Guidance Law for a Surveillance UAV Swarm Tracking a High Capability Malicious UAV

Jason Brown
School of Mechanical and Electrical Engineering
University of Southern Queensland
Springfield, Australia
https://orcid.org/0000-0002-0698-5758

Nawin Raj
School of Sciences
University of Southern Queensland
Springfield, Australia
Nawin.Raj@usq.edu.au

Abstract—**Significant research is currently focused on the issue of malicious UAVs or drones disrupting critical services (e.g. civilian airport operations). One mitigation is to track or pursue a malicious UAV back to its point of origin (and possibly its owner) using a swarm of surveillance UAVs. This becomes of particular academic interest when the malicious UAV has superior capabilities to the individual surveillance UAVs (e.g. in terms of maximum speed). In this paper, we deduce a guidance law (i.e. a rule for determining the direction of flight) for individual surveillance UAVs to maximize the tracking time of a highly capable malicious UAV. We then demonstrate the validity of the analysis using some examples with realistic contemporary UAV capability parameters. The significance of this research is that, in a networked swarm of surveillance UAVs which communicate with each other, if each surveillance UAV maximizes its tracking time, there is a higher probability that the next closest surveillance UAV can be in a position to assume tracking responsibilities when the malicious UAV moves out of tracking range of the original surveillance UAV. In order to demonstrate this, a simulation of a networked swarm of surveillance UAVs which track a high capability malicious UAV is undertaken under various scenarios.**

Keywords — UAV, drone, networking, tracking, pursuit, guidance

I. INTRODUCTION

There have been several instances recently of Unmanned Aerial Vehicles (UAVs), sometimes referred to as drones, acting in a malicious and/or unlawful capacity to disrupt critical services or even cause physical damage to infrastructure. One of the most notorious examples was the use of a malicious UAV to disrupt civilian airline operations at London Gatwick airport in December 2018 [1, 2].

Several different physical, technical, administrative and legal/regulatory controls have been proposed, and in some cases implemented, to deter, detect and manage malicious UAV events [1,2]. An example of a physical control is the ability to capture or destroy a UAV which is acting maliciously or unlawfully while it is in flight, but there are clearly health and safety issues around such a countermeasure. An example of a technical control is to jam or hijack the wireless link between the UAV and its operator, although this is only effective when the UAV is being controlled manually via the wireless link as opposed to being on an autonomous mission. Finally, an example of an administrative and legal/regulatory control is the proposed FAA remote ID initiative to allow identification and tracking of UAVs while in flight, but a malicious UAV is unlikely to support this capability. It seems clear that different controls, and perhaps combinations of controls, are required to satisfy different threat types and scenarios.

Another approach to managing a malicious UAV is to physically track it back to its point of origin (and possibly its owner) without interfering directly with its flight or operation. For example, this can be achieved in principle with ground based or airborne based radar. Airborne based detection and tracking can be implemented using one or more surveillance UAVs [3-5]. A particularly interesting scenario from an academic perspective occurs when the malicious UAV has superior capabilities than the surveillance UAV(s) in terms of such parameters as maximum speed, such that it can outrun or evade any one of them. However, by dispersing multiple surveillance UAVs across a spatial region of interest as part of a swarm, it is still possible to track the malicious UAV by handing off tracking responsibilities of the malicious UAV from one surveillance UAV to the next.

This concept of swarm based tracking is illustrated in Fig. 1, in which *M* represents the malicious UAV with a flight path illustrated by the arrowed line, and *S1*, *S2* and *S3* are surveillance UAVs which are able to detect another UAV inside the area delineated by the dashed circles. The detection method could be, for example, radar based or computer vision based.

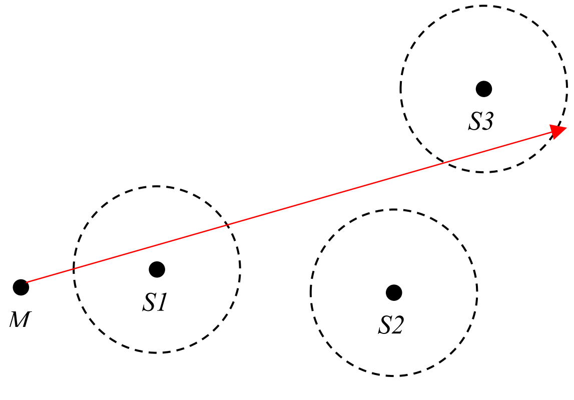

Fig. 1. Using a swarm of surveillance UAVs (*S1*, *S2* and *S3*) to track a malicious UAV (*M*) of superior capability

As the malicious UAV *M* enters the detection area of surveillance UAV *S1*, *S1* can attempt to pursue *M*, but *M* will ultimately exit the detection area and outrun *S1* if it has superior capabilities. If the swarm of surveillance UAVs are networked, *S1* can inform *S2* and *S3* of its estimates of the position, bearing and speed (if available) of *M* as soon as it detects *M*, and continue to do so throughout its pursuit of *M*. This allows *S2* and *S3* to predictively move to positions where the tracking of *M* can seamlessly be handed off from *S1* to *S2* to *S3* over time. Without such networking and predictive pre-positioning of surveillance UAVs, *S2* would not be able to detect and pursue *M* given the flight path of *M*, although *S3* would be able to.

Clearly each surveillance UAV should individually attempt to maximize the time during which *M* remains within its detection range during the pursuit. One objective of this paper is to establish a guidance law for initial pursuit which sets a bearing for *S1* (i.e. the surveillance UAV that first detects *M*) based upon its estimation of the position, bearing and speed of *M* in order to maximize the tracking time. We also discuss aspects of the predictive pre-positioning of other surveillance UAVs in the networked swarm ready for the hand-off of tracking responsibility from one surveillance UAV to the next. Of course, *M* may dynamically change its bearing and speed throughout the pursuit, but the surveillance UAVs can also dynamically change their directional parameters in sympathy based upon the established guidance law. Finally, we execute a simulation of a networked swarm of surveillance UAVs which track a high capability malicious UAV under various scenarios, and in particular with and without the developed guidance law.

The topic discussed in this paper bears some similarities to missile guidance and other forms of interception. Guidance laws such as pure pursuit (i.e. setting an instantaneous course towards the current estimated position of the target) and proportional navigation (i.e. setting an instantaneous course towards a specific predicted future position of the target) are often cited in those cases [6]. However, the objective in this paper is to maximize surveillance time (rather than achieve interception) under the constraint that the pursuing agent has inferior capabilities than the pursued agent and will eventually be outrun.

The paper has the following organisation. Section II provides a review of the literature in this field. Section III establishes a guidance law to maximize the tracking time for the initial surveillance UAV that first detects the malicious UAV. It then provides some illustrative graphical examples using realistic UAV parameters to validate the guidance law and provide insight into it. In Section IV, we discuss the design of the simulation of a networked swarm of surveillance UAVs which track a high capability malicious UAV with the developed guidance law. Section V discusses the results of the simulation. In Section VI, we present our conclusions and areas for further research.

The contributions of this paper are as follows:

- A guidance law for individual surveillance UAVs to maximize the tracking time of a highly capable malicious UAV has been developed, verified and analysed.
- Tracking of a high capability malicious UAV by a networked swarm of surveillance UAVs has been simulated both using the developed guidance law for maximum tracking time and, for comparison, a simple parallel trajectory. Various scenarios have been considered in this simulation e.g. purely reactive tracking by individual surveillance UAVs and predictive tracking by the swarm.

II. Previous Work

In this section, we review and discuss some of the previous research work on using UAV swarms for surveillance of a malicious UAV. This shows quite clearly that while tracking of a malicious UAV using a surveillance UAV swarm has been the subject of significant research, consideration of a guidance law or strategy for tracking when the malicious UAV has superior capabilities has not been investigated to any great degree.

In [3], the authors discuss a UAV defense system comprising a networked UAV swarm of *defense UAVs (dUAVs)* that can self organize and encircle a malicious UAV *(mUAV)* so as to restrict its movement. The operation of the defense system comprises clustering, formation, chase phase and escort phases. However, one assumption of the paper is that the mUAV has a lower top speed than the dUAVs. Our research instead focuses on the scenario where the malicious UAV has superior capabilities than the surveillance UAVs and thereby can outrun individual surveillance UAVs. In this case, employing a swarm to encircle the malicious UAV may not be the best defensive strategy, since the malicious UAV may be able to outrun the whole swarm if it breaks through the virtual encirclement barrier. Instead, the swarm of surveillance UAVs are distributed in space so as to allow handoff of tracking responsibilities from one surveillance UAV to the next as the malicious UAV traverses the region of interest.

In [4], a surveillance UAV swarm is employed to track a target UAV (whether malicious or otherwise) based upon the irregular radio transmissions of a target UAV. The surveillance UAVs use received signal strength indicator (RSSI) sensors to detect these transmissions and estimate the position of the target UAV. The surveillance UAVs then move into different positions to reduce the estimation error of the target UAV position. There is no explicit discussion regarding the relative capabilities of the surveillance and target UAVs.

The authors of [7] propose a guidance law for UAV swarm tracking of a moving target in three dimensions which is an amended pure pursuit strategy. The moving target may be a hostile UAV, but can be other entities such as a flock of birds that need to be escorted away from critical infrastructure. The paper demonstrates that the UAV swarm can maintain a specific formation while avoiding collisions with the target or within the swarm. There is an explicit assumption stated that the target has a lower maximum speed than the tracking UAVs.

An investigation into the hardware and software testbed for a *Counter Unmanned Aerial System (CUAS)* involving UAV swarms that use computer vision for target detection is presented in [8]. Although there is no explicit discussion of the capability of the malicious UAV relative to the surveillance UAVs, this testbed could in principle be employed to test various UAV swarm tracking strategies, including when the malicious UAV has superior capability than the surveillance UAVs.

In [9], the authors consider a swarm of UAVs that employ on-board radar to detect and track a malicious UAV. The swarm is referred to as a *Dynamic Radar Network (DRN)* in this context. Again, the malicious UAV to be tracked is not considered to be of superior capability to the UAVs in the DRN.

III. Theoretical Analysis

A. Model

The model for this introductory theoretical analysis is based upon a horizontal plane at an arbitrary altitude. A surveillance UAV denoted as S is initially hovering at the origin of the co-ordinate system. S can detect a malicious UAV denoted as M at a maximum distance of r. The method of detection is not specified, but, for example, could be via on-board computer vision or radar.

Fig. 2 illustrates the situation when S first detects M at time $t=0$ as a result of M moving towards S. M is assumed to be travelling at a constant speed v (which is greater than the maximum speed of S) in the direction of the x axis at an angle φ $(-\pi/2 \leq \varphi \leq +\pi/2)$ to the line joining S and M. When S detects M, it moves a constant speed $u < v$ and at a constant angle θ relative to the x axis in order to pursue/track M. Acceleration is ignored. The problem is to determine the value of θ $(-\pi/2 \leq \theta \leq +\pi/2)$ that maximizes the duration for which the distance between S and M remains no more than r assuming that S can estimate the parameters φ and v (and r too if this is not already known) as part of the detection of M.

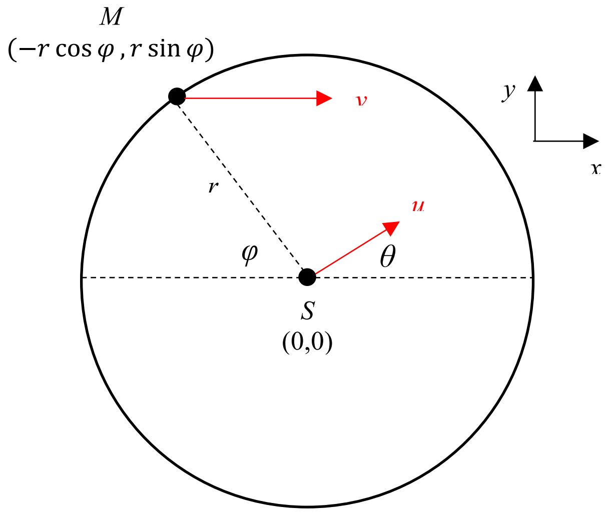

Fig. 2. Model when surveillance UAV (S) first detects malicious UAV (M) at $t=0$

In a realistic pursuit, the malicious UAV is likely to change its speed and/or bearing, and the surveillance UAV is unlikely to be able to estimate the position and velocity of the malicious UAV with complete accuracy. However, this theoretical analysis is still of significant utility, because it provides insight into what action S should take, at least initially, in order to optimise the pursuit.

Note that there is no loss of generality in specifying that M travels along the x axis; the co-ordinate system can always be rotated to ensure that this is the case.

B. Derivation of Maximum Tracking Time

Given the model of Fig. 2, at time t the co-ordinates of S are $(ut\cos\theta, ut\sin\theta)$ and the co-ordinates of M are $(-r\cos\varphi + vt, r\sin\varphi)$. Therefore the distance d between S and M is given by:

$$d^2 = (ut\cos\theta + r\cos\varphi - vt)^2 + (ut\sin\theta - r\sin\varphi)^2 \tag{1}$$

Expanding (1) and simplifying yields:

$$\begin{aligned} d^2 &= (u^2 + v^2 - 2uv\cos\theta)t^2 \\ &\quad +2r(u\cos[\theta+\varphi] - v\cos\varphi)t \\ &\quad +r^2 \end{aligned} \tag{2}$$

At $t = t_{loss}$, S is on the threshold of losing the ability to track M because the distance between the UAVs is equal to the maximum detection distance for S i.e. $d = r$. Substituting $t = t_{loss}$ and $d = r$ into (2), eliminating the $t = 0$ solution (which is the initial condition) and re-arranging gives:

$$t_{loss} = \frac{2r(v\cos\varphi - u\cos[\theta+\varphi])}{(u^2 + v^2 - 2uv\cos\theta)} \tag{3}$$

The problem is for S to determine the value of θ that maximizes t_{loss} (and thereby maximizes the tracking time of M) given the parameters r, φ, u and v. This is achieved by setting the derivative of t_{loss} with respect to θ to zero and solving for θ. The derivative of t_{loss} with respect to θ is given by:

$$\frac{dt_{loss}}{d\theta} = \frac{2ru\sin[\theta+\varphi](u^2 + v^2 - 2uv\cos\theta)}{(u^2 + v^2 - 2uv\cos\theta)^2} - \frac{4ruv\sin\theta\,(v\cos\varphi - u\cos[\theta+\varphi])}{(u^2 + v^2 - 2uv\cos\theta)^2} \tag{4}$$

Setting this derivative to zero yields:

$$\begin{aligned} &[(u^2 + v^2)\sin\varphi]\cos\theta - [(v^2 - u^2)\cos\varphi]\sin\theta \\ &\quad = 2uv\sin\varphi \end{aligned} \tag{5}$$

Using $A\cos[\theta+\alpha] = [A\cos\alpha]\cos\theta - [A\sin\alpha]\sin\theta$ and comparing with Eq. (5), we see that:

$$\begin{aligned} A &= \sqrt{[A\cos\alpha]^2 + [A\sin\alpha]^2} \\ &= \sqrt{[(u^2 + v^2)\sin\varphi]^2 + [(v^2 - u^2)\cos\varphi]^2} \\ &= \sqrt{u^4 + v^4 - 2u^2v^2\cos 2\varphi} \end{aligned} \tag{6}$$

and:

$$\tan\alpha = \frac{[A\sin\alpha]}{[A\cos\alpha]} = \frac{[(v^2 - u^2)\cos\varphi]}{[(u^2 + v^2)\sin\varphi]} = \frac{v^2 - u^2}{[u^2 + v^2]\tan\varphi} \tag{7}$$

Combining (5), (6) and (7), the optimal value $\theta_{optimal}$ of θ is therefore given by:

$$\begin{aligned} \theta_{optimal} = \cos^{-1}&\left(\frac{2uv\sin\varphi}{\sqrt{u^4 + v^4 - 2u^2v^2\cos 2\varphi}}\right) \\ &- \tan^{-1}\left(\frac{v^2 - u^2}{[u^2 + v^2]\tan\varphi}\right) \end{aligned} \tag{8}$$

Note that $\theta_{optimal}$ depends upon φ, u and v, but not r.

C. Analysis of Tracking Time

Fig. 3, Fig. 4 and Fig. 5 illustrate t_{loss}, the time at which the surveillance UAV loses the ability to track the malicious UAV because the distance between the two is greater than r, versus θ, the angle of travel of the surveillance UAV relative to the x axis, for $u = 20m/s$, $u = 25m/s$ and $u = 29m/s$ respectively. These plots are based upon Eq. (3) for various values of φ, the angle between the direction of travel of the malicious UAV and the line joining the surveillance and malicious UAVs at time $t = 0$. A malicious UAV speed of $v = 30m/s$ and a detection/tracking distance of $r = 100m$ are employed. See Fig. 2 for a reminder of the definition of these parameters. Also plotted, as discrete crosses, are the maximum values of t_{loss} predicted by selecting $\theta = \theta_{optimal}$ from Eq. (8). It can clearly be seen that Eq. (8) provides the correct optimal value of θ to maximize the tracking time.

As the surveillance and malicious UAVs become more evenly matched in capabilities (i.e. as u approaches v in moving from Fig. 3 to Fig. 5), the t_{loss} curves become more peaked and therefore the importance of choosing the optimal value of θ increases (it should be noted that the optimal value of θ becomes closer and closer to zero as this transition occurs). This has implications when the surveillance UAV cannot accurately estimate the bearing φ and speed v of the malicious UAV. In such a case, the t_{loss} curves show it is better to over-estimate the optimal value of θ than to under-estimate it, since the curves fall off more slowly when $\theta > \theta_{optimal}$ than when $\theta < \theta_{optimal}$.

In any one of Fig. 3, Fig. 4 or Fig. 5, the maximum of t_{loss} is largest for $\varphi = 0$, and decreases for increasing values of φ. This suggests that in a scenario where a surveillance UAV has advance knowledge of the position and bearing of the malicious UAV (e.g. because another surveillance UAV has already detected the malicious UAV and communicated its trajectory), it would be advantageous for the surveillance UAV with advance knowledge to predictively pre-position itself such that $\varphi = 0$ when it first detects the malicious UAV, thereby maximizing the tracking time. However, the disadvantage of this strategy is that the surveillance and malicious UAVs are then on a collision course.

D. Analysis of Tracking Distance

Another metric of interest is the instantaneous distance d between the surveillance and malicious UAVs as a function of time t. Fig. 6 illustrates this metric based upon Eq. (2) for $u = 25m/s$ and various φ values, assuming the surveillance UAV selects $\theta = \theta_{optimal}$ in all cases. The plots for $u = 20m/s$ and $u = 29m/s$ are very similar, only the scale of the x axis differs.

At time $t = 0$, $d = r = 100m$ by definition. As the surveillance UAV selects $\theta = \theta_{optimal}$, the two UAVs become closer together as time advances before the malicious UAV outruns the surveillance UAV. Only in the case $\varphi = 0$ do the two UAVs collide. This shows that, in general, the guidance law employed in this paper i.e. to maximize the tracking time, is quite different to traditional guidance laws such as proportional navigation which aim to ultimately intercept the malicious entity.

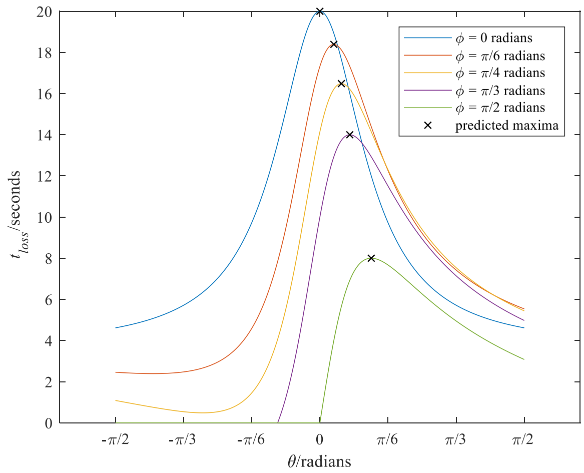

Fig. 3. t_{loss} versus θ for u=20m/s, v=30m/s and various φ values

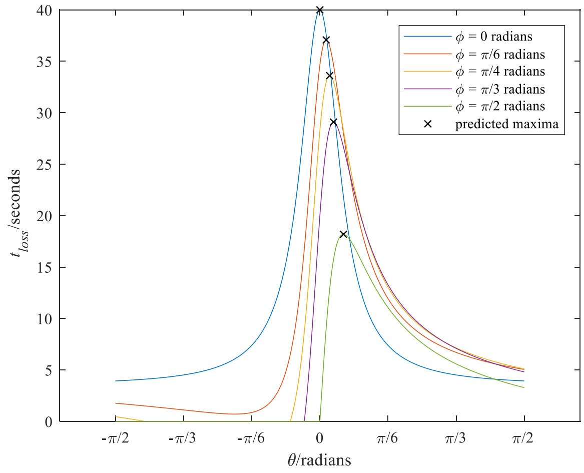

Fig. 4. t_{loss} versus θ for u=25m/s, v=30m/s and various φ values

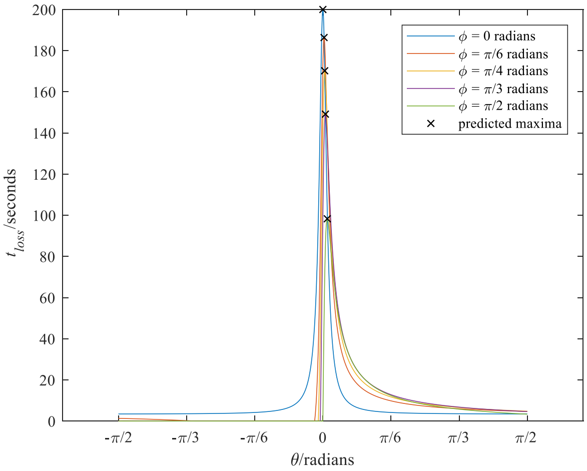

Fig. 5. t_{loss} versus θ for u=29m/s, v=30m/s and various φ values

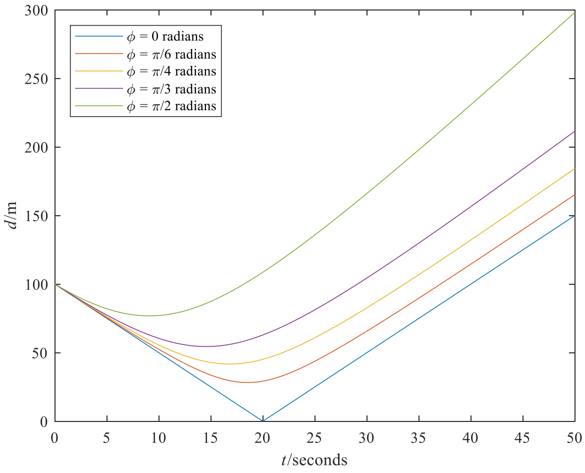

Fig. 6. Distance *d* between surveillance and malicious UAVs versus time *t* for *u*=25m/s, *v*=30m/s and various *φ* values

IV. Simulation Design

A simulation of a surveillance UAV swarm tracking a malicious UAV has been undertaken using MATLAB. Both reactive tracking and predictive pre-positioning have been considered.

Reactive tracking involves a surveillance UAV hovering until it detects the malicious UAV in its own detection zone, after which it actively tracks the malicious UAV until it is outrun. There is no explicit communication or co-ordination between members of the surveillance swarm.

In predictive pre-positioning [10], the first surveillance UAV to detect the malicious UAV communicates the estimated trajectory of the malicious UAV to all other UAVs in the surveillance swarm so they can predictively position themselves in the optimum location ready to track the malicious UAV when it arrives. For the purposes of this paper, the predictive pre-positioning involves surveillance UAVs following the shortest path to the estimated trajectory of the malicious UAV.

In all, four different scenarios have been considered:

i. Reactive tracking in which a surveillance UAV that has detected the malicious UAV moves parallel to the malicious UAV (i.e. with $\theta = 0$) until it is outrun.

ii. Reactive tracking in which a surveillance UAV that has detected the malicious UAV moves with the optimum bearing to maximize tracking time (i.e. with $\theta = \theta_{optimal}$ from Eq. (8)) until it is outrun.

iii. Reactive tracking and predictive pre-positioning, in which surveillance UAVs move towards the estimated trajectory of the malicious UAV once the malicious UAV is initially detected by any member of the swarm, and each surveillance UAV that has detected the malicious UAV moves parallel to the malicious UAV (i.e. with $\theta = 0$) until it is outrun.

iv. Reactive tracking and predictive pre-positioning, in which surveillance UAVs move towards the estimated trajectory of the malicious UAV once the malicious UAV is initially detected by any member of the swarm, and each surveillance UAV that has detected the malicious UAV moves with the optimum bearing to maximize tracking time (i.e. with $\theta = \theta_{optimal}$ from Eq. (8)) until it is outrun.

The parameters of the simulation are specified in Table I. The primary metric of interest is the proportion of time the malicious UAV is actively tracked i.e. within the detection zone of one or more surveillance UAVs.

TABLE I. Parameters of The Tracking Simulation

Parameter	**Value**
Step	1m movement of the malicious UAV
Number of randomized iterations for each set of parameters	500
Shape and size of tracking area	Circular with 15km radius
Surveillance swarm size	Varies between 10 and 1000
Surveillance swarm initial formation	Randomly generated
Surveillance swarm networking method	Broadcast (each UAV hears the transmissions of all other UAVs)
Surveillance UAV speed (*u*)	Three speed capabilities considered: 20m/s, 25m/s, 29m/s
Malicious UAV detection range (*r*)	100m
Malicious UAV speed (*v*)	30m/s
Malicious UAV path	Linear via centre of tracking area

V. Simulation Results and Analysis

Fig. 7, Fig. 8 and Fig. 9 illustrate the proportion of time for which the malicious UAV is actively tracked i.e. it is within the detection zone of one or more surveillance UAVs, as a function of the number of surveillance UAVs in the swarm, for surveillance UAV speeds of $u = 20m/s$, $u = 25m/s$ and $u = 29m/s$ respectively. Therefore, given the fixed malicious UAV speed of $v = 30m/s$, Fig. 7 represents the scenario of a significantly more capable malicious UAV, whereas Fig. 9 represents the scenario of a marginally more capable malicious UAV. All four tracking strategies relating to reactive tracking and predictive pre-positioning are represented in each figure. Clearly, and as expected, a tracking strategy which involves predictive pre-positioning outperforms one which is based on reactive tracking only.

It can be seen that when individual UAVs set an optimal bearing when pursuing the malicious UAV (i.e. with $\theta = \theta_{optimal}$ from Eq. (8)), as opposed to setting a bearing which is parallel to the malicious UAV (i.e. with $\theta = 0$), there is a systematic increase in the proportion of time for which the malicious UAV is actively tracked. The increase is quite small, because with reference to Fig. 3, Fig. 4 and Fig. 5, the optimal bearing is usually quite close to the parallel trajectory. Therefore, the parallel trajectory is only marginally sub-optimal in the majority of pursuit cases.

The superior performance resulting from individual UAVs setting an optimal bearing when pursuing the malicious UAV is perhaps more noticeable when using reactive tracking only (i.e. no predictive pre-positioning). This is to be expected, because when using predictive pre-positioning, some if not most of the surveillance UAVs that take part in the pursuit will have predictively moved to an optimum position on the estimated trajectory of the malicious UAV prior to the arrival of the latter. For these surveillance UAVs, the optimum bearing when tracking the malicious UAV is the parallel trajectory.

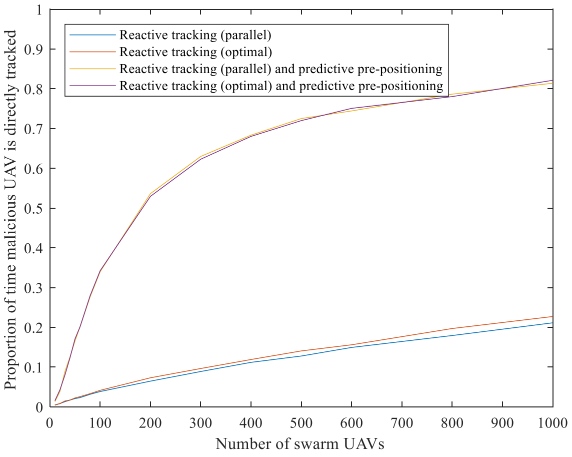

Fig. 7. Proportion of time for which malicious UAV is tracked for different tracking strategies and u=20m/s, v=30m/s

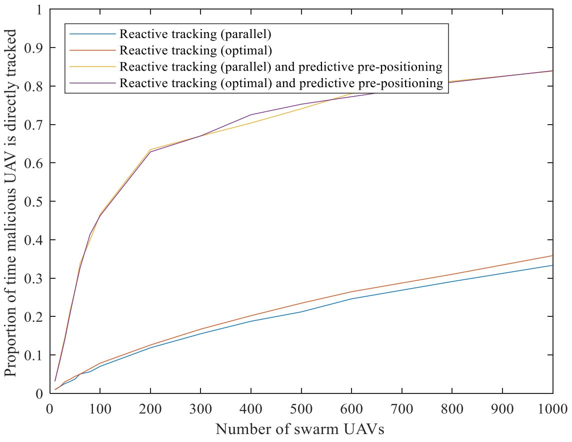

Fig. 8. Proportion of time for which malicious UAV is tracked for different tracking strategies and u=25m/s, v=30m/s

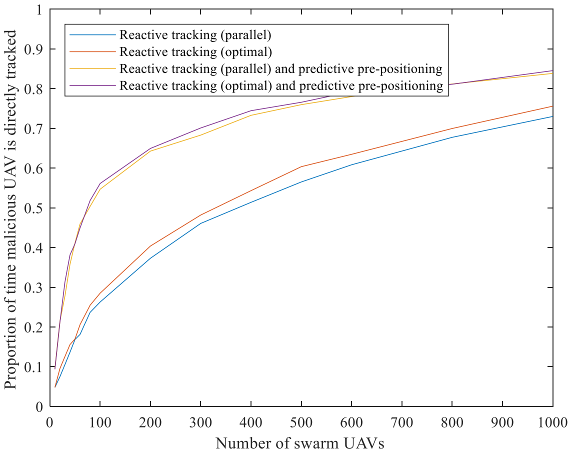

Fig. 9. Proportion of time for which malicious UAV is tracked for different tracking strategies and u=29m/s, v=30m/s

VI. Conclusions

In this paper, we have derived a guidance law that a surveillance UAV should follow to maximize the tracking time of a malicious UAV of higher capability that it has detected for the first time. The law comprises selecting the optimum direction of flight based upon the estimated speed and bearing of the malicious UAV. Although the surveillance UAV will always ultimately be outrun by a malicious UAV of higher capability, maximizing the tracking time is important when there are other geographically dispersed surveillance UAVs ready to take over tracking responsibility as part of a networked surveillance swarm. This is because there is a higher probability that the next surveillance UAV will be in position to hand off tracking responsibility to, and ultimately because fewer surveillance UAVs are required to observe a specific area of airspace.

Example plots have been provided to provide further insight into the implications of the guidance law. One of the interesting observations from these plots is that a surveillance UAV to which tracking responsibility is to be handed off should predictively pre-position itself so that the malicious UAV is heading directly towards it in order to maximize its tracking time. However, this requires some collision avoidance strategy.

The developed guidance law has been employed in a network simulation of a swarm of surveillance UAVs tracking a highly capable malicious UAV with various tracking strategies including reactive tracking and predictive pre-positioning. Although it only offers a small increase in performance in terms of the proportion of time for which the malicious UAV is actively tracked compared to parallel tracking, the increase is nonetheless noticeable and it must be realized that parallel tracking itself is only marginally sub-optimal.

Future work will involve generalizing these results to three dimensions and examining the performance gains possible from organising the surveillance UAV swarm into a regular lattice-like formation.

References

[1] J. O'Malley, "The no drone zone," in Engineering & Technology, vol. 14, no. 2, pp. 34-38, March 2019, doi: 10.1049/et.2019.0201.

[2] D. Schneider, "Regulators seek ways to down rogue drones: Growing antidrone industry offers radar, remote ID, and other tools - [News]," in IEEE Spectrum, vol. 56, no. 4, pp. 10-11, April 2019, doi: 10.1109/MSPEC.2019.8678424.

[3] M. R. Brust, G. Danoy, P. Bouvry, D. Gashi, H. Pathak and M. P. Gonçalves, "Defending Against Intrusion of Malicious UAVs with Networked UAV Defense Swarms," 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 2017, pp. 103-111, doi: 10.1109/LCN.Workshops.2017.71.

[4] F. Koohifar, I. Guvenc and M. L. Sichitiu, "Autonomous Tracking of Intermittent RF Source Using a UAV Swarm," in IEEE Access, vol. 6, pp. 15884-15897, 2018, doi: 10.1109/ACCESS.2018.2810599.

[5] C. Arnold and J. Brown, "Performance Evaluation for Tracking a Malicious UAV Using an Autonomous UAV Swarm," 2020 IEEE 11th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2020

[6] P.T. Kabamba and A. R. Girard, "Fundamentals of Aerospace navigation and guidance, " Cambridge University Press, ISBN: 978-1-107-07094-3, 2014.

[7] X. Wang, G. Tan, Y. Dai, F. Lu and J. Zhao, "An Optimal Guidance Strategy for Moving-Target Interception by a Multirotor Unmanned Aerial Vehicle Swarm," in IEEE Access, vol. 8, pp. 121650-121664, 2020, doi: 10.1109/ACCESS.2020.3006479.

[8] M. Pozniak and P. Ranganathan, "Counter UAS Solutions Through UAV Swarm Environments," 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 2019, pp. 351-356, doi: 10.1109/EIT.2019.8834140.

[9] A. Guerra, D. Dardari and P. M. Djuric, "Dynamic Radar Networks of UAVs: A Tutorial Overview and Tracking Performance Comparison With Terrestrial Radar Networks," in IEEE Vehicular Technology Magazine, vol. 15, no. 2, pp. 113-120, June 2020, doi: 10.1109/MVT.2020.2979698.

[10] J. Brown and N. Raj, "Predictive Tracking of a High Capability Malicious UAV," 2021 11th Annual Computing and Communication Workshop and Conference (CCWC), USA, 2021