Article

Autonomous Navigation of a Solar-Powered UAV for Secure Communication in Urban Environments with Eavesdropping Avoidance

Hailong Huang and **Andrey V. Savkin** *

School of Electrical Engineering and Telecommunications, University of New South Wales,
Sydney NSW 2052, Australia; hailong.huang@unsw.edu.au
* Correspondence: a.savkin@unsw.edu.au

Abstract: This paper considers the navigation of a solar-powered unmanned aerial vehicle (UAV) for securing the communication with an intended ground node in the presence of eavesdroppers in urban environments. To complete this task, the UAV needs to not only fly safely in the complex urban environment, but also take into account the communication performance with the intended node and eavesdroppers. To this end, we formulate a multi-objective optimization problem to plan the UAV path. This problem jointly considers the maximization of the residual energy of the solar-powered UAV at the end of the mission, the maximization of the time period in which the UAV can securely communicate with the intended node and the minimization of the time to reach the destination. We pay attention to the impact of the buildings in the urban environments, which may block the transmitted signals and also create some shadow region where the UAV cannot harvest energy. A Rapidly-exploring Random Tree (RRT) based path planning scheme is presented. This scheme captures the nonlinear UAV motion model, and is computationally efficient considering the randomness nature. From the generated tree, a set of possible paths can be found. We evaluate the security of the wireless communication, compute the overall energy consumption as well as the harvested amount for each path and calculate the time to complete the flight. Compared to a general RRT scheme, the proposed method enables a large time window for the UAV to securely transmit data.

Keywords: unmanned aerial vehicles (UAVs); solar-powered UAVs; wireless communication; secure communication; eavesdropping; security; unmanned aerial vehicles; navigation; autonomous systems; path planning; rapidly-exploring random tree navigation

1. Introduction

Unmanned Aerial Vehicles (UAVs) have been recognized as a new entity in the future wireless communication systems, and UAVs can play different roles in different applications. They can be receivers of navigating commands sent by remote control units when they carry out missions like surveillance [1], and the receivers of the sensory data sent by sensor nodes when they are employed to collect data in wireless sensor networks [2]. They can also be transmitters to send sensory data to desired nodes [3]. UAVs often outperform their counterparts such as unmanned ground robots thanks to their excellent mobility and high probability of having Line-of-Sight (LoS) with other objects. However, the LoS feature can also pose threats in communication security. Consider the case where a UAV needs to send its sensory data to a remote ground unit. When there are eavesdroppers in presence, the transmitted data can be easily collected by the eavesdroppers, which may lead to information leakage [4].

There are different approaches to protecting the wireless communication of UAVs. A common approach is encryption, which encodes a message in such a way that only authorized parties can access it and those who are not authorized cannot. However, if the eavesdropper somehow knows the encoding/decoding schemes used by the transmitter/receiver, it can extract information from the collected data.

In recent years, physical layer security has attracted much attention. The basic idea is to enlarge the received rate at the desired node and reduce that at the eavesdropper, so that even if the eavesdropper could receive the transmitted data, it cannot be decoded successfully. Following this approach, Ref. [5] considers the optimal deployment of a UAV to secure the communication between the UAV and a ground node in the presence of eavesdroppers. Ref. [6] jointly optimizes the trajectory of the UAV and the transmit power of the ground node to avoid eavesdropping. Ref. [7] takes into account the No-fly zone (NFZ), such as the controlled areas with the risks of being targeted by ground-to-air missiles, in the process of path planning. The difference lies in the consideration of the negative impacts of the NFZ. The NFZ in that reference refers to some restricted areas such as some controlled air space, and it does not block the LoS between the UAV and the intended node and that between the UAV and the sun. However, the NFZ considered in the current paper refers to some tall buildings in urban environments. They may not only block the signal propagation but also prevent the UAV from harvesting energy. Then, the avoidance of the NFZ is similar to the conventional obstacle avoidance. Beyond the case with the stationary ground node and the stationary eavesdroppers, the more challenging situation with a moving ground node and moving eavesdroppers is investigated in [3], and the 3D UAV trajectory planning problem has been studied.

One limitation of many publications on this topic is that they consider a free environment, where the UAV, the ground node and the eavesdroppers can have LoS [8]. They may not work in urban environments, since the LoS can be blocked by tall buildings [9]. For example, NFZ considered in [7] refers to some restricted areas such as some controlled air spaces, and they do not block the LoS between the UAV and the intended node and that between the UAV and the sun. Then, the avoidance of the NFZ is similar to the conventional collision avoidance. Moreover, the publication [7], as well as many other papers in this area, does not consider scenarios with some tall buildings in urban environments which may not only block the signal propagation but also prevent the UAV from harvesting energy. Another limitation is that the energy efficiency has not been comprehensively considered in these publications. Solar-powered UAVs have been employed to prolong the operation duration. However, the negative impacts of the urban environment on energy harvesting have not been well considered.

This paper considers using a solar-powered UAV to secure the wireless communication with an intended node in the presence of eavesdroppers in an urban environment, see Figure 1. The term of securing the wireless communication means that the intended ground node is able to decode the data sent by the UAV while the eavesdroppers cannot. The aforementioned limitations are taken into account in this paper. Specifically, we consider a given urban environment, where the positions and shapes of the buildings are known. Any building is modelled by a prism. Then, the UAV should fly outside the prisms. Additionally, given the positions of the UAV and the ground node, we can easily verify whether they have LoS. Similarly, the LoS between the UAV and the sun can be checked, which makes the estimation of the harvested energy amount accurate.

We focus on the UAV path planning problem by taking into account the solar energy harvesting and the instantaneous communication protection. We formulate a multi-objective optimization model to maximize the residual energy of the UAV at the end of the mission, maximize the time period in which the communications between the UAV and the intended node is secure, and minimize the time to arrive at the destination. To address this problem, we propose a Rapidly-exploring Random Tree (RRT) [10] based scheme. This RRT-based scheme captures the nonlinear UAV motion model, and is also computationally efficient considering the randomness nature. From the generated tree, a set of possible paths that end up in a given region, such as the UAV depot (this is to facilitate the

UAV collection after the mission, see Figure 1) can be found. For each possible path, we can verify the security of the wireless communication and compute the overall energy consumption, the harvested amount and the time to complete the path. We then pick the path with the maximum value of a joint metric from the feasible paths. The main contributions of this paper are the new problem formulation and the new RRT-based path planning method. We test the effectiveness of the proposed method via computer simulations. By comparing with a benchmark method, the proposed method guarantees the secure wireless communication with the intended node and prevents eavesdropping in a large time window.
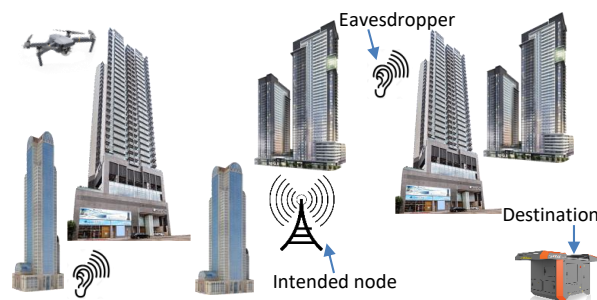

Figure 1. Illustration of the considered scenario.

Related Work

The problem considered in this paper belongs to the classical path planning and secure communication. In this subsection, we first briefly review the typical approaches and then clarify the difference of our work against the existing publications.

Graph search based approaches are the well-studied ones for global path planning. They generally need the environment to be modelled by a graph, where a possible link between two vertices of the graph is associated with a weight indicating the cost or time to traverse the link. Then, many popular graph search algorithms, such as Dijkstra's algorithm [11] and A* algorithm [12], can be applied to compute the shortest path between a start vertex and a destination vertex.

Tangent graph based approaches are another type of tools to compute globally optimal paths. For a non-holonomic robot, say a Dubins car [13], its angular speed is upper bounded (its minimum turning radius is lower bounded). Then, given the obstacles in an environment, the obstacles can be modelled by circles whose radius should be no smaller than the robot minimum turning radius. Furthermore, a set of tangent lines can be added to link a pair of obstacle circles. The generated graph is called the tangent graph and the robot's path in this tangent graph consists of a number of straight line segments and a number of arcs on the obstacle circle [14,15].

Optimization algorithms are often used for the path planning problem. Typical optimization algorithms that have been used include but not limited to the particle swarm optimization [16], the genetic algorithm [17], differential evolution [18] gravitational search algorithm [19]. The methods are in general based on a pool of possible trajectories, and follow some updating rules until the optimal path is obtained. A shortcoming of this class of approaches is that they may converge slowly in normal path planning problems.

The RRT scheme, a randomized method, usually performs well in terms of the computational efficiency [10]. This method is based on the construction of a random tree of possible actions connecting the start position and the destination. When a node of the tree reaches the destination, a feasible path from the start point to the destination can then be identified. Thanks to its computational efficiency, the RRT scheme is promising to be applied in online path planning. The main task is to dynamically grow and manage the tree. For example, when the destination changes or when mobile obstacles come into proximity, some new nodes may be added to the tree and some existing nodes of the tree may be cut to avoid collision [20,21]. Moreover, beyond the general RRT framework, some heuristic methods

have been proposed to guide the tree growth [22,23], which may generate nearly optimal paths while remaining with a probabilistic planning setting.

The considered application scenario is about secure wireless communication. Secure communication is not a new issue in wireless communication, and there are approaches to protecting the security. However, the wireless communication of UAVs brings new challenges. The most important feature is the high probability of LoS with not only the intended node but also malicious nodes (i.e., eavesdroppers). As aforementioned, some strategies have been proposed to increase the security capacity of the UAV wireless communication. Refs. [3,6,7] focus on the UAV mobility management to increase the received rate at the intended node and decrease that at the eavesdroppers. Besides this approach, another class of approaches employs UAVs as jammers [24–26]. Specifically, Ref. [24] considers the optimization of the UAV jammer's trajectory and transmission power. Ref. [25] further takes into account the user scheduling to maximize the secrecy rate. Ref. [26] proposes a strategy where two UAVs send confidential messages to their respective intended node by sharing the same spectrum. A cooperation strategy is designed to maximize the system secrecy rate.

The path planning problem considered in this paper is for a UAV, whose path is 3D. However, most graph search based approaches and tangent graph based approaches focus on the 2D path planning problems. Additionally, the considered application scenario, i.e., securing the wireless communication between the solar-powered UAV and a ground node in the presence of eavesdroppers in urban environments, introduces some new requirements on the UAV path. Specifically, the UAV should ensure that the ground node can successfully decode the sent data while the eavesdroppers cannot decode the sent data.

The rest of this paper is organized as follows. Section 2 presents the system models and states the problem of interest. Section 3 presents the proposed path planning method. Computer simulations are shown in Section 4. Finally, conclusions are given in Section 5.

2. Problem Statement

In this section, we first present the system model and then formulate the problem of interest. The main symbols used in the paper and their meanings are summarized in Table 1.

Table 1. Symbols and meanings.

Symbol	Meaning
$p(t)$	Position of the UAV
$v(t)$	Linear speed on xy-plane
$w(t)$	Angular speed on xy-plane
$u(t)$	Vertical speed
$\theta(t)$	Heading of the UAV on xy-plane
$D(t)$	Drag of the UAV
$f(t)$	Thrust of the UAV
m	The mass of the UAV
P^{sun}	Energy harvesting power of the UAV
$P(t)$	Energy consuming power of the UAV
$Q(t)$	Residual energy of the UAV
$\mathcal{T}$	The random tree
$\mathcal{R}$	The set of paths in $\mathcal{T}$

2.1. UAV Model

We consider a solar-powered UAV that flies in an urban environment. We denote $p(t) = [x(t), y(t), z(t)]$ as the coordinates of the UAV at time t. The following model is used to describe the UAV's motion (This 3D UAV motion model is extended from a 2D model [27] where a forward speed and an angular speed are the control inputs. Beyond these two control inputs, we consider the vertical speed such that the UAV can adjust its altitude):

$$
\begin{cases}
\dot{x}(t) = v(t)\cos(\theta(t)), \\
\dot{y}(t) = v(t)\sin(\theta(t)), \\
\dot{\theta}(t) = w(t), \\
\dot{z}(t) = u(t), \\
\dot{u}(t) = \frac{F(t)-D(t)}{m}.
\end{cases}
\tag{1}
$$

where $\theta(t)$ is the heading of the UAV with respect to the *x*-axis; $v(t)$, $\omega(t)$ and $u(t)$ are its linear horizontal, angular and vertical speeds, respectively; m is the mass of the UAV; and $D(t)$ and $F(t)$ are the drag and thrust forces, respectively. The model (1) and its slight modifications have been widely used to describe the motion of aircraft, wheeled robots, and missiles, see, e.g., [27,28].

The drag force is computed as follows [29]:

$$
D(t) = \frac{1}{2}\rho C_D A v^2(t),
\tag{2}
$$

where ρ is the air density, A is the area of the solar cells of the UAV, $C_D = C_{D0} + \frac{C_L^2}{\varepsilon \pi R_a}$ is the coefficient of drag, C_{D0} is the parasitic drag coefficient, $C_L = \frac{2mg}{\rho A v^2(t)}$ is the coefficient of lift, R_a is the aspect ratio of the wing, and ε is the Oswald efficiency factor.

Moreover, the following constraints are enforced on the UAV's movement at any time *t*:

$$
\begin{cases}
Z^{min} \le z(t) \le Z^{max}, \\
0 < v(t) \le V^{max}, \\
-\Omega^{max} \le w(t) \le \Omega^{max}, \\
-U^{max} \le u(t) \le U^{max}, \\
0 \le F(t) \le F^{max},
\end{cases}
\tag{3}
$$

where the constants $0 < Z^{min} < Z^{max}$ specify the allowed deployment altitude, the constants V^{max}, Ω^{max} and U^{max} specify the bounds of the corresponding speeds of the UAV, and the constant F^{max} is the maximum allowed thrust force.

2.2. Energy Harvesting and Consuming

The solar-powered UAV can harvest energy from the sun. Let P^{sun} denote the harvesting, which can be computed by [29]

$$
P^{sun} = \eta A \cos \phi,
\tag{4}
$$

where η is the efficiency of the solar cell, and ϕ is the incidence angle. ϕ depends on the azimuth angle α_z and the elevation angle α_e of the sun, and α_z and α_e are time-varying in the daytime. Then, ϕ also varies with time.

When flying, the UAV also consumes energy. Let $P(t)$ denote the energy consumption power, and it is calculated by

$$
P(t) = \frac{F(t)v(t)}{\eta_{prop}},
\tag{5}
$$

where η_{prop} is the efficiency of the propeller, and $v(t) = \sqrt{v^2(t) + u^2(t)}$.

Let $Q(t)$ denote the residual energy of the battery of the UAV, which is upper bounded by the capacity Q^{max}. We have

$$
\dot{Q}(t) = P^{sun} - P(t).
\tag{6}
$$

2.3. No-Fly-Zone (NFZ)

There are some buildings in the considered environment, and they occupy some space where the UAV is prohibited. We call this space the NFZ. We model each building by the smallest prism enclosing this building. Each prism has two parallel and congruent bases and a number of flat sides; see Figure 2. The shape of the bases depends on the building. All the prisms are assumed to have one base on the xy-plane and the other above the xy-plane. All the sides of the prisms are assumed to be perpendicular to the xy-plane. Each prism can be characterized by three parameters: (1) an I-by-2 matrix Ξ, (2) an I-by-1 vector ξ, and (3) a scalar h. The integer I depends on the shape of the base. Any point (x, y, z) inside a prism satisfies the following condition:

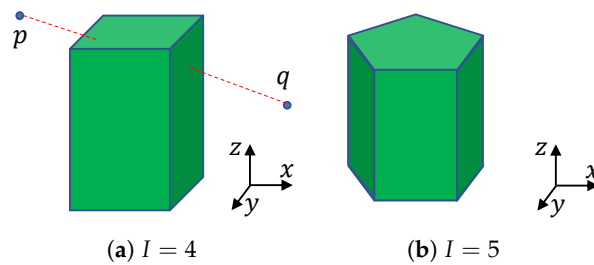$$\begin{cases} \Xi \begin{bmatrix} x \\ y \end{bmatrix} \leq \xi, \\ 0 \leq z \leq h. \end{cases} \tag{7}$$

(a) $I = 4$　　　　　　　　　**(b)** $I = 5$

Figure 2. Prisms.

Given the environment, all the buildings have the corresponding Ξ, ξ and h. At any time, the UAV must not be at a position that satisfies (7). The problem of avoidance of NFZ is similar in spirit to the problem of avoiding collisions with steady obstacles, see e.g., [30,31] and references therein.

2.4. Line-of-Sight (LoS)

In addition to NFZ, the tall buildings may block the wireless channels. Moreover, they may create some shadow regions where the solar-powered UAV cannot harvest energy from the sun. Thus, it is necessary to have an evaluation model to verify whether the LoS condition is available between the UAV and the ground node, and the UAV and the sun.

Suppose that the two entities locate at p and q, respectively. The straight line segment between p and q can be written as follows:

$$\begin{cases} x = x_q + \alpha\tau, \\ y = y_q + \beta\tau, \\ z = z_q + \gamma\tau, \\ \min\{x_p, x_q\} \leq x_q + \alpha\tau \leq \max\{x_p, x_q\}, \end{cases} \tag{8}$$

where $q = (x_q, y_q, z_q)$, $p = (x_p, y_p, z_p)$, and $\frac{\vec{pq}}{\|\vec{pq}\|} = (\alpha, \beta, \gamma)$. The last inequality specifies the range of the free variable τ.

Whether the LoS between p and q is blocked by a prism depends on whether the line segment (8) and corresponding the prism (7) have any intersection points. To this end, we can solve Equations (7) and (8) for each prism. If there are solutions to any prism, the LoS is blocked (see Figure 2); otherwise, the LoS between p and q are not blocked.

Note that, to verify if the LoS between the UAV and the sun is blocked, we need to have the sun's location. Let V be the unit vector representing the sunlight direction. With the azimuth angle α_z and the

elevation angle α_e of the sun, the vector $V = [\cos \alpha_e \cos \alpha_z, \cos \alpha_e \sin \alpha_z, - \sin \alpha_z]^T$ [32]. We can imagine that the sun locates at $q_{sun} = p - V\tau$, where τ takes a large value so that the sun is very far from p. Let $b(t)$ be a binary variable: $b(t) = 1$, if the UAV and the sun have LoS; $b(t) = 0$, otherwise. With the symbol $b(t)$, the residual energy of the UAV should be calculated according to the following equation:

$$\dot{Q}(t) = P^{sun}b(t) - P(t). \tag{9}$$

For the safety of operation, at any time, the residual energy of UAV i cannot be smaller than the threshold Q^{min}:

$$Q(t) \geq Q^{min}. \tag{10}$$

2.5. Secure Communication

Let (x_i, y_i) be the position of the ground node i, and $i = 0, \dots, N$. When $i = 0$, the node refers to the intended ground node, while when $i = 1, \dots N$, the node is an eavesdropper. The intended node is a legitimate node, and it makes sense for the UAV to know its location. For the locations of eavesdroppers, following [33], we assume that they can be measured by an optical camera or a synthetic aperture radar. Here, N is the number of eavesdroppers. Let $d_i(t)$ denote the Euclidean distance between the UAV and node i at time t:

$$d_i(t) = \sqrt{(x(t) - x_i)^2 + (y(t) - y_i)^2 + z(t)^2}.$$

Denote $\kappa(d)$ as a function measuring the communication performance. In the free space, $\kappa(d)$ is a decreasing function of d. In the well-known Friis' formula [34], when the transmitter and the receiver are d apart from each other with LoS, the received signal-to-noise ratio (SNR) is $\kappa(d) = \frac{a}{d^2}$, where a is a given positive constant. Let the binary variable $l_i(t)$ indicate whether the UAV has LoS with node i at t: $l_i(t) = 1$, if they have LoS; $l_i(t) = 0$, otherwise. Let $\kappa(d_i(t), l_i(t))$ denote the SNR between the UAV and node i. $\kappa(d_i(t), l_i(t))$ is defined as follows:

$$\kappa(d_i(t), l_i(t)) = \frac{al_i(t)}{d_i^2(t)}. \tag{11}$$

To secure the wireless communication between the UAV and the intended node, a set of constraints are considered below. The first requirement is that the received SNR at the intended node is no smaller than a threshold γ_c:

$$\kappa(d_0(t), l_0(t)) \geq \gamma_c. \tag{12}$$

This is to ensure that the node can successfully recover the received data at time t. Secondly, the received SNR at each eavesdropper must be no larger than a threshold γ_e ($\gamma_e < \gamma_c$):

$$\kappa(d_i(t), l_i(t)) \leq \gamma_e, \tag{13}$$

for all $i = 1, \dots, N$. This is to ensure that any eavesdropper i cannot recover the captured data.

In general, the constraint (12) requires the UAV to be close enough to the intended node and have LoS with the node, whereas the constraint (13) requires the UAV to be far enough from the eavesdroppers or have no LoS with the eavesdropper. We note that, in cases where several eavesdroppers are located closely, they may block the path for the UAV, and there may not exist a feasible path satisfying (12) and (13). To avoid being eavesdropped, the UAV stops sending data in these cases. We also note that the buildings can reflect wireless signals. This can make the received SNR larger than the value computed by (11). Since the Non-LoS propagation model is complex and out of the scope of this paper, we do not go far in this direction. It is worth pointing out that, if such a model is available, our method can be extended straightforwardly by updating Equation (11).

2.6. Problem Statement

Suppose the UAV operation period is $[0, T]$. The UAV's initial position is $p(0)$ and the initial energy is $Q(0)$. Let $\mathcal{D}$ denote a given bounded and connected destination set. Let T^* denote the time instant at which the UAV arrives at $\mathcal{D}$. In other words, T^* is the time needed to complete the flight. During the period $[0, T^*]$, the UAV transmits confidential data to the intended ground node if the eavesdropping can be avoided. The path planning problem under investigation is to jointly optimize three objectives: minimizing T^*, maximizing the final residual energy $Q(T^*)$ and maximizing the total time the UAV can securely transmit data by finding a sequence of control inputs $v(t), \omega(t), u(t)$. Formally, the problem is formulated as follows:

$$\min_{v(t), \omega(t), u(t)} T^* \tag{14}$$

$$\max_{v(t), \omega(t), u(t)} Q(T^*) \tag{15}$$

$$\max_{v(t), \omega(t), u(t)} \int_0^{T^*} l_0(t) dt \tag{16}$$

subject to

$$Q^{min} \le Q(t) \le Q^{max}, \ \forall t \in [0, T], \tag{17}$$

$$(x(T), y(T)) \in \mathcal{D}, \tag{18}$$

Equations (3), (12) and (13) hold, while (7) does not hold for any prism at any time.

Different from the classic path planning problem which targets on a collision-free path for a mobile robot to safely and quickly arrive at the destination [35], the problem of interest also aims at maximizing the residual energy of the solar-powered UAV and total time duration in which the UAV can securely communicate with the intended node.

3. RRT-Based Path Planning

The problem under consideration cannot be solved by convex optimization tools. The reason lies in the non-convex constraints of (12) and (13), the non-smoothness of the residual energy model (9) due to the shadow region created by the buildings, and the nonlinear UAV model (1). Moreover, the minimization of the flight time and the optimization of the UAV path are difficult to decouple. To overcome these difficulties, we develop an RRT-based path planning method. As aforementioned, the RRT method can easily tackle the nonlinear UAV model, secure communication requirements and the NFZ by randomly generating samples.

Let $\mathcal{T}$ be the random tree. $\mathcal{T}$ consists of a number of vertices. Each vertex is associated with the status of the UAV including its position, heading, linear speed, vertical speed, angular speed, and whether it has LoS with the sun, the intended node and the eavesdroppers. It is assumed that the UAV knows the locations of the intended node, the eavesdroppers and the sun's direction vector; otherwise, it is impossible to guarantee the secure communication and verify the LoS with these entities. The operation period is descritized by a sampling interval δ. This sampling interval restricts the movement of the UAV in a single step.

Following the framework of RRT, we can keep generating random samples between the allowed altitudes Z^{min} and Z^{max} in the environment. For any sample, we look for the closest vertex in the tree $\mathcal{T}$ to this sample. We generate a new vertex with appropriate control inputs satisfying (3), so that the new vertex cannot be closer to the sample after a movement in the interval δ. The new vertex is added to the tree $\mathcal{T}$ if constraint (7) does not hold for any prism in the considered environment. Otherwise, this vertex is deleted. If the candidate vertex is added to the tree $\mathcal{T}$, we further verify whether constraints (12) and (13) hold and if the LoS exists between this vertex and the sun. When a given number of vertices fall into the destination set $\mathcal{D}$, we can terminate the tree growing process.

From the generated random tree $\mathcal{T}$, we can find a number of paths to evaluate. For finding the paths, we consider each of the vertices falling into the destination set $\mathcal{D}$. Specifically, from this vertex, we look backward to identify its parent vertex until the root (i.e., the vertex indicating the initial position of the UAV) is reached. Let $\mathcal{R}$ denote the set of paths found by the above procedure. These paths are feasible for the UAV, since any vertex is generated by appropriate control inputs. Additionally, any vertex is outside the prisms (which is safe for the UAV). The last step is to make the final selection of the path. As the considered problem is a multi-objective problem, we select the path that maximizes the following metric:

$$\max_{\mathcal{P} \in \mathcal{R}} \frac{Q(\mathcal{P}) \int_0^{T(\mathcal{P})} l_0(t)dt}{T(\mathcal{P})}, \tag{19}$$

where $T(\mathcal{P})$ represents the UAV flight time following the path $\mathcal{P}$, $Q(\mathcal{P})$ represents the residual energy of the UAV, and $\int_0^{T(\mathcal{P})} l_0(t)dt$ gives the total time in which the transmission by the UAV is secure. It is worth pointing out that (19) is not the only metric to evaluate a path. An alternative can be a linear combination of the three objectives. Since we need to choose two weights in that kind of metric, we use (19) in this paper to evaluate a path. After evaluating all the possible paths, we can finally find the one having the maximum value of (19). All the procedures of this method are summarized in Figure 3.
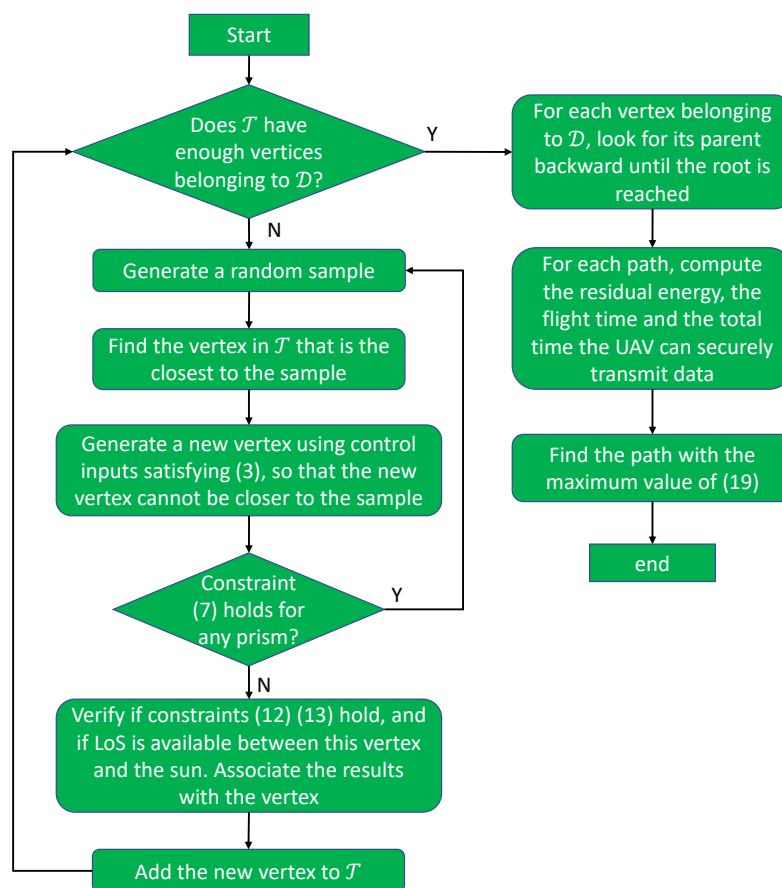

Figure 3. Flow chart of the RRT-based path planning method.

It is worth pointing out that, although the currently considered scenario involves a stationary intended node, the proposed method can also be used for the cases with a moving intended node. Thanks to the computational efficiency, the task of adding new vertices and removing old vertices can be done online.

4. Simulation Results

The effectiveness of the proposed method is shown in this section. The parameters used in the computer simulations are shown in Table 2. We create an urban environment with a number of buildings, as shown in Figure 4. There is an intended node marked by a diamond. There are three eavesdroppers deployed on the roof of some buildings, marked by the black stars. The destination set $\mathcal{D}$ is marked by a blue disk. Our UAV starts from $p(0)$. Applying the proposed scheme, the UAV path is generated in less than one second. We show the UAV path in Figure 5. We plot the results of the residual energy, the flight time and the time window in which the communication is secure in Figure 6. The UAV completes the flight to reach the destination set $\mathcal{D}$ in 102 seconds, and the residual energy is 100 units. In 34% of this period, the UAV can securely communicate with the intended node.

Table 2. Parameters.

Parameter	Value	Parameter	Value
V_{max}	20 m/s	Ω_{max}	1 rad/s
U_{max}	2 m/s	Z_{max}	100 m
Z_{min}	20 m	V	$[0.8, 0, -0.6]$
E_{max}	200	E_{min}	20
δ	1 s	T	150 s
m	0.5 kg	ρ	1.29 kg/m^3
A	0.5 m^2	C_{D_0}	0.011
ϵ	0.1	R_a	10
η_{prop}	0.1	g	9.8 kg^{-2} m^2
a	2.5×10^5	$p(0)$	$[0, 0, 60]$
γ_c	1	γ_e	0.8
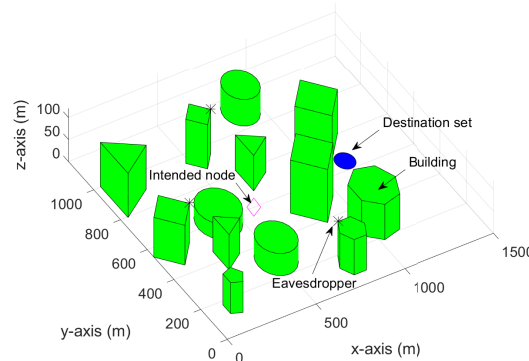
Figure 4. The simulated urban environment.

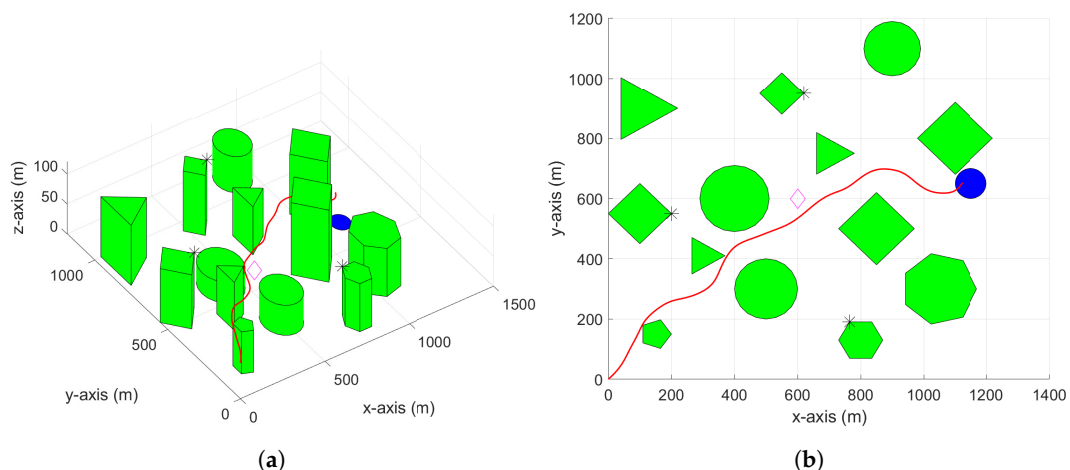(**a**)   (**b**)

Figure 5. 3D (**a**) and 2D (**b**) views of the UAV trajectory by the proposed method.
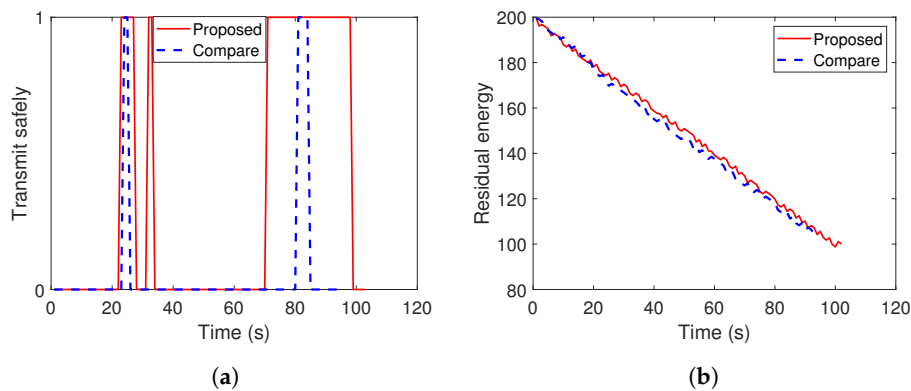
Figure 6. Simulation results of when the UAV can securely transmit data (**a**) and the residual energy (**b**) in case 1.

For comparison, we replace the path selection metric by the minimization of the flight time, and apply it to the above case. The obtained UAV path by this compared method is shown in Figure 7. The corresponding results are shown in Figure 6. Following this path, the UAV arrives at the destination set in 92 seconds, see Figure 6b. The residual energy is 110 units. This path outperforms the above one in these two terms. However, as seen from Figure 6a, this path enables the secure communication in only 6% of the period, which is much less than the proposed method.
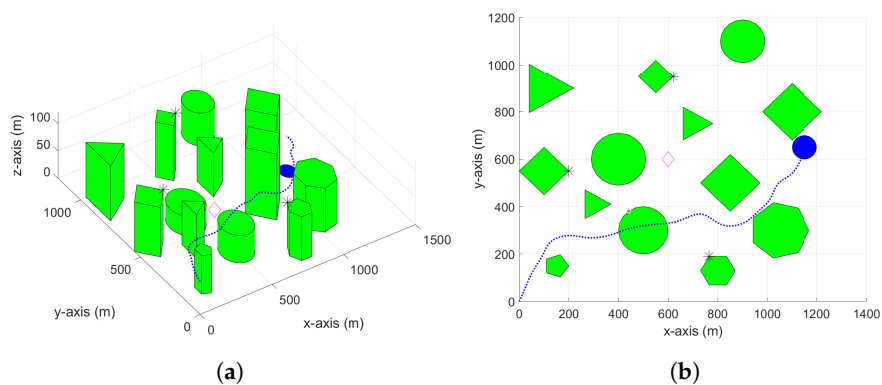
Figure 7. 3D (**a**) and 2D (**b**) views of the UAV trajectory by the compared method.

The proposed method is not restricted to any environment. We create another urban environment and then apply the proposed method and the compared method to construct the UAV path. The UAV path obtained by the proposed method is shown in Figure 8 with both 2D and 3D views. The time window in which the UAV can securely transmit and the residual energy are shown in Figure 9. Similar to the results in Figure 6, the proposed method obtains the UAV path that has a similar flight time and similar residual energy, but a much larger time window for secure communication than the compared method.
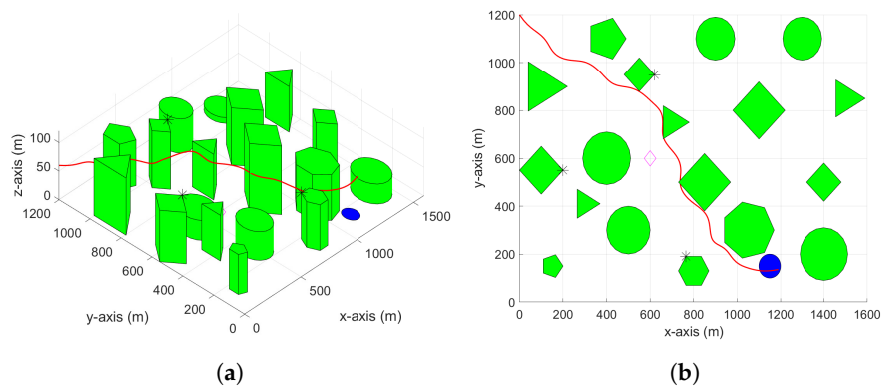
(**a**)   (**b**)

Figure 8. 3D (**a**) and 2D (**b**) views of the UAV trajectory by the proposed method in another urban environment.

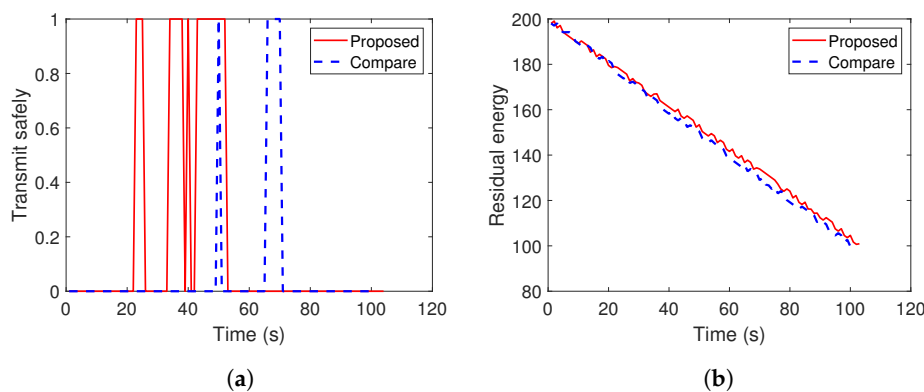(**a**)   (**b**)

Figure 9. Simulation results of when the UAV can securely transmit data (**a**) and the residual energy (**b**) in case 2.

5. Conclusions

In this paper, we considered the application of using a solar-powered UAV for securing the communication with a ground node in the presence of eavesdroppers in urban environments. A path planning problem was formulated with the objective of jointly maximizing the residual energy of the solar-powered UAV at the end of the mission, maximizing the time period in which the UAV can securely communicate with the intended node and minimizing the time to reach the destination. A special attention was paid to the impact of the buildings in the urban environments, which may block the transmitted signals and also create some shadow region where the UAV cannot harvest energy. An RRT-based path planning scheme was presented. The effectiveness of the proposed scheme was tested via computer simulations. The comparison with a general selection of the path to minimize the energy consumption showed that the path generated by the proposed scheme enables the UAV to securely transmit data to the intended node in a larger time window. One of our future efforts is to explore a UAV team for the purpose of securing the communication, where one of the UAVs transmits data and others jam the eavesdroppers. Another research direction is to extend the current work to dynamic environments with either the mobile intended node or moving obstacles in the environment. Then, we will focus on the re-planning of the UAV path.

Author Contributions: Formal analysis, H.H.; funding acquisition, A.V.S.; investigation, H.H.; methodology, H.H.; project administration, A.V.S.; supervision, A.V.S.; writing—original draft, H.H.; writing—review & editing, A.V.S. All authors have read and agreed to the published version of the manuscript.

References

1. Ghaddar, A.; Merei, A. EAOA: Energy-Aware Grid-Based 3D-Obstacle Avoidance in Coverage Path Planning for UAVs. *Future Internet* **2020**, *12*, 29. [CrossRef]
2. Huang, H.; Savkin, A.V. Towards the internet of flying robots: A survey. *Sensors* **2018**, *18*, 4038. [CrossRef] [PubMed]
3. Savkin, A.V.; Huang, H.; Ni, W. Securing UAV Communication in the Presence of Stationary or Mobile Eavesdroppers via Online 3D Trajectory Planning. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1211–1215. [CrossRef]
4. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. *Future Internet* **2020**, *12*, 65. [CrossRef]
5. Wang, D.; Bai, B.; Zhang, G.; Han, Z. Optimal Placement of Low-Altitude Aerial Base Station for Securing Communications. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 869–872. [CrossRef]
6. Cui, M.; Zhang, G.; Wu, Q.; Ng, D.W.K. Robust Trajectory and Transmit Power Design for Secure UAV Communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 9042–9046. [CrossRef]
7. Huang, H.; Savkin, A.V.; Ni, W. Energy-Efficient 3D Navigation of a Solar-Powered UAV for Secure Communication in the Presence of Eavesdroppers and No-Fly Zones. *Energies* **2020**, *13*, 1445. [CrossRef]
8. Yuan, X.; Feng, Z.; Ni, W.; Liu, R.P.; Zhang, J.A.; Xu, W. Secrecy Performance of Terrestrial Radio Links under Collaborative Aerial Eavesdropping. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 604–619. [CrossRef]
9. Huang, H.; Savkin, A.V.; Ding, M.; Kaafar, M.A. Optimized deployment of drone base station to improve user experience in cellular networks. *J. Netw. Comput. Appl.* **2019**, *144*, 49–58. [CrossRef]
10. LaValle, S.M.; Kuffner, J.J., Jr. Randomized kinodynamic planning. *Int. J. Robot. Res.* **2001**, *20*, 378–400. [CrossRef]
11. Dijkstra, E.W. A note on two problems in connexion with graphs. *Numer. Math.* **1959**, *1*, 269–271. [CrossRef]
12. Hart, P.E.; Nilsson, N.J.; Raphael, B. A formal basis for the heuristic determination of minimum cost paths. *IEEE Trans. Syst. Sci. Cybern.* **1968**, *4*, 100–107. [CrossRef]
13. Dubins, L.E. On curves of minimal length with a constraint on average curvature, and with prescribed initial and terminal positions and tangents. *Am. J. Math.* **1957**, *79*, 497–516. [CrossRef]
14. Savkin, A.V.; Hoy, M. Reactive and the shortest path navigation of a wheeled mobile robot in cluttered environments. *Robotica* **2013**, *31*, 323. [CrossRef]
15. Savkin, A.V.; Huang, H. Optimal Aircraft Planar Navigation in Static Threat Environments. *IEEE Trans. Aerosp. Electron. Syst.* **2017**, *53*, 2413–2426. [CrossRef]
16. Zhang, Y.; Gong, D.W.; Zhang, J.H. Robot path planning in uncertain environment using multi-objective particle swarm optimization. *Neurocomputing* **2013**, *103*, 172–185. [CrossRef]
17. Roberge, V.; Tarbouchi, M.; Labonté, G. Comparison of parallel genetic algorithm and particle swarm optimization for real-time UAV path planning. *IEEE Trans. Ind. Inform.* **2012**, *9*, 132–141. [CrossRef]
18. Shen, Y.; Wang, Y. Operating point optimization of auxiliary power unit using adaptive multi-objective differential evolution algorithm. *IEEE Trans. Ind. Electron.* **2016**, *64*, 115–124. [CrossRef]
19. Rashedi, E.; Nezamabadi-Pour, H.; Saryazdi, S. GSA: A gravitational search algorithm. *Inf. Sci.* **2009**, *179*, 2232–2248. [CrossRef]
20. Ferguson, D.; Stentz, A. Anytime RRTs. In Proceedings of the 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems, Beijing, China, 9–15 October 2006; pp. 5369–5375.
21. Otte, M.; Frazzoli, E. RRTX: Asymptotically optimal single-query sampling-based motion planning with quick replanning. *Int. J. Robot. Res.* **2016**, *35*, 797–822. [CrossRef]
22. Ko, I.; Kim, B.; Park, F.C. VF-RRT: Introducing optimization into randomized motion planning. In Proceedings of the 2013 9th Asian Control Conference (ASCC), Istanbul, Turkey, 23–26 June 2013; pp. 1–5.
23. Wang, J.; Meng, M.Q.; Khatib, O. EB-RRT: Optimal Motion Planning for Mobile Robots. *IEEE Trans. Autom. Sci. Eng.* **2020**. [CrossRef]
24. Li, A.; Wu, Q.; Zhang, R. UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 181–184. [CrossRef]
25. Cai, Y.; Cui, F.; Shi, Q.; Zhao, M.; Li, G.Y. Dual-UAV-enabled secure communications: Joint trajectory design and user scheduling. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1972–1985. [CrossRef]
26. Li, Y.; Zhang, R.; Zhang, J.; Yang, L. Cooperative Jamming via Spectrum Sharing for Secure UAV Communications. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 326–330. [CrossRef]

27. Kang, Y.; Hedrick, J.K. Linear tracking for a fixed-wing UAV using nonlinear model predictive control. *IEEE Trans. Control Syst. Technol.* **2009**, *17*, 1202–1210. [CrossRef]

28. Li, H.; Savkin, A.V. Wireless sensor network based navigation of micro flying robots in the industrial internet of things. *IEEE Trans. Ind. Informatics* **2018**, *14*, 3524–3533. [CrossRef]

29. Klesh, A.T.; Kabamba, P.T. Solar-powered aircraft: Energy-optimal path planning and perpetual endurance. *J. Guid. Control. Dyn.* **2009**, *32*, 1320–1329. [CrossRef]

30. Matveev, A.S.; Teimoori, H.; Savkin, A.V. A method for guidance and control of an autonomous vehicle in problems of border patrolling and obstacle avoidance. *Automatica* **2011**, *47*, 515–524. [CrossRef]

31. Hoy, M.; Matveev, A.S.; Savkin, A.V. Algorithms for collision-free navigation of mobile robots in complex cluttered environments: A survey. *Robotica* **2015**, *33*, 463–497. [CrossRef]

32. Wu, J.; Wang, H.; Li, N.; Yao, P.; Huang, Y.; Su, Z.; Yu, Y. Distributed trajectory optimization for multiple solar-powered UAVs target tracking in urban environment by Adaptive Grasshopper Optimization Algorithm. *Aerosp. Sci. Technol.* **2017**, *70*, 497–510. [CrossRef]

33. Zhang, G.; Wu, Q.; Cui, M.; Zhang, R. Securing UAV communications via joint trajectory and power control. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1376–1389. [CrossRef]

34. Friis, H.T. A note on a simple transmission formula. *Proc. IRE* **1946**, *34*, 254–256. [CrossRef]

35. Saeed., R.A.; Recupero., D.R. Path Planning of a Mobile Robot in Grid Space using Boundary Node Method. In Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics, Prague, Czech Republic, 29–31 July 2019; pp. 159–166.