# Automomous Control of Aircraft for Communications and Electronic Warfare: The Promises of Recent Artifical Intelligence Literature

Sean Carver, Ph.D. at Data Machines Corporation

May 17, 2021

**Abstract**

We pose an unsolved problem in autonomous control of aircraft for communications and jamming (electronic warfare). We aim to provide helpful pointers to literature offering approximately optimal solutions to related problems—such as cyber-security, precision farming, and search and rescue. Solutions to these related problems promise applicability to diverse scenarios beyond the scope of the original works—including to the important scenario considered here.

The problem we address lies within the fields of adversarial Multi-Agent Reinforcement Learning (MARL) and active sensing. In our problem, two opposing factions (labeled "blue" and "red") compete to win a zero-sum/purely adversarial game. The blue side tries to maintain communication links between ground-based assets with a fleet of "comms;" whereas the red side tries to jam this network with a fleet of "jammers." An Unmanned Aerial Vehicle (UAV) becomes a comm or a jammer when fitted for one of these purposes.

Each faction lacks access to the state of the opposing side, and must infer this state probabilisticly through positioning its fleet for best sensory performance and localization (active sensing). Moreover, the ground troops of each side, when also positioned appropriately, have the possibility of shooting down any of their adversary's UAVs. Finally, the blue side must simultaneously achieve its objective of keeping units on the ground in communication. Despite best efforts, different units/UAVs can fall in and out of communication with their respective headquarters, making each of the blue and red factions a multi-agent collection, fully cooperating among itself, but with different information, to fight its adversary having opposing goals.

Our contribution poses this problem while pointing to literature for possible ideas for moving the field forward. Finally, we pose a heirarchy of simpler-than-reality mini-games for efficiently investigating solutions leading to a successful implementation for the full adversarial problem in real-world combat.

# 1 Introduction

If unfortunate circumstances compel our leaders to order our armed forces to take a city from an adversary, the command headquarters on the ground would benefit from constant two-way communication with all its other units during the conflict.

In the fog that accompanies such struggles, our forces cannot rely on our enemy's network of cell towers to keep in touch. Instead, two way radios, linked by a network of "comms" (UAVs for communication) will hopefully allow our friendlies to stay connected.

While vastly better than cell phones, such a network has it own set of challenges. Indeed, our adversaries clearly prefer to keep us out of communication. To pursue this preference, they may send up jammers (UAVs for blocking communication). Thus begins a delicate dance of each side positioning its fleet to best find the other's birds and in so doing best keep or block communications.

We study the question of how each side can control its fleet by autonomously ordering and carrying out flight and communications- electronics operation instructions (CEOI) to optimally achieve its objectives. We are interested in the strategies for both sides, because to defeat our enemy, we must understand the intelligent countermeasures they may take. Moreover, in a real war, our side may choose to fly both comms and jammers, requiring strategies for both roles.

Much recent literature has tackled the problem of optimal search and rescue, and several similar scenarios. This effort clearly relates to the problem at hand because, as with rescue, each of our sides benefits from successfully inferring the positions of targets. But there is a difference between search and rescue and electronic warfare. People being rescued presumably want to be found and will presumably cooperate with this effort. But in electronic warfare participants always aim to keep their locations from the other side. As a result, while search and rescue can succeed with a purely active sensing and optimal control solution, in our scenario, we need to learn to counter an opponent's strategy. To this end, we propose to apply artificial intelligence: specifically, adversarial multi-agent reinforcement learning.

This paper reviews the literature relevant to our problem in electronic warfare, but will close with a very brief discussion presenting ideas for applying this work to other domains of interest to us, notably cybersecurity.

# 2 A Heirarchy of Models

We propose models of the battlefield together with capabilties of each side. However, we aim to make our method successful against a real-world adversary on a real-world battlefield, not just against one particular model adversary on one particular model battlefield. The approach we suggest implements a heirarchy of models, from trivial to complex. For the purposes of the exposition, we illustrate just a few pieces of this heirarchy.

We [at Data Machines Corporation (DMC)] previously supported a

simulation environment (ULTRA) to train human commanders to take a city from an adversary. The simulation platform (developed outside of DMC) showed stunning complexity and realism in its details. It included electronic warfare as well as a large array of other features of the conflict.

One might conceive of the following challenge in Artificial Intelligence: consistently beat at ULTRA the best human players of ULTRA. In this sense, ULTRA finds an analog with the dizzyingly complex game StarCraft II, cracked several years ago by reseachers at DeepMind [1]. That said, for electronic warfare, we care about something harder: we care not just that we can beat the best human opponents in the game, but more importantly we care that we can beat our future adversaries on real-world battlefields.

A bot that excels against human players of ULTRA has merit as a goal, but we must worry that that in training against ULTRA will train for any peculiarities of the game that do not exist in the real world—if any such peculiarities actually exist in the game. To counter this possibility, our approach trains our bots against a wide variety of scenarios—both complex scenarios within ULTRA, and simple, even trivial, ones outside of ULTRA. Simple and trivial scenarios, while in themselves will not win a war, can lead to insight about what happens in training, which makes a step in that direction.

# 3 Even trivial scenarios reveal complexities

# 4 A moderately complex model

The field of interest is a square in the Euclidean plane. In this field, there is a "source," or "sender," labeled $S$, a receiver, labeled $R$, and $n$ different "jammers," labeled $J_1, \ldots, J_n$. We do not assume that the ability to communicate is symmetric—a separate calculation is needed when the roles of sender and receiver are reversed. Additionally there are $m$ different comms to facilitate communication.

# 5 Optimal Placement Of Comms

Let $c_i$ denote positions of comms and let $j_k$ denote positions position of jammers. If these quantities are known, we can compute the probability of a successful communication between the headquarters and an asset (see more details below). We denote this probability

$$P(\text{transmission}|c_i, j_k)$$

Some choices still need to be made about how this probability will be computed, but it shouldn't be hard. By total probability,

$$P(\text{transmission}|c_i) = \sum_k P(\text{transmission}|c_i, j_k)P(j_k)$$

It is a sum rather than an integral because we only consider grid points as possible locations. That may need to be generalized. The second factor of each term in the sum is the posterior probability already coded for computation and described below.

A final step in the computation is a optimization over the comm positions $c_i$.

# 6 TL;DR

Let $P_j(d_j)$ be the power of jammer $j$ at the receiver, at distance $d_j$. Let $P_S(d_S)$ be power of the source at the receiver, at distance $d_S$. Let $P_N$ be the power of the ambient noise.

These functions are given by $P_j = \frac{M_j}{d_j^2}$, for $j = 1, \ldots, n$ and $P_S = \frac{M_S}{d_S^2}$; $P_N$ is a constant.

The probability of a successful transmission is given by

$$\text{sigmoid}\left(10\log_{10}\left(\frac{P_S(d_S)}{P_1(d_1) + P_2(d_2) + \ldots + P_n(d_n) + P_N}\right)\right)$$

The quantity in the sigmoid is the strength expressed in decibels, of the signal against the background that includes all jammers and the ambient noise, see Equation (1) in reference [2]

# 7 Some thoughts about the man-in-the-middle

Billy had alerted us to the fact that it was more than just distance to jammer–jammers in the line of sight were more potent than those off of it.

I spent a long time trying to justify putting this feature explicitly in the model. But the model above seemed most consistent with what I was reading in the literature and it made sense. It is distance to receiver that matters. A man in the middle generally will jam the receiver, unless distances are great enough, the ambient noise is small enough, and the proportionality constant of the jammer is small enough compared to the proportionality constant of the sender. This makes sense to me.

There is such a thing as electomagnetic interferece. According to Wikipedia: "The effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy." My reading of this is this: interference happens upon the reception of the signal, in the circuits of a radiocommunication system, not with signal itself. Electomagnetic waves don't interact, as far as I am aware, but it can be impossible to pick out the signal in the noise.

Having said all that, a directional receiving antenna would sharpen the effect of a man-in-the-middle jammer, versus one off to the side, but

for the moment I'm keeping it simple and assuming the antennae have no preferred direction. Could change that next, though, by assuming they are optimally directed to receive the signal in a particular orientation, and to reject signals in substantially different directions.

# 8 Power

The power of the radio signal from a point source at a distance $r$ is given by (assuming the free-space propagation loss model):

$$P_{\text{signal}}(d) = \frac{M}{d^2},$$

where $M$ is a proportionality constant that depends on units, and even with the same units, can be different for different senders. Note that $M$ is the power of the signal at distance 1. The value of $M$ may be know for friendlies but need to be extimated for jammers. Equation (1) in reference [3], showed a similar equation for "path loss" relaxing the free-space propagation loss model with a proportionality exponent possibly different from 2. It seems that the units of distance are important in this model—see reference [3]. I note this observation for the future as I intend to use the free-space propagation loss model for now.

Equation (5) in reference [4] gives

$$M = \frac{P_T G_T G_R}{4\pi},$$

where $P_T$ is the power of the transmitter, $G_T$ is the gain of the transmitter in the direction of the receiver, and $G_R$ is the gain of the receiver in the direction of the transmitter. Presumably the transmitter could be either the jammer or the source. Reference [3], gives a similar equation that may not be entirely consistent that has a dependence on wavelength, Equation (1). The basic thing I get from this is kind of obvious for anyone raised in the era before cable television—it depends on the orientation of the anntena how strong the signal. Again, I am just putting this observation in this document for the future. For the first cut the power received by the anntena is just a function of the distance to the transmitter, not the orientation of the antenna.

# 9 Jamming

One reference I have [4] talks about channel capacity as the maximum bit rate $S \to R$, under the assumption of error correcting codes, etc. So it seems in this paradigm that it is not whether you are jammed or not, but how many bits get through per second. In several references, including this one there is a noise term which adds power to the jammer in a symmetric way. When the decibels in the equation above drops below the 0, the channel capacity falls below the bandwidth of the channel.

I am going to ignore the details of channel capacity and error correcting codes and just say probability of transmission is a function of the ratio of the powers of signal to background, expressed as a sigmoid of decibels.

# References


[1] O. Vinyals, I. Babuschkin, W. M. Czarnecki, M. Mathieu, A. Dudzik, J. Chung, D. H. Choi, R. Powell, T. Ewalds, P. Georgiev, *et al.*, "Grandmaster level in starcraft ii using multi-agent reinforcement learning," *Nature*, vol. 575, no. 7782, pp. 350–354, 2019.

[2] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6, IEEE, 2018.

[3] E. Benner and A. B. Sesay, "Effects of antenna height, antenna gain, and pattern downtilting for cellular mobile radio," *IEEE transactions on vehicular technology*, vol. 45, no. 2, pp. 217–224, 1996.

[4] W. Xu, "On adjusting power to defend wireless networks from jamming," in *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous)*, pp. 1–6, IEEE, 2007.

[5] A. Guerra, N. Sparnacci, D. Dardari, and P. M. Djurić, "Collaborative target-localization and information-based control in networks of UAVs," in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, IEEE, 2018.

[6] D. Nicholson, S. D. Ramchurn, and A. Rogers, "Information-based control of decentralised sensor networks," in *Defense Industry Applications of Autonomous Agents and Multi-Agent Systems*, pp. 15–32, Springer, 2007.

[7] M. Pechoucek, S. G. Thompson, and H. Voos, *Defense Industry Applications of Autonomous Agents and Multi-Agent Systems*. Springer, 2008.

[8] E. Testi, E. Favarelli, and A. Giorgetti, "Reinforcement learning for connected autonomous vehicle localization via UAVs," in *2020 IEEE International Workshop on Metrology for Agriculture and Forestry (MetroAgriFor)*, pp. 13–17, IEEE, 2020.

[9] B. Grocholsky, A. Makarenko, T. Kaupp, and H. F. Durrant-Whyte, "Scalable control of decentralised sensor platforms," in *Information Processing in Sensor Networks*, pp. 96–112, Springer, 2003.

[10] A. Ryan and J. K. Hedrick, "Particle filter based information-theoretic active sensing," *Robotics and Autonomous Systems*, vol. 58, no. 5, pp. 574–584, 2010.

[11] G. M. Hoffmann and C. J. Tomlin, "Mobile sensor network control using mutual information methods and particle filters," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 32–47, 2009.

[12] C. Andrieu, A. Doucet, S. S. Singh, and V. B. Tadic, "Particle methods for change detection, system identification, and control," *Proceedings of the IEEE*, vol. 92, no. 3, pp. 423–438, 2004.

[13] W. Cadeau, X. Li, and C. Xiong, "Markov model based jamming and anti-jamming performance analysis for cognitive radio networks," *Communications and Network*, vol. 2014, 2014.