1-1-2023

Improved rate of secret key generation using passive re-configurable intelligent surfaces for vehicular networks

Hina Ayaz

Muhammad Waqas
Edith Cowan University, m.waqas@ecu.edu.au

Ghulam Abbas

Ziaul Haq Abbas

Muhammad Bilal

See next page for additional authors

10.3390/su15010342
Ayaz, H., Waqas, M., Abbas, G., Abbas, Z. H., Bilal, M., & Kwak, K. S. (2023). Improved rate of secret key generation using passive re-configurable intelligent surfaces for vehicular networks. Sustainability, 15(1), Article 342.
https://doi.org/10.3390/su15010342

sustainability

MDPI

Article

Improved Rate of Secret Key Generation Using Passive Re-Configurable Intelligent Surfaces for Vehicular Networks

Hina Ayaz [1], Muhammad Waqas [2,3], Ghulam Abbas [1,4], Ziaul Haq Abbas [4,5], Muhammad Bilal [6,*] and Kyung-Sup Kwak [7,*]

[1] Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Topi, Swabi 23640, KP, Pakistan
[2] Computer Engineering Department, College of Information Technology, University of Bahrain, Zallaq 32038, Bahrain
[3] School of Engineering, Edith Cowan University, Perth, WA 6027, Australia
[4] Telecommunications and Networking Research Center, GIK Institute of Engineering Sciences and Technology, Topi, Swabi 23640, KP, Pakistan
[5] Faculty of Electrical Engineering, GIK Institute of Engineering Sciences and Technology, Topi, Swabi 23640, KP, Pakistan
[6] Department of Computer Engineering, Hankuk University of Foreign Studies, Yongin-si 17035, Republic of Korea
[7] Department of Information and Communications Engineering, Inha University, Incheon 22212, Republic of Korea
* Correspondence: m.bilal@ieee.org (M.B.); kskwak@inha.ac.kr (K.-S.K.)

Abstract: The reconfigurable intelligent surfaces (RIS) is a new technology that can be utilized to provide security to vehicle-to-vehicle (V2V) communications at the physical layer. In this paper, we achieve a higher key generation rate for V2V communications at lower cost and computational complexity. We investigate the use of a passive RIS as a relay, to introduce channel diversity and increase the key generation rate (KGR), accordingly. In this regard, we consider the subsets of consecutive reflecting elements instead of the RIS as a whole in a time slot, i.e., instead of a single reflector, the subsets of reflectors are utilized to redirect the signal to the receiver via passive beam forming. Simulations are conducted for different sizes of RISs and subsets of reflectors per RIS. From the results obtained, it can be seen that when we consider a subset of reflectors instead of the RIS as a single entity, it becomes increasingly difficult to intercept the signal at the eavesdropper. In the proposed scheme, the KGR reaches up to 6 bps per time slot.

Keywords: Re-configurable intelligent surfaces; reflecting elements; vehicle-to-vehicle communications; physical layer security; eavesdropper; secret key generation rate; performance gain

check for updates

Citation: Ayaz, H.; Waqas, M.; Abbas, G.; Abbas, Z.H.; Bilal, M.; Kwak, K.-S. Improved Rate of Secret Key Generation Using Passive Re-Configurable Intelligent Surfaces for Vehicular Networks. *Sustainability* **2023**, *15*, 342. https://doi.org/10.3390/su15010342

Academic Editors: Cheng-Chi Lee, Dinh-Thuan Do and Agbotiname Lucky Imoize

Received: 23 October 2022
Revised: 18 December 2022
Accepted: 20 December 2022
Published: 26 December 2022

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, 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 [3,4]. 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 availability [5]. 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 environment [6,7]. 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 [8,9].

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 [10]. Nevertheless, security at the physical layer (PL) is largely provided by using either a key-less or a key-based approach [7,11]. 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 [12]. 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 [7,13].

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 [12]. The individual elements can be controlled by adjusting the phase shift angle using phase [11,14]. In [15], 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 [10,16]. It has the capability to redirect the signal by adjustment of the RE called meta-surface elements [12]. 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 [12,17]. 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].

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 [18] 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 [19] 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 [20] 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 [21] 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.

In [22], the 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.

In [23], channel key extraction in a static multi-user down link scenario is considered. It is observed that due to the high channel similarity between users, the problem of low-key generation arises. To address this, they have proposed a joint user allocation and RIS reflection parameter adjustment scheme. The authors of [24] exploited the random nature of a wireless channel's secret key generation. An RIS is used to induce randomness in a static wireless environment for key generation.

The authors of [25] have investigated the IRS-assisted SKG method, which tries to generate as many secret keys as possible by modifying the placement of the RIS reflecting elements. They investigated the position of the IRS elements by using the CSI to increase the secret key generation rate.

In [26], 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 [27] 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 [28] 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 [29] 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. To summarize our findings, Table 1 presents a comparison of the proposed scheme with the algorithms and schemes employed to increase the key generation rate.

Table 1. Comparison of the proposed scheme with the state of the art.

Year	Ref.	Proposed Methodology	RIS/ Traditional Relay	KGR	Static/ Dynamic Env.	VANET Based
2022	[29]	IRS assisted optimal time allocation	Active RIS	1.6 bps	static	×
2021	[15]	Heuristic-based scheme along with DRL	Active RIS	5 bps	Static	×
2021	[20]	multi-layer cluster-wise key generation for ultra dense VANETs	None	single key	dynamic	✓
2021	[21]	Batch-authentication scheme using Public key encryption at trusted RSU	None	single key	dynamic	✓
2021	[22]	Discrete phase shift SKG approach	RIS	10^2 bps	static	×
2021	[23]	Joint user Channel allocation and adjustment of RIS reflection parameters	RIS	12 bps	static	×
2021	[24]	Use of continuous individual phase shift	RIS	16 bps	static	×
2021	[25]	Modification in the placement of RIS reflecting elements and position adjustment	RIS	14 bps	static	×
2021	[28]	Randomized channel response of cooperative RIS on OFDMA	RIS	8^3 bps	static	×
2020	[13]	Induced randomness for a static environment at transceivers. Code hashing with QAM	Passive RIS	150 keys	Static	×
2018	[7]	Coalition formation algorithm for selection of optimal relay pairs, based on social ties, for key agreement.	traditional relay	6 bps	dynamic	×
2018	[19]	Quantization Scheme for key generation using Public key encryption	None	single key	dynamic	✓
2022	Our scheme	Use of set of RIS elements to increase the key generation rate	Passive RIS	up to 6 bps	dynamic	✓

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 [22] 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 [30]. 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 [30]. 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 [31]. 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 [32] 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 [7].

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.

The received signal strength is represented by $Y_j^{\Delta t}$, where $j = \{S, D\}$. It is assumed that during the interval Δt, the location of the legitimate vehicles is known. Based on this, we can target the specific reflecting elements of the RIS to introduce randomness in the signal. Initially, the source and destination exchange training symbols x determine the CSI conditions and location of the communicating vehicles, to establish the key exchange process. Thus, the received signals at the source and the destination vehicles, at a time interval Δt, are given as

$$Y_S^{\Delta t} = (h_{DS} + h_{DRS})x + w_S^{\Delta t}, \tag{1}$$

where h_{DS} is the channel coefficient from destination to source vehicle, and h_{DRS} is the channel coefficient from D-to-E via the RIS R. Expanding h_{DRS}, we obtain

$$Y_S^{\Delta t} = (h_{DS} + \sum_{j=m}^{N_j} h_{DRS}^i e^{-k\theta_n})x + w_S^{\Delta t}. \tag{2}$$

Here, m is the start of the combination of a set of reflectors chosen at Δt. Now, the received signal at the destination is given by

$$Y_D^{\Delta t} = (h_{SD} + h_{SRD})x + w_D^{\Delta t}, \tag{3}$$

where h_{SD} is the channel coefficient from S-to-D vehicle, and h_{SRD} is the channel coefficient from S to E via the RIS R. Similarly, after expanding h_{SRD}, we obtain

$$Y_D^{\Delta t} = (h_{SD} + \sum_{j=m}^{N_j} h_{SRD}^i e^{-k\theta_n})x + w_D^{\Delta t}, \tag{4}$$

where x is the message being exchanged between the legitimate vehicles, w_D and w_S are the noise values received at D and S vehicles respectively, and both these noise values should also satisfy $w_S \sim CN(0, \delta_D^2)$ and $w_S \sim CN(0, \delta_D^2)$, respectively. $e^{-k\theta_n}$ is the coefficient of the RIS where k is the constant and θ_n is the angle at which the signal is reflected from the reflecting elements of an RIS.

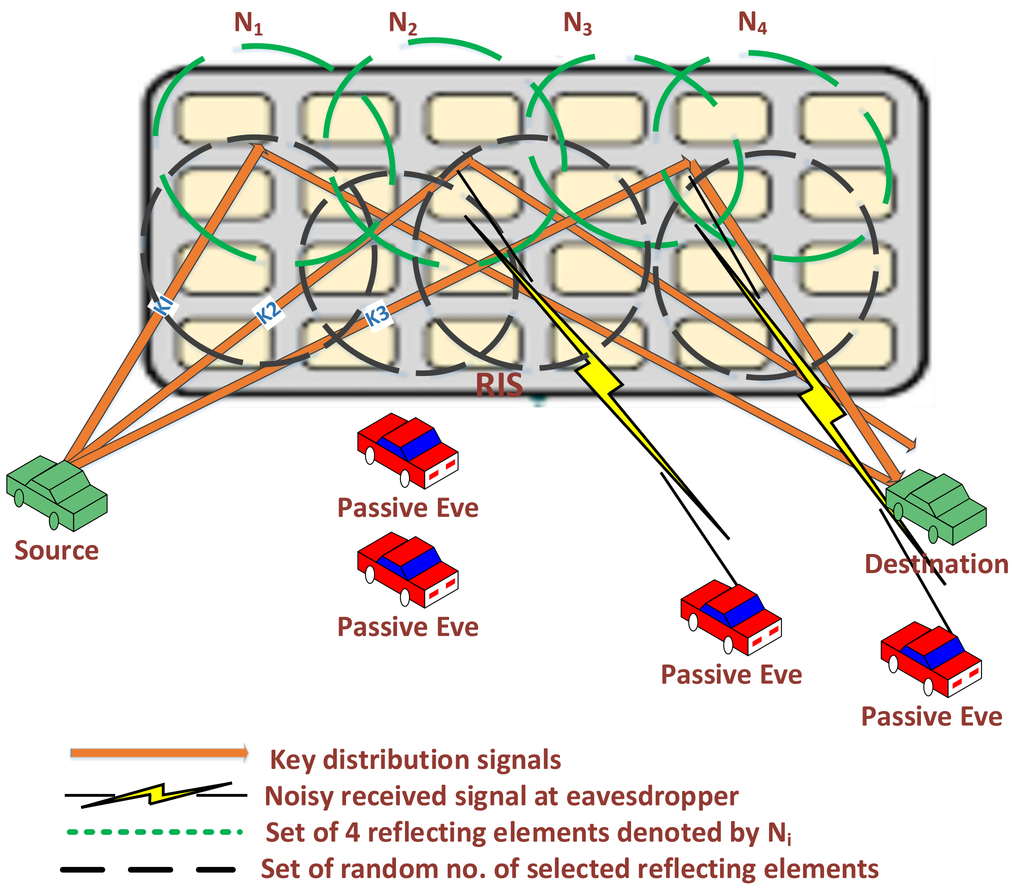
N1
N2
N3
N4
K1
K2
K3
RIS
Source
Passive Eve
Passive Eve
Passive Eve
Passive Eve
Destination
Key distribution signals
Noisy received signal at eavesdropper
Set of 4 reflecting elements denoted by Ni
Set of random no. of selected reflecting elements

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

All the links, i.e., h_{SD}, h_{DS}, h_{SRD} and h_{DRS} satisfy the property that $h_\phi \sim CN(0, \delta_{h_D})$, where $\phi \in \{SD, DS, SE, DE\}$. The RIS assisted links are $h_{SRD} \in C^{N \times 1}$ and $h_{DRS} \in C^{N \times 1}$, respectively. N_j denotes the set of reflecting elements of an RIS on which the signal is incident. It is considered that the eavesdropper is at a distance of half the wavelength from the receiving vehicle. Thus, its CSI information is different from that of the destination vehicle, and cannot tap into the information being exchanged between the legitimate vehicles.

Based on the above layout, there are two types of scenarios.

1. An inbound vehicle that is approaching the source or destination can share the same channel if the distance is less than half the wavelength.
2. An outbound vehicle that is moving away from the legitimate communicating vehicles does not share the same channel.

In both cases, the communication time period is limited. The vehicles tend to be in range for a very short amount of time for any legitimate vehicles or eavesdroppers. The other possibility is that sharing the same CSI is also high for the eavesdropper during the contact period. An inbound vehicle (approaching vehicle) can easily intercept the information signal being exchanged. To address the issue of generating the keys in a given time slot, the next section discusses a proposed methodology in which a set of RIS elements are used to increase the KGR.

5. Proposed Methodology

In our proposed scheme, we have considered that the RIS is a passive relay to reduce capital expenditure. To introduce channel reciprocity, we have considered different sets of reflecting elements of an RIS. As the information signal being exchanged is in the form of a lobe rather than a straight line, that covers up a section of the RIS. We consider different sets of reflecting elements of the RIS instead of considering the RIS as a whole. The angle of incidence is assumed to be controlled by the sender, as the location of the communicating devices and direction of motion are exchanged via the training symbols. The signal is considered to be in the form of a beam that is directed towards a set of reflecting elements that satisfies the half wavelength distance condition for the time duration, i.e., Δt. The steps of our proposed scheme are given in the Algorithm 1.

Algorithm 1 Increase in KGR by using a set of reflecting elements of an RIS.

```
At the start of each time slot
Step# I Initialization:
Sender $S$ and receiver $r$ exchange training symbols $X_i$ for
1. location exchange via GPS locator
and
2. Direction of motion
Step# II Selection of a set of reflecting elements:
During time slot $\Delta t$ based on location
1. Select a set of reflecting elements from $j$, where $j = 1, 2, 3 \ldots, N$
2. Use of a different set of $j$ for the next information
exchange, by using different combinations.
End
```

5.1. Initialization

During this step of Algorithm 1, the training symbols are exchanged between the legitimate transceivers, location identification, and direction of motion. For simplicity, we assume that the communicating devices are equipped with GPS, and the channel conditions remain unchanged during the time interval, i.e., Δt.

5.2. Selection of a Set of Reflecting Elements

In this step, the set of reflecting elements is selected for the exchange of information signals. As the channel conditions are assumed to remain unchanged for the duration of Δt, the next information signal will be directed towards the next set of reflecting elements, i.e., each signal is directed towards a different set of reflecting elements. Here, even if the eavesdropper is aware of a communication taking place, it cannot intercept the information signal as it does not have the complete CSI and cannot interpret which set of reflecting elements is being used for the information exchange.

5.3. Subsequent Time Slot

During this step, as soon as the channel conditions change, the legitimate communicating devices should start over from Step 1 where the training symbols are re-exchanged until the communication ends.

6. RIS-Based Secrete Key Generation Rate

SKG represents the upper bound for KGR where h_S and h_D represent the main CSI of the source and destination vehicle at Δt, respectively. h_E is the CSI of the eavesdropper. Thus, we can represent the full SKG for mutual information by

$$C = x(h_S; h_D / h_E), \tag{5}$$

where C is the SKG, x is the mutual information being exchanged. As depicted in Figure 1 of the system model, the source and destination vehicles send training/probing signals to each other at the start of each time slot, for which the CSI at the legitimate communicating vehicles can be represented as

$$h_S^{\Delta t} = h_{DS} + \mathcal{W}_S^{\Delta t}. \tag{6}$$

By expanding (6), we obtain,

$$h_S^{\Delta t} = (h_{DS} + h_{DRS}) + \mathcal{W}_S^{\Delta t}. \tag{7}$$

$$= (h_{DS} + \sum_{i=m}^{N_i} h^i_{DRS} e^{-k\theta_n})x + \mathcal{W}_S^{\Delta t} \tag{8}$$

Similarly, at the receiving vehicle side,

$$h_D^{\Delta t} = \mathcal{H}_{SD} + \mathcal{W}_D^{\Delta t}. \tag{9}$$

By expanding (9) at the destination side, we obtain

$$h_D^{\Delta t} = (h_{SD} + h_{SRD}) + \mathcal{W}_D^{\Delta t}, \tag{10}$$

$$= (h_{SD} + \sum_{i=m}^{N_i} h^i_{SRD} e^{-k\theta_n})x + \mathcal{W}_D^{\Delta t}. \tag{11}$$

Here, $\mathcal{W}_S$ and $\mathcal{W}_D$ represent the observed noise values received at the legitimate source and destination vehicles, respectively. It includes all the terms of direct and relayed channels noise terms. Also, they satisfy, $\mathcal{W}_S \sim CN(0, \delta_{\mathcal{W}_S^2})$ and $\mathcal{W}_D \sim CN(0, \delta_{\mathcal{W}_D^2})$. The distribution values for channel estimation that involves communication via the RIS are, $\mathcal{H}_{DS} \sim CN(0, \delta^2_{\mathcal{H}_{DS}})$ and $\mathcal{H}_{DS} \sim CN(0, \delta^2_{\mathcal{H}_{DS}})$, respectively, i.e., both from *D-to-S* and from *S-to-D*. $\delta^2_{\mathcal{H}_{DS}}$ and $\delta^2_{\mathcal{H}_{DS}}$ can be further expressed as,

$$\delta^2_{\mathcal{H}_{DS}} = \delta^2_{DS} + \sum_{i=m}^{N_i} e^{-k\theta_n} \delta^2_{DRS}, \tag{12}$$

and

$$\delta^2_{\mathcal{H}_{SD}} = \delta^2_{SD} + \sum_{i=m}^{N_i} e^{-k\theta_n} \delta^2_{SRD}. \tag{13}$$

In the coherent time slot, the channels of the legitimate vehicles are in reciprocity with respect to each other. Thus, it can be established that $\delta^2_{\mathcal{H}_{DS}} = \delta^2_{\mathcal{H}_{SD}}$, according to Snell's law [33–35].

The direction of motion is exchanged during the initial probing of the channel estimation and the distances between source, destination and eavesdropper vehicles are half the wavelength, which makes it difficult for E to tap into the information being exchanged between the legitimate vehicles. This further simplifies (5) that can be represented as

$$\begin{aligned} C &= \mathcal{I}(h_S; h_D/h_E), \\ &= \mathcal{I}(h_S; h_D), \end{aligned} \tag{14}$$

$$C = A_d^{\Delta t}(h_S) + A_d^{\Delta t}(h_D) - A_d^{\Delta t}(h_S, h_D), \tag{15}$$

where $A_d^{\Delta t}(.)$ represents the differential entropy's at time interval Δt for the legitimate source and destination vehicles. To obtain shared keys after the CSI information is acquired at both ends, (12) must be satisfied [36]

According to [22], due to channel reciprocity the channel coefficients between S and D and between the RIS is almost equal thus, it can be represented by

$$h_S = h + w_S, \quad \text{and} \quad h_D = h + w_D, \tag{16}$$

where $h \sim CN(0.\delta_h^2)$, $w_S \sim CN(0.\delta_S^2)$ and $w_D \sim CN(0.\delta_D^2)$, respectively. In addition, the SKG rate for the duration Δt can be presented as

$$\mathcal{I}(x;y) = \log_2\left(1 + \frac{\delta_h^2}{\delta_{w_S}^2 + \delta_{w_D}^2 + \frac{\delta_{\mathcal{W}_{\mathcal{S}}}^2 + \delta_{\mathcal{W}_{\mathcal{D}}}^2}{\delta_h^2}}\right). \tag{17}$$

Combining the distribution of channel estimations via the RIS with that of (17), the SKG rate can be represented as

$$\mathcal{I}(h_S;h_D) = \log_2\left(1 + \frac{\delta_{\mathcal{H}_{SD}}^2}{\delta_{\mathcal{W}_S}^2 + \delta_{\mathcal{W}_D}^2 + \frac{\delta_{\mathcal{W}_S}^2 + \delta_{\mathcal{W}_D}^2}{\delta_{\mathcal{H}_{SD}}^2}}\right). \tag{18}$$

The channel coherency and reciprocity observe the noise values, i.e, $\mathcal{W}_S$ and $\mathcal{W}_D$ are both independent and equivalent to each other. Thus, $\delta_{\mathcal{W}_S}^2 = \delta_{\mathcal{W}_D}^2 = \delta_h^2$. Hence, it further simplifies (18) and the SKG rate can be expressed as

$$\mathcal{I}(h_S;h_D) = \log_2\left(1 + \frac{\frac{\delta_{\mathcal{H}w}^4}{\delta_w^4}}{1 + \frac{2\delta_{\mathcal{H}_{SD}}^2}{\delta_w^2}}\right). \tag{19}$$

Combining (9), (13) with (19), the final SKG rate equation can be deduced as

$$\mathcal{I}(h_S;h_D) = \log_2\left(1 + \frac{\frac{\left(\delta_{SD}^2 + \sum_{i=m}^{N_i} \delta_{h_{SRD}^i}^2 \quad e^{-k\theta_n}\right)}{\delta_{\mathcal{W}}^4}}{\frac{1+2\left(\delta_{DS}^2 + \sum_{i=m}^{N_i} \delta_{h_{DRS}^i}^2 \quad e^{-k\theta_n}\right)}{\delta_{\mathcal{W}}^2}}\right). \tag{20}$$

From (20), it can be observed that by adjusting the selection of the reflecting surfaces of an RIS for Δt, there is an increase in the SKG rate for the moving vehicles.

7. Simulation Results

For simulation, we have considered that each vehicle is equipped with at least two antennas. We also consider a single passive RIS in our scenario. The number of reflectors is denoted by N, where $N = \{16, 32, 64\}$. The vertical distance between the legitimate vehicles is considered between 1 to 16 meters (angular distance is considered). The path loss, i.e., δ is considered up to 30 dB. Δt i.e., the time duration is kept 1 second. It is also assumed that the vehicles are in motion at varying distances. For a specific time slot, the number of vehicles passing through a certain point is taken between 5 to 8. The list of simulation parameters is given in Table 2.

Table 2. Simulation parameters.

Parameters	Configuration
No. of Antennas	2
Size of RIS	16, 32, 64
Vertical distance	1–16 m
Path loss	0.68–30 dBm
Set of RIS elements	3, 4, 5, 6

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.

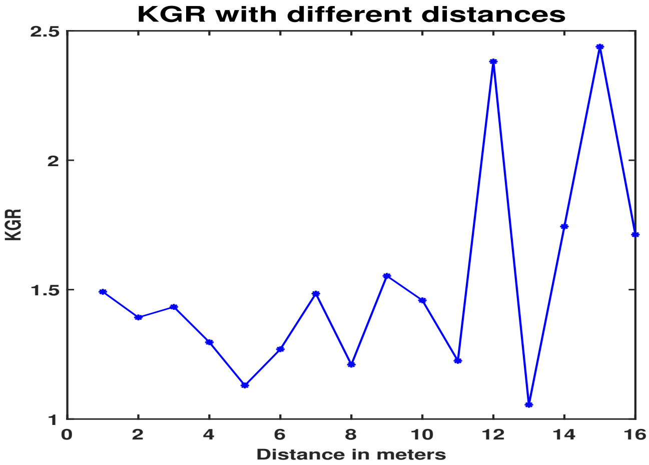

Figure 2. Considering a set of 4 reflectors per group, varying the distance between source and destination, while keeping noise constant.

In Figures 3 and 4, we consider 3 and 5 sets of reflectors as a group per RIS, respectively. Here, we also consider noise as a constant value. The distance between the source and destination is varying constantly, as they are considered in motion. The distance of the eavesdroppers is also varied between 4–16 m. It can be observed from the graph that for a set of 3 reflectors, the KGR reaches a maximum of 1.7 bps. When we consider a set size of 5 reflectors, the KGR reaches up to 3.5 bps. As the distance drops, the KGR for 3 and 5 sets of reflectors drops up to 0.73 bps and 1.3 bps, respectively. In the case of 3 RE per set, the possible sets are more in number as compared to that of 5 RE per set. Yet, in the case of 3 RE, the KGR is 1.7 bps at max. The reason is that the consecutive phase shifts at the RIS are very small, which results in minimum noise values, which further decreases the KGR.

In Figures 3 and 4 the key values are also fluctuating. This is due to distance. As we are considering moving vehicles, i.e., both the legit communicating entities as well as the eavesdroppers. In the figures, the KGR drops as soon as the eavesdropper is in signal-receiving range, i.e., the distance of the eavesdropper from the RIS is less in comparison to that of the legit communicating vehicles, or the eavesdropper is in the signal-receiving range of the receiver or the sender, which results in a drop in the KGR. In the case of 5 RE per set, there is a significant increase in the KGR, as the consecutive phase shifts are larger. Thus, the probability of the eavesdropper sharing the same channel is further reduced, increasing KGR.

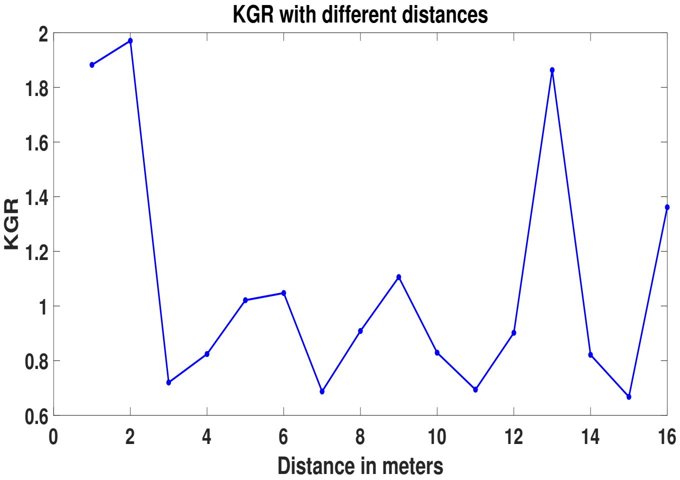

Figure 3. Considering a set of 3 reflectors per group, varying the distance between source and destination, while keeping noise constant.

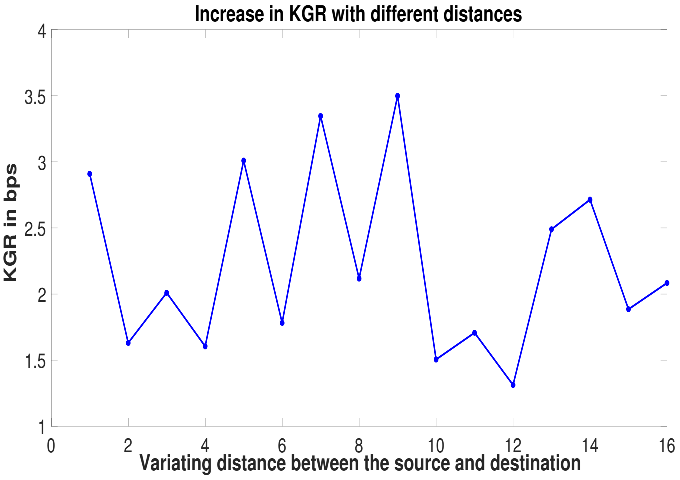

Figure 4. Considering a set of 5 reflectors per group, varying the distance between source and destination, while keeping noise constant.

Table 3 is a comparison between the three groups where we consider 3, 4, and 5 sets of reflectors for the same-sized RIS. As mentioned previously, only the distance is varied between the source and destination, while other values, such as noise and interference, are kept constant and as low as possible. The KGR has a better rate when we are considering a set of 5 reflectors as compared to a set of 3 and 4 reflectors. The KGR increases up to 3.5 bps for a set of 5 reflectors, even when the distance between the eavesdroppers and the communicating devices decreases. The KGR for a set of 5 reflectors drops to 1.34 bps. The reason is the distance of the eavesdropper in comparison to both the source and destination vehicle, followed by the overlapping of the consecutive communication signal between the source and destination, due to the smaller set size of the reflecting elements. As previously mentioned, if we can change the set size based on the angle of incidence of the signal, i.e., in Figure 4, the KGR is improved per time slot and reaches up to 3.5 bps. The results for a set of 4 reflectors are also much better in comparison to that of a set of 3 reflectors where the KGR increases up to 2.5 bps and drops to 1.11 bps, depending on the distances between the eavesdropper from the legit communicating vehicles. From this comparison, it can be observed that the distance between the eavesdroppers and the communicating devices has a great impact on the key generation rate. This is due to the reason that the incident signal is in the form of a lobe that might cover more reflectors. The angle of incidence also affects the number of reflectors being covered by the signal. Therefore, 5 reflectors as a group provide much better performance.

Table 3. Comparison table.

Set of Reflectors	Increase in KGR	Decrease in KGR
3	1.7 bps	0.76 bps
4	2.5 bps	1.11 bps
5	3.5 bps	1.34 bps

Figure 5 represents the possible subsets per RIS, of size 16, 32, and 64, respectively. Here we are considering a random number for the subset of reflectors. It can be observed from the graph that the possible subsets for an RIS-sized 64 are much higher, i.e., 5000, in comparison to that of 32- and 16-sized RISs, which are up to 2250 and 1000 subsets, respectively. Thus, large-sized RIS provides a larger variation in the number of subsets, resulting in an increased number of possible keys being generated.

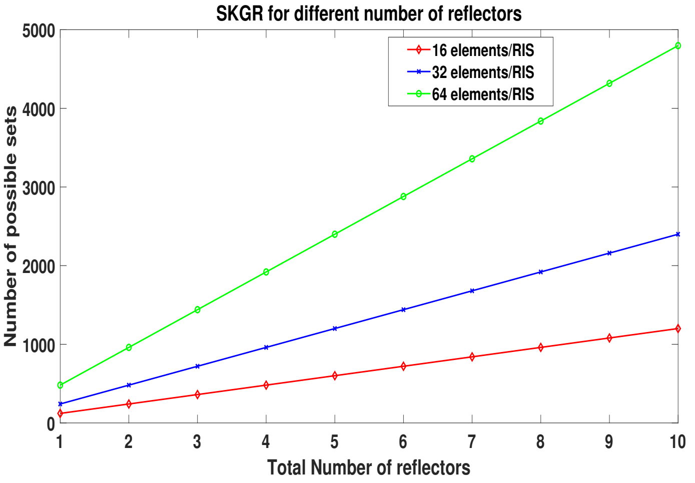

Figure 5. KGR for a random set of reflectors, for different sized RISs.

Figure 6 shows the effects of changes in noise values on the SKGR. For our previous simulations, we considered the worst-case scenarios where there was minimal noise. Here, with the increase in noise values, the SKGR starts to provide a better performance, as it reaches up to 1.8 bps. Thus, from the simulation results conducted noise also has a significant impact on SKGR. An induced noise at the eavesdroppers can also significantly improve the SKGR at the communicating devices.

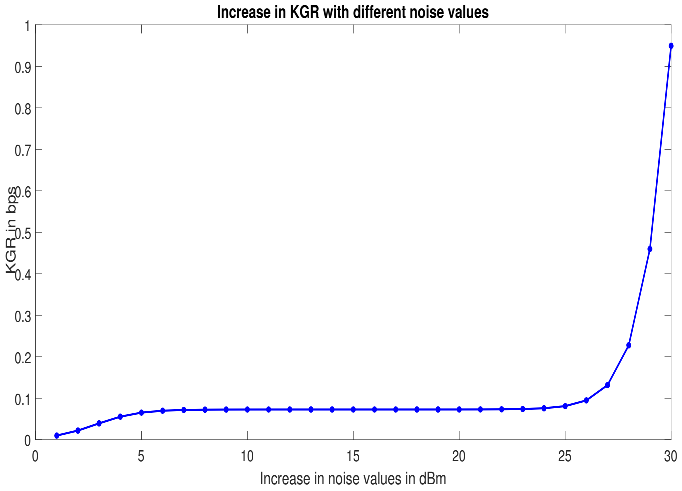

Figure 6. Effect of increase in noise on KGR.

To validate our results in Figure 7, we have implemented the existing DPS of a static environment on the vehicular environment and then the results are compared with our proposed scheme. In Figure 7, a random distribution is adopted for both the legitimate as well as the eavesdropper vehicles. The DPS mechanism performs well but, as soon as the eavesdropper gets within signal-receiving range, there is a sharp decrease in the KGR per time slot.

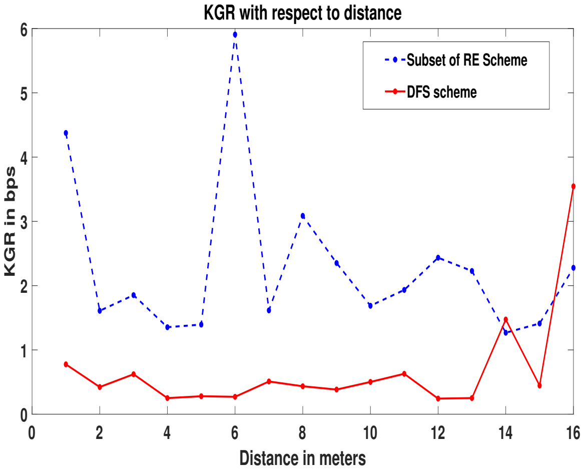

Figure 7. Comparison between our scheme, i.e., sets of RE and DFS scheme for random distances.

Although the RIS has signal boosting and diminishing properties (if the eavesdropper is in range), it can still receive the information signal being exchanged between legitimate vehicles. This is because of the mobile nature of the eavesdropper vehicle. Even though there is a significant drop in the key generation due to the same channel usage by both parties, the proposed scheme still performs better as it is using a subset of RE instead of the RIS as a single device.

In the proposed scheme, indicated by the blue line in Figure 7, the KGR reaches up to 6 bps, while in the worst case it drops to 1.6 bps for a VANET-based environment. The DPS scheme reaches up to 3.7 bps for the best-case scenario, while for most of the other cases it remains below 1 bps. Although an active RIS is better in terms of phase adjustment, it adds extra capital expenditure (CAPEX), which is not desirable.

8. Conclusions

It can be concluded that for a dynamic environment where the devices are in motion, the use of a subset of reflectors for key generation is more proficient. The direction of motion as well as the distance of the eavesdropper from the legitimate users have great significance, i.e., if the eavesdropper has a distance that is less than one wavelength, then it can easily intercept the signals and can tap into the communication streams. To reduce these chances, a subset of reflectors is used in this paper for key exchange, to minimize the possibility of tapping. With the use of a subset of adjacent reflectors, the key generation rate increases per time slot up to 6 bps. The possible variation in the number of subsets that can be created also reaches up to 5000 subsets. With mobility, the KGR reduces drastically, but to increase the KGR, the use of a subset of RE is better than the DFS scheme for a time slot. As a future work we aim to use an active RIS, where we can control the movement of the reflecting elements. Moreover, we also aim to consider other important environmental features, such as the speed and direction of vehicles, in our future work.

Author Contributions: Conceptualization, H.A.; data curation, H.A.; formal analysis, M.W.; investigation, H.A. and M.W.; methodology, H.A.; project administration, M. B., K.-S.K., M.W. and G.A.; software, Z.H.A.; Fund Acquisition, M.B. and K.-S.K.; supervision, M.B., M.W. and G.A.; writing—review and editing, M.W., G.A. and Z.H.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported in part by by the National Research Foundation of Korea-Grant funded by the Korean Government (Ministry of Science and ICT)-NRF-2020R1A2B5B02002478), in part by Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by Korea Government (MSIT) (No. 2019001816), and in part by Science and Engineering Research Board (SERB) for supporting this work, Grant number TAR/2019/000286.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Notation/Symbol	Description
Δt	Time interval
S	Source
D	Destination
E	Eavesdropper
R	RIS
w	AWGN/noise
N	Reflectors/reflecting elements
N_j	Specific set of reflecting elements
θ_n	Angle of the nth reflector
k	Constant
x	Message exchanged
h	channel coefficient
$\mathcal{W}$	Observed noise

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. [CrossRef] [PubMed]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
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. [CrossRef]
10. Liu, Y.; Liu, X.; Mu, X.; Hou, T.; Xu, J.; Di Renzo, M.; Al-Dhahir, N. Reconfigurable intelligent surfaces: Principles and opportunities. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1546–1577. [CrossRef]
11. Di Renzo, M.; Debbah, M.; Phan-Huy, D.T.; Zappone, A.; Alouini, M.S.; Yuen, C.; Sciancalepore, V.; Alexandropoulos, G.C.; Hoydis, J.; Gacanin, H.; et al. Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 1–20. [CrossRef]
12. Makarfi, A.U.; Rabie, K.M.; Kaiwartya, O.; Adhikari, K.; Li, X.; Quiroz-Castellanos, M.; Kharel, R. Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective. *arXiv* **2020**, arXiv:2004.11288.
13. Aldaghri, N.; Mahdavifar, H. Physical Layer Secret Key Generation in Static Environments. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2692–2705. [CrossRef]
14. Huang, W.; Han, Z.; Zhao, L.; Xu, H.; Li, Z.; Wang, Z. Resource Allocation for Intelligent Reflecting Surfaces Assisted Federated Learning System with Imperfect CSI. *Algorithms* **2021**, *14*, 363. [CrossRef]

15. Liu, Y.; Wang, M.; Xu, J.; Gong, S.; Hoang, D.T.; Niyato, D. Boosting Secret Key Generation for IRS-Assisted Symbiotic Radio Communications. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–6.
16. Di Renzo, M.; Zappone, A.; Debbah, M.; Alouini, M.S.; Yuen, C.; De Rosny, J.; Tretyakov, S. Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2450–2525. [CrossRef]
17. Yuan, X.; Zhang, Y.J.A.; Shi, Y.; Yan, W.; Liu, H. Reconfigurable-intelligent-surface empowered wireless communications: Challenges and opportunities. *IEEE Wirel. Commun.* **2021**, *28*, 136–143. [CrossRef]
18. Hamdi, M.M.; Yussen, Y.A.; Mustafa, A.S. Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A Review. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 11–13 June 2021; pp. 1–7.
19. Bottarelli, M.; Epiphaniou, G.; Ismail, D.K.B.; Karadimas, P.; Al-Khateeb, H. Quantisation feasibility and performance of RSS-based secret key extraction in VANETs. In Proceedings of the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK, 11–12 June 2018; pp. 1–8.
20. Gupta, D.N.; Kumar, R. Distributed key generation for secure communications between different actors in service oriented highly dense VANET. In *Cloud and IoT-Based Vehicular Ad Hoc Networks*; Wiley Online Library: Hoboken, NJ, USA, 2021; pp. 221–232.
21. Vijayakumar, P.; Azees, M.; Kozlov, S.A.; Rodrigues, J.J. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 1630–1638. [CrossRef]
22. Hu, X.; Jin, L.; Huang, K.; Sun, X.; Zhou, Y.; Qu, J. Intelligent Reflecting Surface-Assisted Secret Key Generation With Discrete Phase Shifts in Static Environment. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1867–1870. [CrossRef]
23. Gao, Y.; Guo, D.; Xiong, J.; Ma, D. Intelligent Reflecting Surface Assisted Multi-User Robust Secret Key Generation for Low-Entropy Environments. *Entropy* **2021**, *23*, 1342. [CrossRef]
24. Yang, S.; Han, H.; Liu, Y.; Guo, W.; Zhang, L. Intelligent Reflecting Surface-induced Randomness for mmWave Key Generation. *arXiv* **2021**, arXiv:2111.00428.
25. Lu, X.; Lei, J.; Shi, Y.; Li, W. Intelligent reflecting surface assisted secret key generation. *IEEE Signal Process. Lett.* **2021**, *28*, 1036–1040. [CrossRef]
26. Chen, Y.; Li, G.; Pan, C.; Hu, L.; Hu, A. Intelligent reflecting Surface-Assisted secret key generation in multi-antenna network. *arXiv* **2021**, arXiv:2105.00511.
27. Staat, P.; Elders-Boll, H.; Heinrichs, M.; Kronberger, R.; Zenger, C.; Paar, C. Intelligent reflecting surface-assisted wireless key generation for low-entropy environments. In Proceedings of the 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Helsinki, Finland, 13–16 September 2021; pp. 745–751.
28. Ji, Z.; Yeoh, P.L.; Chen, G.; Pan, C.; Zhang, Y.; He, Z.; Yin, H.; Li, Y. Random shifting intelligent reflecting surface for OTP encrypted data transmission. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1192–1196. [CrossRef]
29. Liu, Y.; Huang, K.; Sun, X.; Yang, S.; Wang, L. Intelligent Reflecting Surface–Assisted Wireless Secret Key Generation against Multiple Eavesdroppers. *Entropy* **2022**, *24*, 446.
30. Wei, Y.; Zeng, K.; Mohapatra, P. Adaptive wireless channel probing for shared key generation based on PID controller. *IEEE Trans. Mob. Comput.* **2012**, *12*, 1842–1852. [CrossRef]
31. Zhang, J.; Duong, T.Q.; Marshall, A.; Woods, R. Key generation from wireless channels: A review. *IEEE access* **2016**, *4*, 614–626. [CrossRef]
32. ElMossallamy, M.A.; Zhang, H.; Song, L.; Seddik, K.G.; Han, Z.; Li, G.Y. Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 990–1002.
33. Möller, D. Volume 2 History, Change and Sustainability. In *Chemistry of the Climate System*; De Gruyter: Berlin, Germany, 2020.
34. Dziewierz, J.; Gachagan, A. Correspondence: Computationally efficient solution of Snell's law of refraction. *IEEE Trans. Ultrason. Ferroelectr. Freq. Control.* **2013**, *60*, 1256–1259.
35. Dajer, M.; Ma, Z.; Piazzi, L.; Prasad, N.; Qi, X.F.; Sheen, B.; Yang, J.; Yue, G. Reconfigurable intelligent surface: Design the channel–A new opportunity for future wireless networks. *Digit. Commun. Netw.* **2021**, *8*, 87–104.
36. Ye, C.; Reznik, A.; Shah, Y. Extracting secrecy from jointly Gaussian random variables. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 2593–2597.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.