A local communication model for improving stealth in collaborative UAV networks.

Nícolas Pereira Borges [1], Cinara Guellner Ghedini[1], Carlos H. C. Ribeiro[1]

[1]Computer Science Division. Aeronautics Institute of Technology.
São José dos Campos, SP, Brazil

nicolas@ita.br, cinarag@gmail.br, carlos@ita.br

Abstract. *Some missions, mainly military, can be performed by unmanned aerial vehicles (UAVs), which cooperate to achieve a common objective. Considering that the detection of UAVs can compromise a mission, this work proposes a local communication model to improve the stealth of collaborative UAV networks. The model supports mechanisms for detection and avoidance of threats. Once a threat is detected, a policy to turn off the UAVs communication radars is applied. It also comprise mechanisms for connectivity maintenance and collision avoidance. For 150 simulation scenarios, we empirically show that, with the proposed model, as the number of UAVs increases, exposure to threats decreases.*

1. Introduction

In the last years, the number of applications relying on unmanned aerial vehicles (UAVs) have significantly increased, since they are capable of carrying out missions that are too dangerous or too difficult for a human. The term collaborative UAV networks refers to applications where UAVs act cooperatively to achieve a common goal, exchanging time-critical local information [Kim and Seo 2012]. Some applications are critical, especially for military purposes where the UAVs need to perform missions in hostile environments, and as a consequence taking actions to reduce their exposure to threats [Kacena 1995]. In the context of this paper, threats refer to static land surveillance radars.

There are two possible approaches to reduce the exposure of UAVs to threats, focusing either on the physical or communication level. The first approach implies that the information exchanged by the UAVs in a communication network should have a low probability of being detected by a threat [Bash et al. 2013]. The second approach specifies that not only the communication among the UAVs should provide a low detection probability but also the UAVs themselves should exhibit a low probability of being physically detected, named stealthy dissemination and physical stealth, respectively [Turgut et al. 2009]. According to [Kacena 1995], stealth can be defined as a combination of techniques and technologies that can include radar, acoustic, visual, smoke and contrails, that aims at increasing the enemy's difficulty in detecting, tracking, guiding or predicting their future position in space.

One factor that impacts stealthy dissemination is the type of communication used by the UAVs. One of the most common approaches of communication between UAVs are radars that operate in high frequency, such as High Frequency Radar (HF), Very High Frequency Radar (VHF), Ultra High Frequency Radar (UHF) and or even Microwave. This kind of communication can be detected by a Radar Warning Receiver (RWR). Another factor that impacts the stealth level of UAVs is their physical features: some UAVs possess features and equipments aimed at improving their stealth level, however, these equipments are expensive and can improve, but not ensure, stealth all along the flight.

One of the open issues in collaborative UAV networks is the modelling of a UAV network, in which the UAVs work collaboratively to dynamically improve its stealthiness.

In this sense, this works aims at developing a parametrized model of a UAV network that works cooperatively to improve its physical stealthiness while improving the chance of the UAVs remain connected, which, in turn improves the mission's success probability. The model considers a high frequency radar approach and a local communication model evaluated through simulated scenarios composed by a UAV network, and a start and a goal positions. Due the uncertainty of the scenario, unexpected threats are normally detected on the flight path, thus, UAVs must detect and evade from them. A potential application is a ground crew that needs support to operate in a hostile environment without information about the position of the enemy's surveillance radar. These radars can trigger fire-control radars (FCR), which are able to destroy the airplanes, making the mission too risky for manned planes. Besides, if a stealth UAV is shot down, the financial loss will be probably large. The proposed solution is mainly important for a set of UAVs that do not possess physical stealth features to improve the mission success probability.

The rest of this paper is organized as follows. Section 2 presents the related work. Section 3 presents the methodology of this research, describing the proposed model. The experiment and results are detailed in Section 4. Finally, Section 5 presents the conclusions.

2. Related Work

There are several researches regarding collaborative UAV networks and stealthiness in the literature. However, the proposed approach cannot be easily compared to others because stealth approaches on collaborative UAV networks have not been deeply addressed yet. The most related approach proposes a model to improve mission success rate, based on a stealth approach that consists in a policy for turning off radars [Borges et al. 2016]. As in our work, the UAVs need to detect and avoid threats. On the other hand, it is based on a global communication model instead of a local one, which is not applicable in a real-world scenario, as the UAVS can only share information with others that are in the same communication range. In addition, it does not consider mechanisms aiming at ensuring network connectivity and avoiding collision among the UAVs.

Regarding UAVs and stealth, [He and Dai 2013] propose a 3D-based collaborative approach, based on genetic algorithms for improving stealth by optimizing attitude angles, because yaw and pitch angles affects the probability of an UAV being detected by an enemy radar. [Zhen et al. 2014] propose a real-time replanning algorithm that allows UAVs, starting from different positions, to arrive at the destination at the same same in a dynamic threat scenario. [Kothari et al. 2009] present a model to generate paths for multiple UAVs in real time, from a given starting locations to goal locations in the presence of static and dynamic obstacles, generating non-conflicting paths in obstacle rich environments. In this work, only information related to the collision avoidance mechanism is exchanged among the UAVs. Besides, obstacles are physical, instead of represented by forbidden zones as in the case of radars.

[Turgut et al. 2009] present a way to quantify the stealth of a sensor node (stealth level) with a numerical metric and propose a local model, based on a try and bounce (TAB) approach, where the nodes that are exposed, i.e. whose have a stealth level lower than a threshold, do not reply to messages sent by other UAVs, meaning that their are in a threat region.

Regarding the control strategy for connectivity maintenance, we consider a technique for maintaining the overall network connectivity through a decentralized estimation of the algebraic connectivity [Sabattini et al. 2013a]. The connectivity maintenance framework can be enhanced to consider additional objectives. In particular, as shown in [Lee et al. 2013], the concept of generalized connectivity can be utilized for simultaneously guaranteeing connectivity maintenance and collision avoidance among the UAVs.

3. Stealth improvement model

This section describes the model that aims at improving the stealth of the UAVs, using an approach based on a combined control law that includes connectivity maintenance, collision avoidance and flight path planning mechanisms.

3.1. Scenario

Consider a scenario composed exclusively of UAVs and threats. Each UAV is able to communicate with other UAVs within the same communication radius, which results in a communication topology that can be represented by an undirected graph, where each UAV is a vertex and each communication link is an edge. Every time a UAV want to share some information with all connected vertices, a Depth-First Search procedure is applied [Tarjan 1972]. A UAV cannot share information with those that are in different connected components.

Figure 1 presents the general scenario considered here. Threats are represented by circles, which are defined by their center position (threat position) and its radar range. The UAVs have to flight from the starting location to the goal using a collaborative approach to detect and avoid threats with an active stealth policy. It is assumed that all UAVs are flying at the same height, therefore, the developed model is two-dimensional. Each UAV can only detect threats when its RWR detects the radio emissions from the threats. In turn, the threat can detect UAVs by its radar range.

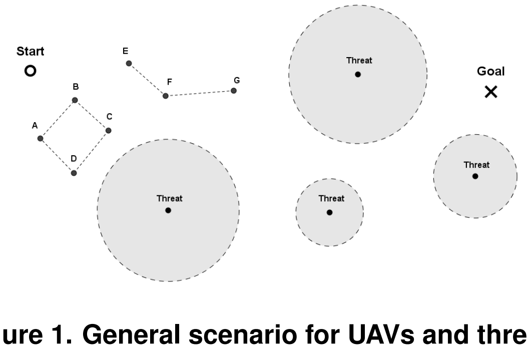

Figure 1. General scenario for UAVs and threats.

3.2. Flight Formation

There are several flight formations used on conventional airplanes, however some of them are not applicable to UAV scenarios because in the context of unmanned planes, there is no concept of pilot's vision range. The only mechanism usually present in UAVs are a high frequency radar for communication and the RWR. Therefore, the flight formation can only consider these variables. According to [Giulietti et al. 2000], in a typical flight formation there are the roles of leader and wingmans. In this context, the wingman follows the trajectory of the leader, taking the other aircrafts as a reference to keep its own position inside the formation. The leader's responsibility is to define the trajectory to the goal. In a rigid flying formation, inter-aircraft distances must be kept constant.

In hostile environments, where the UAVs do not have information about the threat locations, exposure should be reduced. In this sense, there is a flight formation, named trail, that is used to air-to-ground attack on dangerous environments. Figure 2 presents an example of the trail formation The numbers above the UAVs correspond to their formation ranking (*id*). The UAV with *id* 1 is the leader of the a connected component and responsible for calculating the trajectory to the goal, while the others are the wingmans, which always calculate the trajectory to the successor, i.e. the UAV that have $id = a - 1$, where a is the current UAV i. The problem with such formation is that in a ground-to-air situation, the UAVs are not supported by any other UAV in the formation, consequently, if one of them fails or is hit by an enemy, the network can become disconnected.

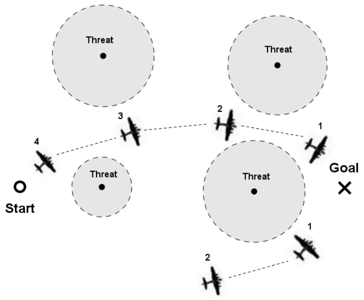

Figure 2. Trail formation for UAVs.

For generating this formation, the UAV that is chosen to be the leader of a connected component of the network is the one that is closest to goal. The other UAVs' ranking are generated based on the length of their path to the leader: the closer a UAV is to the leader, the lower is its ranking position. The formation ranking, however, cannot be static because the connection between two UAVs may be lost, so it is essential for the communication that failures can be detected and recovery as quick as possible [Giulietti et al. 2000]. In our context, faults can be defined as the loss of connection between two UAVs.

Another possible scenario where it is necessary to update the flight formation is when there are two connected components that are close enough to be merged. For updating a flight formation, the number of connected UAVs within a formation ranking 1 is verified. If there are more than one, the leader will be the UAV with formation ranking 1 that have the shortest path to the goal. The other UAVs rank indexes are updated based on their distance to the new leader, as previously described. Figure 3 illustrates a connection failure (on the left) and the resulting ranking reconfiguration (on the right). On the other hand, Figure 4 illustrates how two flight formations are merged.

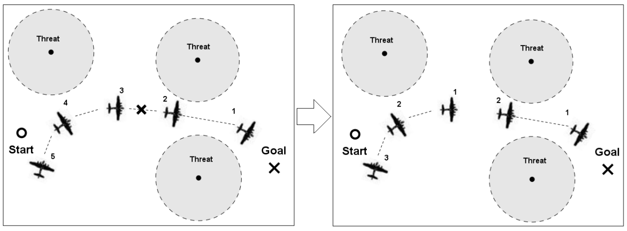

Figure 3. Connection fault example.

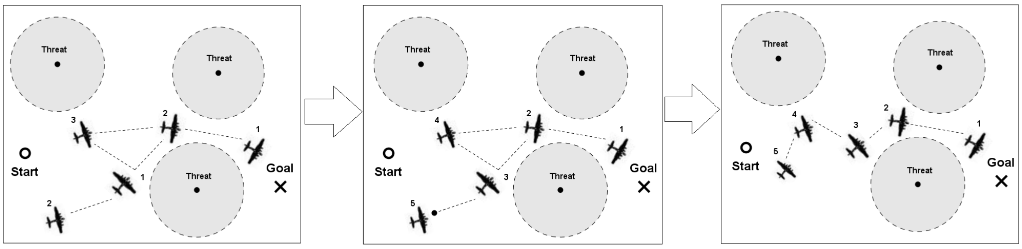

Figure 4. Merge of two flight formations.

3.3. Flight path planning

Flying toward the target, the UAVs perform dynamic detection of the threats. Once a threat is detected, it is necessary to plan a trajectory in order to avoid this region. There are several approaches for planning UAVs paths, based on genetic algorithm [He and Dai 2013], neural networks [Glasius et al. 1995], and heuristics, such as the TangentBug [Breitenmoser et al. 2010].

Regarding obstacle avoidance, such as threats, one of the most frequently work referred in the literature is the Rapidly-Exploring Random Tree (RRT) [LaValle 1998], [Kothari et al. 2009], [Zhen et al. 2014]. The main idea behind RRT is to build a tree of feasible trajectories towards randomly generated intermediate goal points, by extending branches that will not pass through any forbidden region. RRT produces as output a path composed of consecutive lines, which can then be processed in order to optimize the resulting path. Figure 5 presents the output of the RRT algorithm, given a start and a target point: the lines generated by RRT (branches), the path and the optimized path (reduced path).

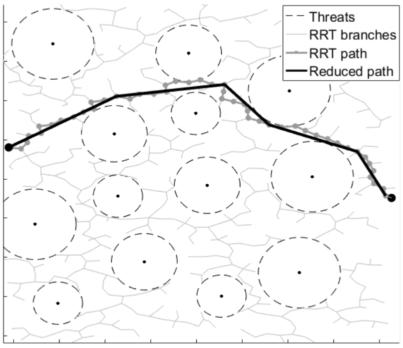

Figure 5. The RRT path planning operation.

A characteristic of RRT is that it provides only a linear piecewise representation of the trajectory. Thus, it may be necessary to apply a path smoothing method for generating feasible trajectories. Common path smoothing methods, such as B-Splines, cannot be used because they are usually ineffective for avoiding threat regions, as highlighted in [Borges et al. 2016]. The smoothing procedure considered here is based on an algorithm proposed to perform horizontal segmentation of highways [Coelho et al. 2015]. It considers that at each time the angular coefficient varies, a set of points in a neighborhood is selected and, on this set of points, a circle is fit [Coope 1993], resulting in the radius and center coordinates of the circle that best adjust to the set of points. These points are then replaced by the generated circle.

3.4. Connectivity maintenance and collision avoidance

According to [Basu and Redi 2004], whenever a group of robots is performing a task, such as providing airborne relay capabilities in disaster or military contexts, it is essential to initiate and maintain communications to ensure timely and efficient task completion. Given that the connectivity maintenance of UAVs is critical, in addition to RRT, it is also necessary to use an approach to maintain the UAVs connected while flying thought the trajectory. In this sense, [Sabattini et al. 2013b] presents an approach to solve the global connectivity problem in a decentralized manner through the algebraic connectivity property. The connectivity maintenance mechanism is able to perform in the presence of additional objectives such as the collision avoidance, as demonstrated in [Robuffo Giordano et al. 2013]. In our context, the obstacles are the UAVs themselves. This approach was already successfully applied in the context of multi-robot systems [Ghedini et al. 2016].

The combined mechanism assumes that each UAV have a goal to reach during a time interval. Given the path generated by the RRT, the goal of the UAVs is the first position in the path planning, i.e., the position that UAVs would move at moment $t+1$, where t is the current time, if they only use the RRT. Based on this, the position of the UAV i, at a moment t, can be defined as:

$$P_i(t) = \alpha(t)w_\alpha + \beta(t)w_\beta + \gamma(t)w_\gamma, \quad (1)$$

where α, β and γ are the gains for the algebraic connectivity (w_α), the collision avoidance (w_β) and the path planning (w_γ), respectively.

The parameters for the algebraic connectivity and collision avoidance are the speed of the UAVs, their radar's range and their current positions. The UAVs positions are calculated for a time interval, with a partial differential equations solver. The UAV positions P are simulated for a time interval $[0,t]$ and its next position will be $P(t)$.

3.5. Stealth

There are different models for intrusion detection that, according to [Abdel-Fattah et al. 2010] can be classified into three groups: Standalone, Distributed and Cooperative and Hierarchical. This work adopts the distributed and collaborative approach. However, for stealthiness purposes, the UAVs that detect a threat cannot continue sharing information while in a critical area, otherwise the content of the communication can be heard by the enemy, which could compromise the entire mission. The solution for this problem was based on TAB communication protocol, presented in [Turgut et al. 2009]. In TAB, if a node is in a critical area, it does not communicate with other nodes. If other nodes cannot communicate with a single node, they assume that the region where that node is should be avoided. Thus, in our scenario, if an UAV detects a threat, it turns off its radar to reduce the exposure to threat.

The act of turning off the radar not guarantee that the UAVs will not be detected by the enemies radar. However the probability of being detected by a threat will be reduced because threats cannot detect the UAV by the waves emitted by its communication radar. At this moment, we are considering that the UAV, before turning off the radar, informs its direct neighbours about the threat. The probability of this communication be detected exists, but is low, due to the fact that the UAVs radar's range are normally lower than the threats radar's range. The threats, considered at this work as surveillance radars, operate in a low frequency band, consequently the time spent to process the echo of the UAV will be longer than the time spent by the UAV to detect the threat. Currently, we are not addressing the effect of variation of RWR range, so we assume that the RWR range is the same range used for communication between UAVs. This communication policy can be improved by an approach where the neighbours of the UAV (that turned off the radar) estimate the threat position instead of receive this information by the exposed UAV.

Besides detecting the presence of threats, the RWR can also estimate its position using two different kind of approaches: the Direction Find (DF), which consists in analyze the direction of the electromagnetic wave emitted, and the Time Difference of Arrival (TDOA), which consists in verify the time between the electromagnetic pulses [Exército 2009].

For the last, after detecting and estimating the threats position, the region that the UAVs will try to avoid is represented by a circle, centered in the position of the threat, with radius equal to the sum of the distance between UAV and the threat with the communication range of the UAVs. As the RWR is a passive receiver, it is not necessary to turn off this equipment. Therefore, the UAV will only turn on its radar again when the RWR does not detect the presence of any threat. The act of turning off the communication radar will not ensure that the UAV will become undetectable to the enemy radar, but will reduce its exposure. The UAV that turned its radar off, will trace a line to the goal, and flight on this direction while is inside a threat region.

4. Simulations

The experiments aims at verifying the impact of the insertion of a stealth policy in a collaborative network of UAVs with a local communication model. For this, three datasets containing 50 scenarios each were generated: one with 5 threats, one with 10 threats and other with 15 threats. These scenarios have approximately 3,500 meters distance from the starting to the goal position. The threats range varying from 200 to 400 meters, while the UAVs range for communication and RWR is 150 meters. The number of edges used in RRT, for each path planning, was 1500.

The first analysis consists of evaluating the exposure of UAVs to threats, varying the number of UAVs. The results show that the average distance traveled by the UAVs exposed to threats decreases when the number of UAVs increases. This occurs because the number of UAVs performing the detection of the threats increases, therefore, the UAVs that are in the back of formation tend to be less exposed than those in the front, making the UAV's average distance traveled in region exposed to threats to reduce. Figure 6 presents the average distance traveled in threat regions for different amounts of UAVs for scenarios with different number of threats.

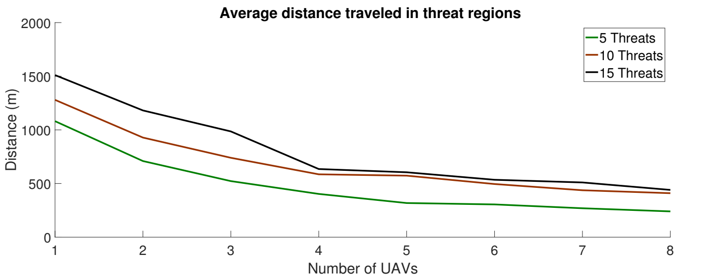

Figure 6. Average distance traveled in threat regions.

Another important aspect to analyse is the fraction of scenarios in which at least a single UAV reached the goal without been detected by any threat. This analysis is justified because, depending on the kind of mission, the non-exposure of only one single UAV can define the mission success. Figure 7 shows the results for different number of UAVs in the network. Notice that the number of UAVs significantly impacts the UAVs stealthiness: when the number of UAVs increases, the fraction of scenarios where at least one UAV reached the goal without being detected significantly increases. For all the three datasets, the percentage varies, on average, from 0 to approximately 84% by changing the number of UAVs from 1 to 8. Moreover, the number of UAVs necessary to improve the chance of at least one UAVs remaining undetected during the mission increases according to the number of threats in the scenario.

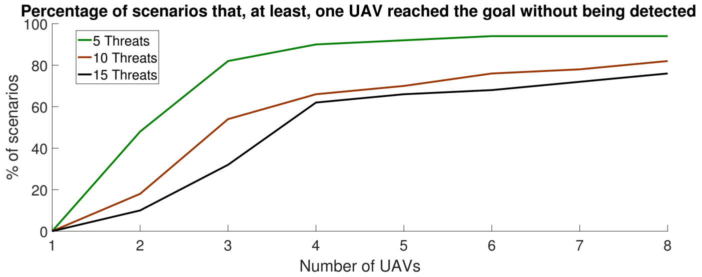

Figure 7. Total amount of scenarios that, at least, one UAV reached the goal without being detected by any threat.

5. Conclusion

In this paper, a model to improve stealth in collaborative UAV networks under local communication constraints was presented. The strategy employed a flight formation in trail, which is used in real-world scenarios, such as for air-to-ground attack on hostile environments. Besides that, a combined control law that includes path planning, collision avoidance and connectivity maintenance was also implemented. The findings show that UAVs working collaboratively can be stealthier than a single UAV and, as long as the number of UAVs increases, their exposure to threats may decrease, leading one or more UAVs to fly without being detected.

For future work, instead of considering only surveillance radar as threats, the inclusion of fire-control radars can be explored. In the proposed scenario the UAVs only need to reach the goal, but a model that considers a back home functionality taking into account energy management is a worthwhile research. Considering that the possibility of exchanging information impacts the performance of the stealth approach, the addition of a mechanism to improve the network robustness to failure of elements regarding connectivity, as presented in [Ghedini et al. 2016], can increase the probability that the network remains connected if an UAV fails, turns off its radar or is destroyed. In addition, different flight formations can be explored. Finally, the 3D modelling of the scenario will allow exploring other stealth approaches considering yaw and pitch angle [He and Dai 2013].

Acknowledgments

The authors thank CNPQ (procs. no. 132693/2016-0) and FAPESP (procs. no. 2012/25058-9) for the financial support to carry out this research.

References

[Abdel-Fattah et al. 2010] Abdel-Fattah, F., Dahalin, Z. M., and Jusoh, S. (2010). Article:distributed and cooperative hierarchical intrusion detection on manets. *International Journal of Computer Applications*, 12(5):32–40. Published By Foundation of Computer Science.

[Bash et al. 2013] Bash, B. A., Goeckel, D., and Towsley, D. (2013). Limits of reliable communication with low probability of detection on awgn channels. *IEEE Journal on Selected Areas in Communications*, 31(9):1921–1930.

[Basu and Redi 2004] Basu, P. and Redi, J. (2004). Movement control algorithms for realization of fault-tolerant ad hoc robot networks. *IEEE Network*, 18(4):36–44.

[Borges et al. 2016] Borges, N. P., Ghedini, C. G., and Ribeiro, C. H. C. (2016). Improving mission success rate in collaborative uav networks based on a stealth approach. In *Simpósio de Ciência e Tecnologia do Instituto de Estudos Avançados*, volume 1, pages 190–195.

[Breitenmoser et al. 2010] Breitenmoser, A., Schwager, M., Metzger, J.-C., Siegwart, R., and Rus, D. (2010). Voronoi coverage of non-convex environments with a group of networked robots. In *Robotics and Automation (ICRA), 2010 IEEE International Conference on*, pages 4982–4989. IEEE.

[Coelho et al. 2015] Coelho, A. H., Borges Jr, N. P., Borges, N. P., Gallo, M. D., and Valente, A. M. (2015). Automatic horizontal road design information extraction from georeferenced polygonals: A brazilian federal highway network study. *Journal of Civil Engineering and Architecture*, 9:1513–1522.

[Coope 1993] Coope, I. D. (1993). Circle fitting by linear and nonlinear least squares. *Journal of Optimization Theory and Applications*, 76(2):381–388.

[Exército 2009] Exército, E.-M. (2009). *Emprego da Guerra Eletrônica*, volume 1. Estado-Maior do Exército.

[Ghedini et al. 2016] Ghedini, C., Ribeiro, C. H. C., and Sabattini, L. (2016). Improving the fault tolerance of multi-robot networks through a combined control law strategy. In *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 209–215.

[Giulietti et al. 2000] Giulietti, F., Pollini, L., and Innocenti, M. (2000). Autonomous formation flight. *IEEE Control Systems*, 20(6):34–44.

[Glasius et al. 1995] Glasius, R., Komoda, A., and Gielen, S. C. (1995). Neural network dynamics for path planning and obstacle avoidance. *Neural Networks*, 8(1):125–133.

[He and Dai 2013] He, P. and Dai, S. (2013). Stealth coverage multi-path corridors planning for uav fleet. In *Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on*, pages 2922–2926. IEEE.

[Kacena 1995] Kacena, N. G. (1995). Stealth: An example of technology's role in the american way of war. Technical report, DTIC Document.

[Kim and Seo 2012] Kim, S. W. and Seo, S. W. (2012). Cooperative unmanned autonomous vehicle control for spatially secure group communications. *IEEE Journal on Selected Areas in Communications*, 30(5):870–882.

[Kothari et al. 2009] Kothari, M., Postlethwaite, I., and Gu, D.-W. (2009). Multi-uav path planning in obstacle rich environments using rapidly-exploring random trees. In *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*, pages 3069–3074. IEEE.

[LaValle 1998] LaValle, S. M. (1998). Rapidly-exploring random trees: A new tool for path planning.

[Lee et al. 2013] Lee, D., Franchi, A., Son, H., Ha, C., Bulthoff, H., and Robuffo Giordano, P. (2013). Semiautonomous haptic teleoperation control architecture of multiple unmanned aerial vehicles. *IEEE/ASME Transactions on Mechatronics*, 18(4):1334–1345.

[Robuffo Giordano et al. 2013] Robuffo Giordano, P., Franchi, A., Secchi, C., and Bülthoff, H. H. (2013). A passivity-based decentralized strategy for generalized connectivity maintenance. *The International Journal of Robotics Research*, 32(3):299–323.

[Sabattini et al. 2013a] Sabattini, L., Chopra, N., and Secchi, C. (2013a). Decentralized connectivity maintenance for cooperative control of mobile robotic systems. *The International Journal of Robotics Research (SAGE)*, 32(12):1411–1423.

[Sabattini et al. 2013b] Sabattini, L., Chopra, N., and Secchi, C. (2013b). Decentralized connectivity maintenance for cooperative control of mobile robotic systems. *The International Journal of Robotics Research*, 32(12):1411–1423.

[Tarjan 1972] Tarjan, R. (1972). Depth-first search and linear graph algorithms. *SIAM journal on computing*, 1(2):146–160.

[Turgut et al. 2009] Turgut, D., Turgut, B., and Bölöni, L. (2009). Stealthy dissemination in intruder tracking sensor networks. In *2009 IEEE 34th Conference on Local Computer Networks*, pages 22–29.

[Zhen et al. 2014] Zhen, Z., Gao, C., Zhao, Q., and Ding, R. (2014). Cooperative path planning for multiple uavs formation. In *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2014 IEEE 4th Annual International Conference on*, pages 469–473. IEEE.