sensors

MDPI

Article

Secure Networking with Software-Defined Reconfigurable Intelligent Surfaces

Francesco Chiti *, Ashley Degl'Innocenti and Laura Pierucci

Department of Information Engineering, University of Florence, 50139 Firenze, Italy
* Correspondence: francesco.chiti@unifi.it; Tel.: +39-055-2758588

Abstract: Reconfigurable intelligent surfaces (RIS) are considered of paramount importance to improve air–ground and THz communications performance for 6G systems. Recently, RISs were proposed in Physical Layer Security (PLS), as they can (i) improve the secrecy capacity due to the controlled directional reflections' capability of RIS elements and (ii) avoid potential eavesdroppers, redirecting data streams towards the intended users. This paper proposes the integration of a multi-RISs system within a Software Defined Networking (SDN) architecture to provide a specific control layer for secure data flows forwarding. The optimisation problem is properly characterised in terms of an objective function and an equivalent graph theory model is considered to address the optimal solution. Moreover, different heuristics are proposed, trading off complexity and PLS performance, to evaluate the more suitable multi-beam routing strategy. Numerical results are also provided, focusing on a worst case scenario which points out the improvement of the secrecy rate from the increase in the number of eavesdroppers. Furthermore, the security performance is investigated for a specific user mobility pattern in a pedestrian scenario.

Keywords: reconfigurable intelligent surfaces; software-defined networking; physical layer security; secrecy capacity optimization

Citation: Chiti, F.; Degl'Innocenti, A.; Pierucci, L. Secure Networking with Software-Defined Reconfigurable Intelligent Surfaces. *Sensors* **2023**, *23*, 2726. https://doi.org/10.3390/s23052726

Academic Editors: Nicola Zannone, Giuseppe Piro and Savio Sciancalepore

Received: 30 January 2023
Revised: 27 February 2023
Accepted: 28 February 2023
Published: 2 March 2023

1. Introduction

Recently, Intelligent Reflective Surfaces (IRS) have been consideredof paramount importance for beyond 5G and 6G cellular systems, [1] in order to increase the link efficiency in terms of data rate, coverage, and connectivity, as well as being a good means to reduce energy consumption. Since one of the most relevant challenges for 6G are the air-to-ground communications, IRSs can also be employed to enlarge the cellular coverage provided by aerial platforms or the unmanned aerial vehicle, and consequently to optimize the air-to-ground average rate [2], as well as in conjunction with the non-orthogonal multiple access (NOMA) technique for the uplink cellular network [3]. Another key enabling the technology for 6G is Terahertz (THz) communications. IRSs applied in THz systems can dynamically control the propagation of THz signals and overcome the signal communication disruption due to obstacles by steering the THz signals in the desired direction, or, they can act as relays to increase the coverage area [4]. Specifically, IRS is a planar array with a high number of passive small reflecting surface/elements, called tiles, which allow one to change the amplitude and phase of the incident electromagnetic wave in order to reflect it passively in the desired spatial direction, mainly towards the receiver or another IRS, in a reconfigurable way [1,5].

This vision paves the way towards the related concept of the reconfigurable intelligent surface (RIS) [6], where a software controller can jointly optimise and configure the input and reflecting waves based on sensed data. Furthermore, as RISs can interact, reconfigure and program the wireless environment, they can be adopted to enhance the Physical Layer Security (PLS). Specifically, RISs can improve the secrecy capacity of the channel, by allowing data streams to reach the intended users, avoiding eavesdroppers as much

as possible by means of directional reflections, especially for the Internet of Things (IoT) scenario [7].

Considering an IoT domain, the novel concept of Software-Defined Networking (SDN) allows the reactive control of traffic flows by configuring the network resources to meet the application requirements [8]. Indeed, SDN is a networking approach that decouples the *control* of the network resources from the operations related to the information *forwarding*. Through specific software-based SDN Controllers, the entire network could be centrally managed with an improved efficiency thanks to the separation between the control plane and hardware devices (data plane). Moreover, SDN combines the benefits of the virtualisation and compute continuum, thus allowing the definition of new intelligent architectures that support more complex network functionalities to offer a more advanced service, e.g., through the integration of wired and wireless systems. According to this promising vision, the SDN architecture has been recently proposed to enhance the PLS, where a SDN Controller is able to perform a device selection in order to optimise the secrecy capacity [9].

To address the above issues, this paper introduces a SDN Controller in a RIS-aided system to dynamically optimise the path between the source and destination (legitimate user) through multiple RISs in order to avoid malicious nodes, where we assume RISs as secure nodes. Differently from other papers in the literature, which analyze attacks to the RIS controller, we consider uplink communications from legitimate users to the base station (or access point) where the eavesdroppers want to replace legitimate transmissions, therefore considering the worst case scenario due to the lower uplink transmission powers. According to the multiple RIS approach, each authorised network device cooperates for a common goal (i.e., multi-hop cooperative RISs), with the advantage of increasing the power gain of $O(M^4)$, where M represents the number of reflecting elements, which exceed the value of $O(M^2)$ related to the single RIS reflection link, as discussed in [10].

Specifically, graph theory methodologies have been applied for designing a PLS anti-eavesdropping strategy. In particular, a weighted graph is derived from the network topology, where a Shortest Path Algorithm (SPA) is applied to evaluate the appropriate path in order to connect the source and destination node, with the aim of improving security metrics.

Furthermore, to the best of our knowledge, the use of multiple RIS-assisted system applied to the case of mobile users has not been investigated before. This paper presents, indeed, a mobility pattern in a pedestrian scenario, with a limited area (i.e., such as a square) being representative of a realistic case study occurring in an urban scenario to test the security related performance of the proposed integrated multiple-RISs and SDN approach.

The most relevant challenges of this paper can be detailed as follows:

- We design a cooperative multi-beam multi-hop routing strategy that involves multiple IRSs to select the best reflection path between source and destination to improve PLS performance also in the case of mobile IoT devices with moderate speed;
- We analytically derive the overall end-to-end (e2e) sum-secrecy rate maximisation problem subject to the constraint for assuring a target capacity at the destination;
- We propose different heuristics to avoid eavesdroppers with a reasonable complexity;
- We propose the integration of IRSs into an SDN architecture to address the implementation of the proposed framework.

The paper is organised as follows. Section 2 reviews some papers related to RIS technologies and their application towards PLS. Section 3 presents a comprehensive model for the considered secure multiple RIS-aided IoT system, along with the related SDN architecture. In addition, the optimisation problem is presented, together with the low complexity heuristics. Then, Section 4 shows the numerical results in terms of the average secrecy rate for different eavesdroppers' deployments. Section 5 addresses our main results and indicates the future directions for a secure multi-RIS system.

2. Related Work

Several comprehensive surveys on the emerging RIS technology are provided in the literature, e.g., in [5,11], focusing on potential applications, challenges, hardware architecture and practical constraints, while highlighting its ability to control and manage the wireless channel to enhance the communication performance.

The authors in [12] enlarge the perspective of a programmable wireless environment by providing a review on the impact of double or multiple RIS use. First, they analyse the advantages of multiple RISs with respect to single-reflection links and, then, highlight two main issues: (i) the channel state acquisition with a low overhead in the case of bad channel conditions due to a large number of obstacles and (ii) the multi-RIS selection optimisation for each user to maximise the total throughput and narrow interference among users.

In the existing literature, several papers usually consider attack models directly to the controller of RIS systems, which provides decisions on the spatial reflections of the signals, therefore increasing the vulnerability of the received signal, as in [13–15]. The vulnerability of pilot signals is considered, where pilot signals are transmitted to alter the channel state estimation to the legitimate users, i.e., the pilot spoofing attack. In [16], the RIS is used to improve the security of traditional key generation technology. An RIS-assisted Manipulating attack (RISM) is considered, where a malicious user can destroy the uplink and down link channel reciprocity. Then, a slewing rate detection method was proposed which can detect and separate the attacked path, maximising the key generation rate.

A classical approach to improve PLS is investigated in [7], where a scenario with an access point (AP) aided by RIS, a legitimate user and one eavesdropper, was evaluated. The paper provides the well-known result that the secrecy rate was improved by increasing the number of RIS elements and decreasing the average signal-to-noise ratio (SNR) that was closer to the eavesdropper.

In another contribution, RISs are used for enhancing the PLS of wireless communications systems [17] and, in particular, the classical scenario, with an RIS assisting a multi-antenna transmitter to secure the wireless system, with a single-antenna receiver and one eavesdropper, is adopted. The block coordinate descent (BCD) and minorisation maximisation (MM) techniques are developed to solve the non-convex optimisation problem related to the joint optimisation of the beamformer at the transmitter, and the RIS phase shifts to maximise the secrecy rate.

The authors in [18] consider the problem of the secrecy rate maximisation in the case of eavesdroppers equipped with a multiple-input multiple-output multi-antenna (MIMOME) and an RIS-assisted Gaussian wiretap channel (WTC). In particular, the block successive maximisation (BSM) method is adopted which considers a lower bound on the secrecy rate to optimise the input covariance matrix, while the maximisation is carried out for each individual phase shift.

In [19], the secure communication is analyzed in a STAR-RIS configuration, i.e., where the source and legitimate user cannot be at the same side of the RIS, and integrated with the non-orthogonal multiple access (NOMA) strategy. Furthermore, an artificial noise (AN) was introduced to improve the secure communications. The non-convex optimization problem related to AN and NOMA parameters and the number of RIS elements to improve the secrecy rate is solved by using the successive convex approximation (SCA) and semi-definite relaxation (SDR) techniques.

In [20], the authors consider a multiple antenna system at the transmitter side, and include a legitimate user and an eavesdropper. To secrete the information, the RIS reflection coefficients are weighted with multiplicative random coefficients in each transmission, but the channel matrix is diagonally maintained for the intended user. As a consequence, the legitimate user can decrypt the information, while the eavesdropper cannot decode it. The paper suggests three different reflection randomness schemes to diagonalize the channel matrix by using: (1) the space-shift keying (SSK) modulation, (2) quadrature space-shift keying (QSSK) modulation and forcing the diagonal elements to have real values,

(3) multiple phase-shift keying (PSK) and converting diagonal elements to assume real values again.

Differently, the paper [21] suggests that the induced randomness on the RIS reflection coefficients could also be performed on the signal received by the eavesdroppers and consequently they can collaborate to estimate the RIS-generated random channel and decode the secret key.

Finally, as discussed in [19], RISs are integrated in an SDN architecture to enforce the advanced PLS, with the main goal of detecting the position of possible eavesdroppers and steering the wireless waves in the space to avoid being close to malicious users through the orchestration of a set of metasurfaces.

In this paper, we consider an integrated SDN-RISs architecture as in [19], where multiple RISs dynamically act as relays to support e2e data flow delivery with the aim of avoiding eavesdroppers present in the path. However, differently from [19], which only shows the feasibility of an integrated reconfigurable antenna system with SDN, (i) we have proposed several heuristics with increasing computational complexity to optimize the multi-beam routing strategy focused towards PLS and (ii) we demonstrated the simulation results related to the secrecy rate performance also considered users' mobility.

In conclusion, to the best of our knowledge, the use of SDN and the multiple RIS-assisted system applied to the case of mobile users has not been investigated before in the literature.

3. System Model

In deriving a suitable model for investigating the proposed approach performance, we consider an outdoor scenario comprised of $K+2$ legitimate nodes, where a source A_0 transmits to a destination A_{K+1} (e.g., the base station), on a path $\Omega = (A_0, A_1, \ldots, A_{K+1})$ formed by K RISs and a number of E_{N_e} eavesdroppers, as pointed out in Figure 1.

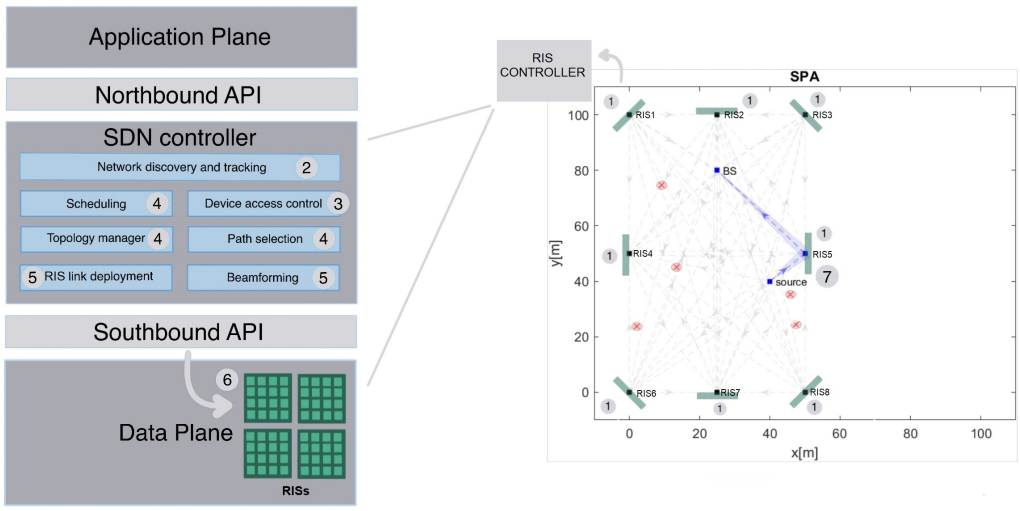

Figure 1. Proposed SDN-oriented system architecture, where the Control Plane is decomposed into functional blocks interacting with the local RIS controller.

In particular, we propose the integration of multiple RISs into a SDN general framework. To this purpose, we refer to the classic architecture composed of the Application, Control and Data Planes (AP, CP, DP) already proposed in [18], but focused on security rather than mere communications. Specifically, RISs belong to DP and in turn are connected to the SDN Controller via a proper gateway, where a southbound interface is implemented to allow a bidirectional control message exchangein order to monitor and control the e2e data forwarding. As this connection is wired, the adoption of the standard OpenFlow protocol can be assumed [22].

Moreover, the following operations were considered in Figure 1 as part of the Controller management logic:

- *Network Discovery* and *Tracking*: responsible for the device location through an algorithm of the compressed sensing of wavefronts involving RISs [23];
- *Device Access Control*: intended for classifying the users;
- *Topology Manager*: responsible for maintaining an accurate abstract representation of the network;
- *Decision Engine* and *Path Selection*;
- *RIS Link Deployment* and *End-Device Beamforming*.

It is worth noticing that these functionalities are based on information collected by the SDN Controller via proper messaging and processed by a specific algorithm in order to derive the global network state. Figure 1 also presents the steps in orchestrating the overall control workflow performed by the SDN Control:

1. Channel state information (CSI) sensing;
2. Network discovery (usually represented as an annotated graph) and device tracking;
3. Device access control;
4. Topology management and optimum path selection;
5. RIS link set-up and end-device beamforming;
6. e2e data flow transmission;
7. Device configuration.

The SDN Controller abstracts the network topology into an anti-eavesdropping weighted graph, where the legitimate nodes are part of the vertex set and the links between them are part of the edge set. Usually, RISs can provide additional paths as an alternative to the direct path, in the case where it is not available due to obstacles and/or poor channel quality. In general, the e2e capacity of a source to the destination flow over a given path $\Omega = (A_0, A_1, \ldots, A_{K+1})$ is given by:

$$C_{\Omega}^{d} = \log_2(1 + \gamma_d) \quad \text{[bps/Hz]} \tag{1}$$

where γ_d is the received signal to noise ratio (SNR) at the destination. Similarly, the e2e capacity of the wiretap channel can be detailed as follows:

$$C_{\Omega}^{E} = \log_2(1 + \gamma^{E}) \quad \text{[bps/Hz]} \tag{2}$$

where γ^E is the e2e SNR for the eavesdropper.

If we consider the presence of eavesdroppers, whose goal it is to intercept the legitimate communications, it is necessary to select the path that maximises the secrecy rate, which is defined by [24] as:

$$C_{\Omega}^{S} = \max\left(C_{\Omega}^{d} - C_{\Omega}^{E}, 0\right) \quad \text{[bps/Hz]} \tag{3}$$

It could be pointed out that a secure communication is possible if and only if the legitimate user experiences a greater channel capacity than the one of the eavesdroppers.

In a free-space propagation scenario, where an ideal isotropic transmit antenna transmits to a lossless receiving antenna located at distance d, then, it is well known that the received power is:

$$P_{rx} = \frac{A}{4\pi d^2} P_{tx} \tag{4}$$

where P_{tx} is the transmitted power and $\beta_d = \frac{A}{4\pi d^2}$ is the free-space channel gain, or pathloss; $A = \frac{\lambda^2}{(4\pi)}$ is the area of an isotropic receive antenna.

First, we consider an uplink communication aided by one RIS. The RIS has M passive reflecting elements, also called tiles, that can reflect the incident signal in a reconfiguirable way, but without amplifying it. In particular, each tile controls the individual phase and magnitude of each reflected signal. We assume a line-of-sight (LoS) propagation.

The e2e-received signal at the destination can be modeled as:

$$r_{RIS} = \boldsymbol{g}^T \boldsymbol{\Theta} \boldsymbol{h} \sqrt{P_{tx}} s + n \tag{5}$$

where s the source signal, and $n \sim N_{\mathbb{C}}(0, \sigma^2)$ is the additive white Gaussian noise (AWGN) at the receiver with variance σ^2. Moreover, $\boldsymbol{\Theta} = diag(\mu_1 e^{j\theta_1}, \ldots, \mu_M e^{j\theta_M})$ is the reflection coefficient matrix, where $\mu_1, \ldots, \mu_M \in [0, 1]$ and $\theta_1, \ldots, \theta_M \in [0, 2\pi)$ are the amplitude and the phase-shift variables, respectively. Moreover, $\boldsymbol{h} = [h_1, \ldots, h_M]^T$ with $h_m = |h_m| e^{-j\phi_m}$ represents the vector of the channel from the source to the RIS, while $\boldsymbol{g} = [g_1, \ldots, g_M]^T$ with $g_m = |g_m| e^{-j\psi_m}$ denotes the vector of the channel from the RIS to the destination. Finally, the channel capacity is given by:

$$\log_2(1 + SNR_{RIS}) \tag{6}$$

where:

$$SNR_{RIS} = |\boldsymbol{g}^T \boldsymbol{\Theta} \boldsymbol{h}|^2 \frac{P_{tx}}{\sigma^2} = \Big| \sum_{m=1}^{M} \mu_m |h_m| |g_m| e^{j(\theta_m - \phi_m - \psi_m)} \Big|^2 \frac{P_{tx}}{\sigma^2} \tag{7}$$

as proposed in [25], where the *far-field approximation* approximation is also introduced. According to this, by assuming the source located at distance d in angle η and the destination located at distance δ in angle ω, if both the source and destination are lying within the far-field region of the RIS, or equivalently that $d\cos(\eta) >> \sqrt{MA}$ and $\delta\cos(\omega) >> \sqrt{MA}$, the SNR can be approximated as:

$$SNR_{RIS} = M^2 \varsigma_{d,\eta} \varsigma_{\delta,\omega} \frac{P_{tx}}{\sigma^2} \tag{8}$$

where:

$$\varsigma_{d,\eta} = \beta_{d\cos(\eta)} \cos^3(\eta) = \frac{A\cos(\eta)}{4\pi d^2} \tag{9}$$

and:

$$\varsigma_{\delta,\omega} = \beta_{\delta\cos(\omega)} \cos^3(\omega) = \frac{A\cos(\omega)}{4\pi \delta^2} \tag{10}$$

3.1. Multi-RIS Setup

As previously introduced, we assume that multiple RISs are deployed to assist in the communication by providing different e2e LoS paths to connect the source and destination. However, this brings us to a trade-off: on one hand, each RIS in the path introduces a M^2 passive beamforming gain, on the other, it makes the multi-reflection pathloss term more significant. The received power over the considered path $\Omega = (A_0, A_1, \ldots, A_{K+1})$ can be expressed according to [10], as:

$$|h_{A_0, A_{K+1}}(\Omega)|^2 = \frac{M^{2K} N \beta^{K+1}}{d^{\alpha}_{A_0, A_2} d^{\alpha}_{A_K, A_{K+1}} \prod_{k=1}^{K} d^{\alpha}_{a_k, a_{k+1}}} \tag{11}$$

where:

$$\kappa(\Omega) = \frac{\sqrt[\alpha]{\beta}^{K+1}}{d_{A_0, A_2} d_{A_K, A_{K+1}} \prod_{k=1}^{K-1} d_{a_k, a_{k+1}}} \tag{12}$$

is the pathloss term for a multi-RIS e2e path, and N is the number of antennas available at the BS, $\beta = \frac{A\cos(\omega)}{4\pi}$ and $A = (\lambda/4)^2$.

3.2. Problem Statement

In order to optimise the physical security policy within an SDN framework, we resort to Graph Theory by relying on an equivalent shortest simple-path problem (SSPP), as proposed in [10] for a different objective function. As we are interested in finding the best e2e path that maximises the secrecy rate, the general optimisation problem (OP) can be formulated as:

- Objective $\max_{\Omega} \quad C_{\Omega}^{S}$;
- Subject to $\gamma_d \geq \gamma_{th}$;
- Given $(x_1, y_1), (x_{K+1}, y_{K+1}), (x_{RIS_i}, y_{RIS_i}), (x_e, y_e)$, $\forall e = 1, \ldots, E$, $\forall i = 2, \ldots, K-2$.

where $\Omega = (A_1, A2, \ldots, A_K)$ is the path that maximises the e2e secrecy rate. In the OP, we introduced the constrain γ_{th}, which is a target threshold that guarantees a sufficient channel capacity at the destination such that paths below that threshold are not taken into account.

We assume the SDN Controller is aware of the positions of legitimate users in the network and is able to estimate the presence and the positions of the eavesdroppers. This is performed by collecting (un)intended uplink signals received by IRS with a specific southbound interface control sub-protocol, storing it and further processing them with a generic localisation algorithm, e.g., a compressed sensing approach that is usually adopted in distributed passive sensing systems.

We derive a directed weighted graph $\mathcal{G}^E = (\mathcal{V}, \mathcal{E})$ that can abstract our network topology in the presence of eavesdroppers and apply a shortest path algorithm (SPA) to solve the OP. Then, the problem shifts to the formulation of an appropriate model for weights in the graph. In particular, the vertex set $\mathcal{V}$ is given by the legitimate nodes and the edge set $\mathcal{E}$ is represented by the links between them. The weight of the edge connecting the i-th and j-th vertexes is given by:

$$W_{i,j}^{E} = \xi * W_{i,j} + \hat{e} = \xi * \ln \frac{d_{i,j}}{M\sqrt{\beta}} + \hat{e} \tag{13}$$

Due to the complexity of the problem, which implies a high control overhead, we present five heuristics which simplify the weights $W_{i,j}^{E}$ to be applied in the derived graph; specifically, the heuristics are sorted by less to more computational complexity. In (13), the key idea is to balance the contribution of the distance/pathloss term (first term) and the impact of the eavesdroppers on each link ($\hat{e}$), while we propose the following heuristics:

HEU1 $\xi = cost$, $\hat{e} = cost = 1 \quad \forall e \in E$ detected in the coverage area.

HEU2 $\xi = cost$, $\hat{e} = \rho \cdot \hat{X} \quad \forall e \in E$ detected in the coverage area. $\rho = cost$ and where $\hat{X} = \max_{i,j=1,\ldots,|V|} W_{i,j}$, thus relating $W_{i,j}^{E}$ to the higher weight in $W_{i,j} \quad \forall$i,j=1, . . . , |V|.

HEU3 $\xi = cost$, $\hat{e} = \frac{2 \cdot \hat{X}}{\log_{10}(\max_e P_{i,e})}$, where $\max_e P_{i,e}, e \in E$ is the maximum value of the pathloss term in the channel between the transmitting node and each eavesdropper.

HEU4 $\xi = cost$, $\hat{e} = \frac{2 \cdot \hat{X}}{|\log_{10}\left(\sum_{e=1}^{E} P_{i,e}\right)|}$, where $\sum_{e=1}^{E} P_{i,e}$ is the sum of the pathloss terms between the transmitting node and each eavesdropper.

HEU5 $\xi = cost$, $\hat{e} = \log_{10}\left(\sqrt{\sum_{e=1}^{E} P_{i,e}}\right)$.

Finally, we address two different operative scenarios:

- *Cooperative*: eavesdroppers are able to communicate with each other in order to combine the wiretapped signals and detect the legitimate user signals,
- *Non Cooperative*: eavesdroppers are independent and do not share information with each other.

As a consequence, the total wiretapped SNR over the path $\Omega = (A_0, A_1, \ldots, A_{K+1})$ is, respectively:

$$(c) \quad \gamma_{\Omega}^{E} = \sum_{r_{i,j} \in \Omega} \sum_{e=1}^{E} \gamma_{i,j,e}^{E} \tag{14}$$

$$(nc) \quad \gamma_{\Omega}^{E} = \max_{1 \le e \le E} \sum_{r_{i,j} \in \Omega} \gamma_{i,j,e}^{E} \tag{15}$$

It is worth noting that in the cooperative scenario, eavesdroppers cooperate via exchanging messages, thus making it possible in principle for a SDN Controller to monitor, detect and localise them.

4. Numerical Results

In this section, we evaluate the performance achievable in the previously introduced scenarios to increase the physical layer security. In order to evaluate the secrecy rate performance, the numerical simulations are carried out by using the Matlab framework. We consider an outdoor multi-RIS system covering an area of size 100 m $\times$ 50 m with a single antenna transmitting source, one receiving Base Station with N = 32 antennas, eight RISs deployed in fixed locations and E_{N_e} eavesdroppers randomly distributed.

As shown in Table 1, we assume $M = 10^3$, $P_{tx} = 26$ dBm, $\sigma^2 = -94$ dBm, the carrier frequency is set at 6 GHz; the source is located at (40,10) m and the base station is located at (25,50) m. In all heuristics, we consider $\xi = 1$, except in HEU4, where we set $\xi = 0.55$ as a reasonable value in our approach. In HEU2, we consider $\rho = 0.25$.Finally, we present both scenarios (c) and (nc). (a) represents the worst case scenario, since the eavesdroppers collaborate to combine the wiretapped signals and consequently C_{Ω}^{E} is larger, even though detection and location processes through the SDN Controller are more affordable.

Table 1. Parameters for numerical simulation.

Parameter	Value	Description
M	10^3	Number of reflecting elements
P_{tx}	26 dBm	Transmit power of user equipment
σ^2	-94 dBm	Noise power
f_c	6 GHz	Carrier frequency
ζ	1	In all heuristics except HEU4, where we set $\zeta = 0.55$. Reasonable values for our approach, as a result of an empirical optimization.
ρ	0.25	In HEU2, as a reasonable value for our approach, and as a result of an empirical optimization.

In Figure 2, we consider the performance related to scenario (c). The average secrecy rate versus the number of eavesdroppers is shown according to the proposed heuristics and compared with (i) the optimal solution (exhaustive search) and (ii) the case where the basic SPA is applied to a graph only to maximise the e2e capacity (blind search). We do the same for scenario (nc) in Figure 3. It can be pointed out that the more complex the heuristics, the closer their performance is to the optimal solution, while HEU2 is similar to the blind search, which simply ignores the presence of eavesdroppers. As expected, the performances in scenario (c) are worse. In Figure 2, the gap between the optimal solution and the best proposed heuristics is larger then Figure 3. In this instance, eavesdroppers are not able to communicate with each other, so the wiretapped SNR will be smaller, benefitting the secrecy rate.

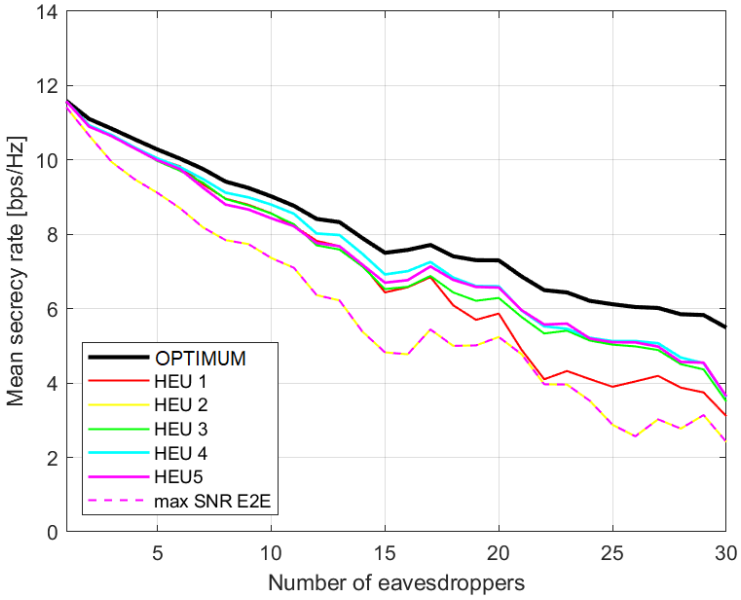

Figure 2. Average secrecy rate with regards to number of eavesdroppers for different approaches. Scenario (c) with cooperative eavesdroppers.

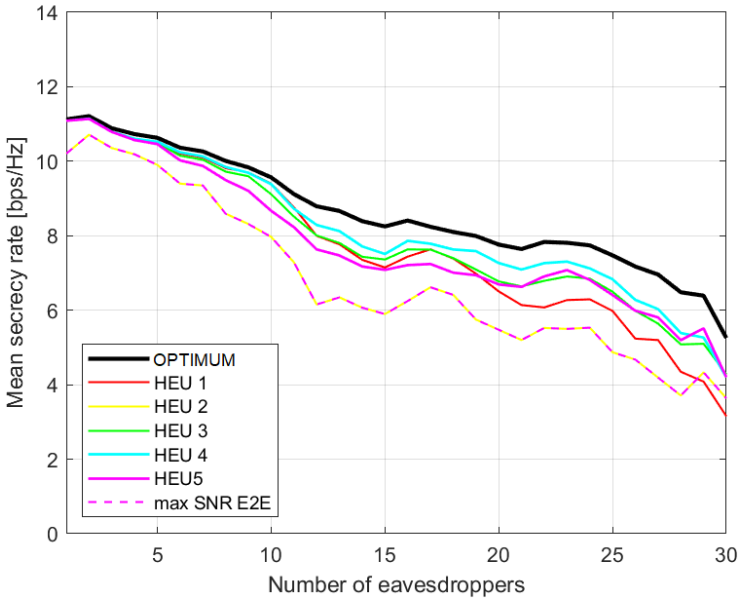

Figure 3. Average secrecy rate with regards to number of eavesdroppers for different approaches. Scenario (nc) with non-cooperative eavesdroppers.

This result is confirmed by Figures 4 and 5, which show the related secrecy rate loss with regards to the optimum performance, defined as:

$$\frac{C^S_{opt} - C^S_{HEU_i}}{C^S_{opt}}, i = 1, 2, \ldots, 5$$

Here, it is more evident that HEU4 is closer to the optimum one. In addition, as expected, in all of the considered cases, the secrecy performance decreases when the number of eavesdroppers increases. Moreover, it is worth noting that both HEU1 and HEU2 are computationally lighter than HEU3, HEU4 and HEU5, since they require fewer operations to evaluate the graph weights. Moreover, it is worth noting that both HEU1 and HEU2 are computationally lighter than HEU3, HEU4 and HEU5, since they require fewer operations

to evaluate the graph weights. While HEU1 and HEU2 simply inspect the coverage area of a connection link for the presence of one or more eavesdroppers, the other heuristics build on this procedure. Therefore, they require more computational and storage resources. In particular, HEU1 and HEU2 do not require one to evaluate SNR for each eavesdropper, but only to estimate the presence of eavesdroppers in the link coverage area.

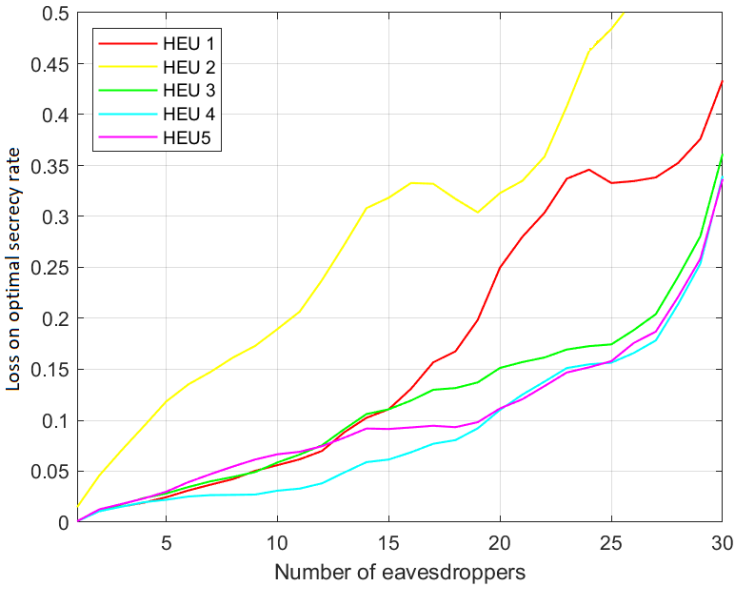

Figure 4. Percentage loss over optimum secrecy rate. Scenario (c) with cooperative eavesdroppers.

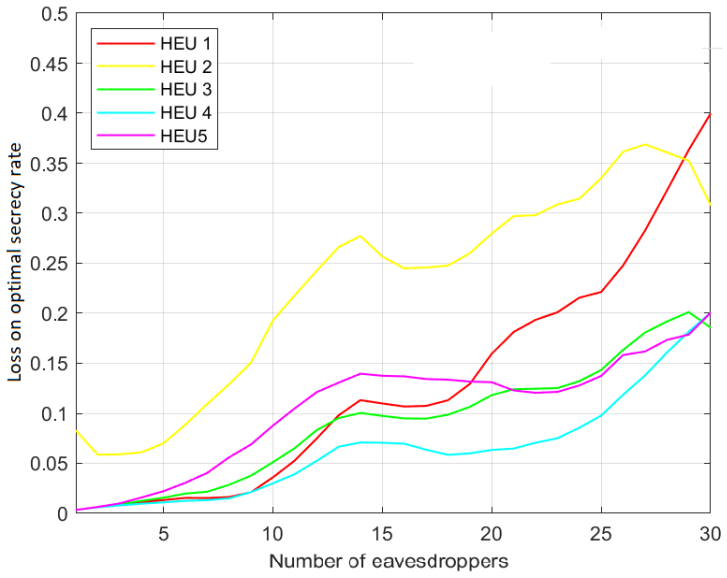

Figure 5. Percentage loss over optimum secrecy rate. Scenario (nc) with non-cooperative eavesdroppers.

In order to correctly represent the network topology with a weighted graph, the SDN Controller needs to estimate the location of the eavesdroppers using a positioning protocol. To take into account the impact of this procedure, we introduce in the previous analysed case an uncertainty on the position of eavesdroppers modelled as a uniformly randomly distributed variable with a mean value equal to 1.5 m. In Figure 6, we examine the impact on the secrecy rate by considering five eavesdroppers: it can be noticed that reducing the accuracy on the localisation makes it harder to avoid the effect of the eavesdroppers, so that the overall performance worsens.

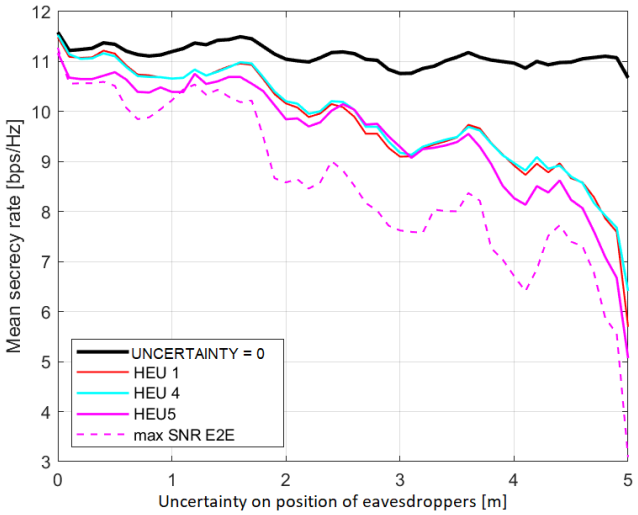

Figure 6. Average secrecy rate versus uncertainty on eavesdroppers' position.

On a further note, to generalise the investigation of the security related performance, we introduced three concurrent mobile users in an urban scenario, whose mobility patterns are shown in Figure 7, where two of them move longitudinally (blue and green lines) and the other one follows a zig-zag trajectory (black line), all at a pedestrian speed. In addition to that, $E_{N_e} = 20$ fixed eavesdroppers are introduced. To handle this case, we endow the SDN Controller with a scheduler module which adopts a weighted round robin policy; specifically, users are served by the SDN Controller in a static exclusive order (user 1, user 2 and user 3) and they cannot share any RIS within their e2e path. The average secrecy rate achieved by each user is, respectively, $C_1^S = 10.8138, C_2^S = 9.9317, C_3^S = 9.9996$.

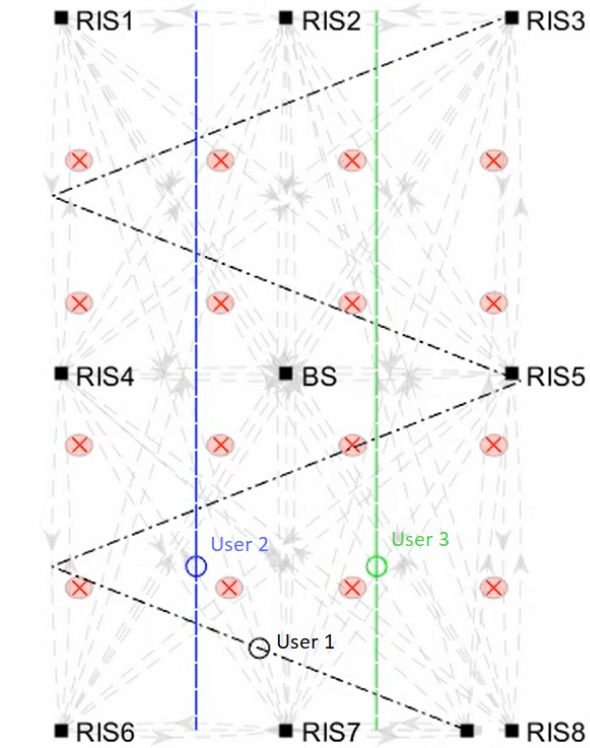

Figure 7. Multi-user composite mobility pattern: two users follow a linear trajectory (blue and green lines), while the third user follows a zig-zag trajectory (black line).

In Figure 8, the instantaneous secrecy rate is plotted as a function of simulation time; it can be pointed out that the scenario geometry and the position of eavesdroppers influence the performance. In particular, as one user passes close to an eavesdropper, the secrecy rate decreases, whereas its performance improves for more favourable positions along its path.

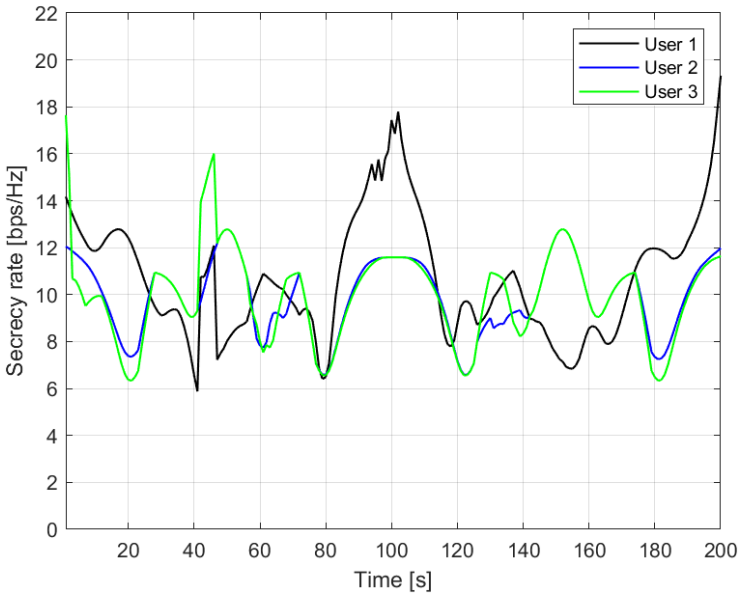

Figure 8. Average secrecy rate versus simulated time.

5. Conclusions

This paper focuses on integrating a multi-RIS system within an SDN-oriented architecture to improve the PLS performance via a secure data forwarding strategy. Specifically, the SDN Controller is able (i) to detect the presence of possible eavesdroppers and (ii) to perform the best path selection involving multiple RISs with the aim of improving the secrecy rate at the destination. We apply this framework to uplink communications from a source to a destination (mainly a base station), where multiple RISs are involved. We supposed that eavesdroppers adopt a collaborative approach to intercept the source signal; however, this allows the SDN Controller to detect their presence and, in turn, to react and dynamically select another path through the multiple RISs. To this goal, an equivalent graph theory model is first provided to evaluate the optimal solution, and, then different heuristics are proposed, trading off complexity and PLS performance, in order to evaluate the more suitable multi-beam routing strategy. Numerical results point out the effectiveness of the proposed approach by the increasing in the number of eavesdroppers. Furthermore, the security performance is investigated for a specific user mobility pattern in a pedestrian scenario.

Author Contributions: Conceptualization, F.C. and L.P.; methodology, F.C., L.P. and A.D.; software, A.D.; validation, F.C., L.P. and A.D.; investigation, F.C. and L.P.; data curation, A.D.; writing—original draft preparation, F.C., A.D. and L.P.; writing—review and editing, F.C., A.D. and L.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001—program "RESTART").

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

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

References

1. Wu, Q.; Zhang, R. Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network. *IEEE Commun. Manag.* **2020**, *58*, 106–112. [CrossRef]
2. Hashida, H.; Kawamoto, Y.; Kato, N. Intelligent Reflecting Surface Placement Optimization in Air-Ground Communication Networks Toward 6G. *IEEE Wirel. Commun.* **2020**, *27*, 146–151. [CrossRef]
3. Zhao, J.; Chen, R.; Cai, K.; Zhu, Y.; Han, Z. RIS-Assisted Air-to-Ground Communications with Non-Orthogonal Multiple Access. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021; pp. 1–6. [CrossRef]
4. Yang, F.; Pitchappa, P.; Wang, N. Terahertz Reconfigurable Intelligent Surfaces (RISs) for 6G Communication Links. *Micromachines* **2022**, *13*, 285. [CrossRef] [PubMed]
5. Wu, Q.; Zhang, S.; Zheng, B.; You, C.; Zhang, R. Intelligent Reflecting Surface-Aided Wireless Communications: A Tutorial. *IEEE Trans. Commun.* **2021**, *69*, 3313–3351. [CrossRef]
6. 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]
7. Do, D.T.; Le, A.T.; Ha, N.D.X.; Dao, N.N. Physical layer security for Internet of Things via reconfigurable intelligent surface. *Future Gener. Comput. Syst.* **2022**, *126*, 330–339. [CrossRef]
8. Mishra, P.; Puthal, D.; Tiwary, M.; Mohanty, S.P. Software Defined IoT Systems: Properties, State of the Art, and Future Research. *IEEE Wirel. Commun.* **2019**, *26*, 64–71. [CrossRef]
9. Liaskos, C.; Mamatas, L.; Pourdamghani, A.; Tsioliaridou, A.; Ioannidis, S.; Pitsillides, A.; Schmid, S.; Akyildiz, I.F. Software-Defined Reconfigurable Intelligent Surfaces: From Theory to End-to-End Implementation. *Proc. IEEE* **2022**, *110*, 1466–1493. [CrossRef]
10. Mei, W.; Zhang, R. Cooperative Beam Routing for Multi-IRS Aided Communication. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 426–430. [CrossRef]
11. Lei, X.; Wu, M.; Zhou, F.; Tang, X.; Hu, R.Q.; Fan, P. Reconfigurable Intelligent Surface-Based Symbiotic Radio for 6G: Design, Challenges, and Opportunities. *IEEE Wirel. Commun.* **2021**, *28*, 210–216. [CrossRef]
12. Mei, W.; Zheng, B.; You, C.; Zhang, R. Intelligent Reflecting Surface-Aided Wireless Networks: From Single-Reflection to Multireflection Design and Optimization. *Proc. IEEE* **2022**, *110*, 1380–1400. [CrossRef]
13. Brilli, L.; Pecorella, T.; Pierucci, L.; Fantacci, R. A Novel 6LoWPAN-ND Extension to Enhance Privacy in IEEE 802.15.4 Networks. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6. [CrossRef]
14. Wang, H.; Zhu, T.; Li, D.; Jiang, R.; Wang, X.; Xu, Y. Intelligent Attack Analysis for IRS Communications with Incomplete Information. *Procedia Comput. Sci.* **2022**, *202*, 269–276.
15. Liu, X.; Tao, Y.; Zhao, C.; Sun, Z. Detect Pilot Spoofing Attack for Intelligent Reflecting Surface Assisted Systems. *IEEE Access* **2021**, *9*, 19228–19237. [CrossRef]
16. Hu, L.; Li, G.; Luo, H.; Hu, A. On the RIS Manipulating Attack and Its Countermeasures in Physical-layer Key Generation. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Virtual, 27–30 September 2021; pp. 1–5. [CrossRef]
17. Yu, X.; Xu, D.; Schober, R. Enabling secure wireless communications via intelligent reflecting surfaces. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; IEEE: New York, NY, USA, 2019; pp. 1–6.
18. Mukherjee, A.; Kumar, V.; Tran, L.N. Secrecy Rate Maximization for Intelligent Reflecting Surface Assisted MIMOME Wiretap Channels. In Proceedings of the MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November–2 December 2021; IEEE: New York, NY, USA, 2021; pp. 261–266.
19. Mathioudakis, F.; Liaskos, C.; Tsioliaridou, A.; Nie, S.; Pitsillides, A.; Ioannidis, S.; Akyildiz, I. Advanced Physical-layer Security as an App in Programmable Wireless Environments. In Proceedings of the 2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Atlanta, GA, USA, 26–29 May 2020; pp. 1–5. [CrossRef]
20. Luo, J.; Wang, F.; Wang, S.; Wang, H.; Wang, D. Reconfigurable Intelligent Surface: Reflection Design Against Passive Eavesdropping. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 3350–3364. [CrossRef]
21. Wei, Z.; Guo, W.; Li, B. A Multi-Eavesdropper Scheme Against RIS Secured LoS-Dominated Channel. *IEEE Commun. Lett.* **2022**, *26*, 1221–1225. [CrossRef]
22. Tourrilhes, J.; Sharma, P.; Banerjee, S.; Pettit, J. SDN and OpenFlow Evolution: A Standards Perspective. *Computer* **2014**, *47*, 22–29. [CrossRef]

23. Liaskos, C.; Tsioliaridou, A.; Pitilakis, A.; Pirialakos, G.; Tsilipakos, O.; Tasolamprou, A.; Kantartzis, N.; Ioannidis, S.; Kafesaki, M.; Pitsillides, A.; et al. Joint compressed sensing and manipulation of wireless emissions with intelligent surfaces. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; IEEE: New York, NY, USA, 2019; pp. 318–325.
24. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]
25. Björnson, E.; Sanguinetti, L. Power Scaling Laws and Near-Field Behaviors of Massive MIMO and Intelligent Reflecting Surfaces. *IEEE Open J. Commun. Soc.* **2020**, *1*, 1306–1324. [CrossRef]