular ad hoc network. Secur. Priv. 2018, 1, e39.
6. Pepper, R. Cisco Visual Networking Index (VNI) Global Mobile Data Traffic Forecast Update. Technical Report, Cisco, February 2013. Available

online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 19 December 2022).

7. Waqas, M.; Ahmed, M.; Li, Y.; Jin, D.; Chen, S. Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays. IEEE Trans. Wirel. Commun. 2018, 17, 3918–3930.
8. Renault, É.; Mühlethaler, P.; Boumerdassi, S. Communication security in vanets based on the physical unclonable function. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
9. Ali, I.; Hassan, A.; Li, F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. Veh. Commun. 2019, 16, 45–61.