Cooperative Electronic Attack using Unmanned Air Vehicles

Mark J. Mears

Wright-Patterson Air Force Base, AFRL/VACA, WPAFB, OH 45433-7531, USA

***Abstract*— In this paper, an attempt is made to define electronic attack of integrated air defenses using multiple unmanned air vehicles acting in a coordinated fashion, and to define features of the problem that are salient in the context of cooperative control. The utility of Electronic Attack is described in the context of integrated air defense systems which rely on RADAR sites that act as a network to gather information about potential airborne threats. General concepts for use of multiple vehicles against RADAR systems are described and formulated in terms of cooperative path planning and resource allocation. Then some approaches to solving the technical problems are described. Although the interests expressed in this paper are motivated by capabilities that might be afforded by many unmanned autonomous vehicles, the concepts are relevant for manned aircraft working in concert with groups of air vehicles.**

I. Introduction

In the evolution of warfare, a number of skills, arts, and sciences have been developed. As a method is developed for attacking, so that one can effectively exploit an enemies weakness, an associated method of defense is created to make the attack less effective. Then, to make the attacking method viable in the face of defense tactics, approaches are sought to undo the defense. This sequence of development and opposing developments of tactics for warfare has been in existence for as long as man has engaged in battle.

With the advent of RADAR (RAdio Detection And Ranging), warfare took on an electronic dimension around which an entire discipline, know as Electronic Warfare (EW), has evolved. RADAR was used during WWII as a counter-measure to detect attacking enemy aircraft and allow time to ready anti-aircraft resources e.g. anti-aircraft artillery and interceptor aircraft. Electronic Attack (EA) is a counter-counter-measure to reduce the effectiveness of RADAR systems to allow flight of aircraft without harm from RADARs and associated missiles. This is done by either distracting the RADAR with confusing or deceptive information, or by blinding the RADAR making it unable to detect, track, engage, or destroy threats.

In the past, EA has often been achieved by flying specially designed EW aircraft between a RADAR site and the shielded strike configured aircraft. In these cases, the RADAR may able to determine the direction to the jamming aircraft, but is denied range information and any information about the strike aircraft. There may also be the potential to have the RADAR *drop track* and have to try to reacquire its target.

The type of EA activity that is the focus of this paper is referred to as non-destructive Suppression of Enemy Air Defenses (SEAD) [1]. For any mission this is an integral part of the planning that is jointly done by the military forces involved, however we are considering here a subset of the complete SEAD problem. In this paper, a primary interest is how the requirements of the EA problem are manifest in cooperative control requirements.

The new considerations presented in this paper are based on coordinated use of multiple unmanned air vehicles (UAVs) for EW. More specifically, we consider use of UAVs for EA which is a subset of the whole of EW. Whereas conventional EA is most often done using an aircraft working together with one or two aircraft which are being hidden from the view of a RADAR site, in this paper we are discussing UAVs working together with each other and with groups of aircraft that are to be protected.

The use of UAVs for any task presents a number of technical challenges and the use of UAVs for EA presents additional technical problems that relate specifically to EA. In the context of control systems, we define three broad categories for these problems: 1) resource allocation, 2) tightly coupled path planning, and 3) communication.

This paper is structured to introduce the EA, and consider aspects of the problem that particularly relate to cooperative control. Section II gives a high level view of the threat posed by enemy RADAR and Integrated Air Defense Systems (IADS). Section III describes the components of Electronic Warfare (EW) and how EA fits into EW. Section IV describes the parts of Electronic Counter Measures and describes EA in that context. Some work done in the area of cooperative control of UAVs is described in section V and the potential roles of UAV in EA is described in section VI. Some cooperative control work for EA is described in section VII, and section VIII draws some conclusions about cooperative control using UAVs.

II. The Threat/RADAR&IADS

RADAR system units operate on the basic principle of sending out radio frequency energy *Electromagnetic radiation* (EM) and then "listening" for the reflected signal from distant targets. The footprint of radio signals sent out by RADAR systems often have a lobe structure with a large "main beam", or "mainlobe" and many smaller gain directions called "sidelobes" as shown in figure 1.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cooperative Electronic Attack using Unmanned Air Vehicles	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Laboratory,Air Vehicles Directorate,Wright Patterson AFB,OH,45433**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**9**	

During normal operation, the gain of the mainlobe is so

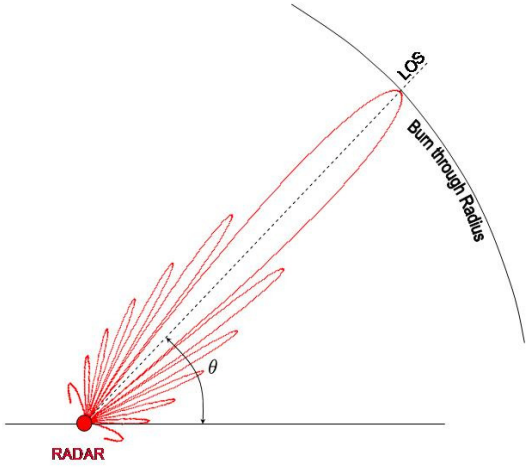

Fig. 1. RADAR Lobe Structure

much larger than the sidelobes, that the direction of the target with respect to some reference is assumed to be the direction in which the mainlobe is pointed. The direction of the main beam is also referred to as the Line-of-Sight (LOS) and in figure 1, this angle is denoted by θ. Distance to the target can be obtained by measuring the difference between the time of signal transmission and the time of reception of the reflected signal. The range rate can be determined by the doppler shift of the reflected signal and the angular rate can be estimated from a sequence of angular measurements (shifts in the direction of the the centroid of the mainlobe) of the target. The end result is a measurement of the position and velocity of vehicles within *detection range* of the RADAR [2]. The size of this *detection range* is influenced by RADAR power limitations, antenna gain, electronic noise and environmental factors. Since the RADAR is able to point the mainlobe in any direction, we abstract the shape of this region as a circle with the radius of the circle given by the *burn-through-radius*, R_B, so noted because the target *burns through* the noise clutter at that range. (This is also referred to as the RADAR's *threat circle*.)

RADARs are also capable of receiving energy through their sidelobes. However, this effect is undesirable (from the RADAR point of view). Since the majority of the EM sent out by the RADAR is through the main lobe and the largest gain for the returned signal is also through the mainlobe, energy received through a sidelobe can cause the RADAR to indicate an angle to the target which is errant. In order to minimize this effect, many RADARs are able to notch out, or cancel their sidelobes.

Today's integrated RADAR systems are complex networked entities that communicate with other RADAR units to correlate information, and that communicate with missile systems to engage and destroy perceived threats. Various types of RADAR with tailored characteristics typically make up a defense network with a hierarchy that includes early warning, tracking, and terminal guidance RADARs. The units are geographically placed to defend key assets and overlap to prevent gaps in coverage. Mobile RADARs, that *light-up* only when prompted by other RADARs in the network, are used to create some uncertainty for attackers. Also, layers of different types of RADARs can be assumed to have communication linkages and geographic coverages to minimize the likelihood that an adversary will be able to penetrate defense and escape unharmed.

Each of the RADAR units themselves, will have modes to allow precision information gathering [2]. Lobe structure adjustment, mono-pulse operation, frequency alteration, pulse-repetition-frequency changes, pulse-to-pulse agility, multi-static operation and signal *gating* are but a few of the tools that can be used to prevent adversaries from avoiding detection and destruction. Robustness to the afore mentioned *counter-counter-counter measures* is vitally important for EA methods to be useful. It would not be wise to invest heavily in "point solutions" in the *warfare tradespace* that could be easily foiled by simple modifications from an adversary.

However, it is not the aim of this paper to focus on nuances of RADAR units or Integrated Air Defense Systems (IADS). We abstract detailed properties and treat only those features of RADAR that are salient for consideration of coordinated UAV for EA.

III. Electronic Warfare

Electronic Warfare (EW) [3] is defined as the use of Electromagnetic radiation (EM) to control the EM spectrum, or directed energy to attack an enemy. EW can be divided into three main components. Electronic Protection is one category involving passive and active means for preventing adverse impact of EM on combat capability. Electronic Warfare Support (ES) is the subdivision of EW that deals with actions to gather information about sources of adverse EM activity. Electronic Attack (EA) is the category that deals with use of EM, directed energy, or use of anti-radiation missiles to adversely affect enemy combat capability [3].

EA can also be put in the context of Suppression of Enemy Air Defenses (SEAD) [1]. SEAD can be either destructive or disruptive. In military doctrine, destructive SEAD means destruction of target in a permanent way. Disruptive SEAD means neutralizing RADARs temporarily. Therefore, EA of an IADS can be considered to be part of disruptive SEAD.

SEAD can also be broken down into the following three categories: 1) suppression over a large area, 2) "localized" suppression of small areas for time intervals, and 3) suppression against targets of opportunity. UAVs have the potential to contribute toward all three. Given enough UAVs, large areas could be persistently covered. Small teams or UAVs could suppress EM in localized areas of interest for specified times opening corridors for operations. By leaving

teams of UAVs in the areas of interest, Time Sensitive Targets (TST) may be suppressed also.

IV. Electronic Counter Measures

Electronic means for countering RADARs are generally referred to as Electronic Countermeasures (ECM). They fall into six general categories. These methods are 1) use of chaff, 2) gate stealing, 3) angle deception and 4) use of decoys, 5) noise jamming and 6) false target generation. Varied as these RADAR countermeasures are, cooperative control of UAVs can contribute to EA effectiveness in each category.

Chaff has the effect of increasing the noise in the RADAR return signal and can be used to screen areas, or in end-game maneuvers, in conjunction with evasive maneuvers to break a missiles seeker's lock. Chaff is a simple means of ECM, but can be effective, particularly when used in conjunction with other methods.

A second method, called **Gate Stealing** is a method of gradually dominating the true return signal with an artificial signal. In order to maintain good signal to noise ratio of an observed target, RADARs *gate* a target's range, speed, or both. Once the RADAR has acquired a strong signal, the gain is lowered and the artificial signal is free to manipulate the RADAR's perception independent of the activities of the real aircraft.

Another method of dealing with RADARs is for aircraft to cause the RADAR to see their image at angles different from the Line-of-Sight. This can be implemented by bouncing EM signals from the terrain to the RADAR, or by altering the shape of the wave front by adjusting the phase of EM sent from different places on the aircraft. These methods are referred to as **Angle Deception**.

Decoys are devices that distract RADAR by drawing their attention. They can be expendable entities which serve their purpose with no plan for recovery, or they can be towed devices which are reeled out behind the aircraft to act as false targets when the aircraft is threatened, and then get reeled back in after the danger is past. The variety of decoy devices continually increases. As the expendable types of decoys get more complex, the line between decoy, munition and generic UAV is becoming blurred. However, increased emphasis on mobile RADARs would lead one to believe that one of the primary roles of decoys will be to cause unseen, hiding RADAR sights to give away their position by becoming active in response to the decoys.

The use of RADAR counter measures work best when their use is coordinated. The characteristics of each ECM type leads to preplanned methods for their use. However, in the context of cooperative control, where one is concerned with position of UAVs and planning their movement, the following two ECM methods are of most interest.

Noise Jamming is an ECM method where EM energy is transmitted to a RADAR in order to raise the noise level and make it harder for the RADAR to extract the signal. This approach is not covert since the enemy is immediately aware of a threatening presence. However, although the RADAR will know the Angle of Arrival (AoA) of the signal, it will be denied range or range rate preventing use of useful fire control information. The need to manage power over frequency ranges and over time during EA has resulted in different types of noise jamming including *barrage*, *spot* and *bin masking*.

Jamming can be categorized according the relative location of the jamming vehicle, the vehicle being shielded, and the RADAR. In this context one can define *Stand-in* and *Stand-off* jamming [4]. Stand-in jamming of RADAR implies that the jamming vehicle is between the shielded vehicle and the RADAR, whereas Stand-off jamming means the shielded vehicle is closer to the RADAR than the jammer. Jamming can also be either *Escort*, where a special jamming aircraft fly with aircraft that are to be shielded, or *Self-protection*, where an aircraft is able to supply its own jamming support [4].

The effect of jamming can be seen in figure 2. Since the

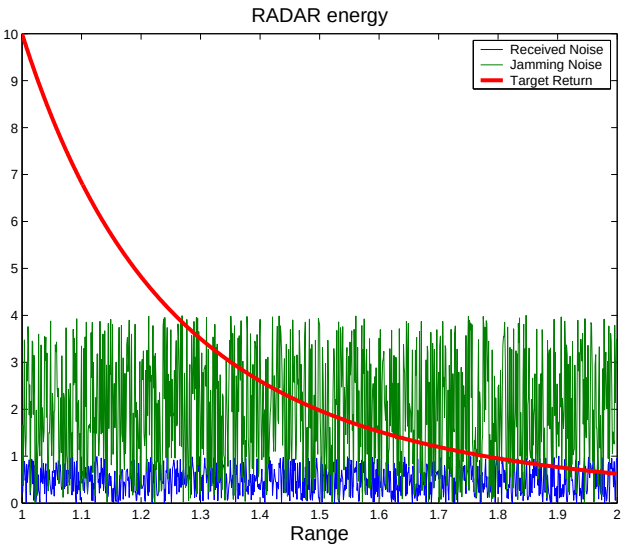

Fig. 2. Target signal and Noise

energy of RADAR spreads over an increasingly large area as it travels out to a target, the energy that reaches a target is inversely proportional to square of the range. This same phenomenon is at work for the energy reflected from the target back to the RADAR. Thus, the energy reflected back to a RADAR is inversely proportional to R^4.

Figure 2 shows a return signal from a target which is shrinking proportional to $\frac{1}{R^4}$. Also shown in figure 2 are two noise levels. The lower noise level represents the noise that would be inherent in a RADAR output. This noise would be due to electrical sources and environmental clutter. The high noise level represents a noise level that would be output by a RADAR when jamming is being used. Where the target signal rises above the nominal noise at a range of about 1.8 units, the target would be able to approach the RADAR to about 1.25 units before being detected if jammed.

One reason that jamming can be effective is that the energy from the jamming vehicle, received by the RADAR, is proportional to $\frac{1}{R^2}$, while the reflected energy received by the RADAR from the target is proportional to $\frac{1}{R^4}$. The energy received from the target is $\frac{K_1}{R^4}$ and the jamming energy received is $\frac{K_2}{R^2}$ where K_1 and K_2 are constants associated with the antenna sizes and gains, transmitted power, time-on-target and RADAR cross section. To observe the impact of distance independent of other factors, we assume $K_1 = K_2$ and show the result in non-dimensional distance units in figure 3. From this figure we can see that in order

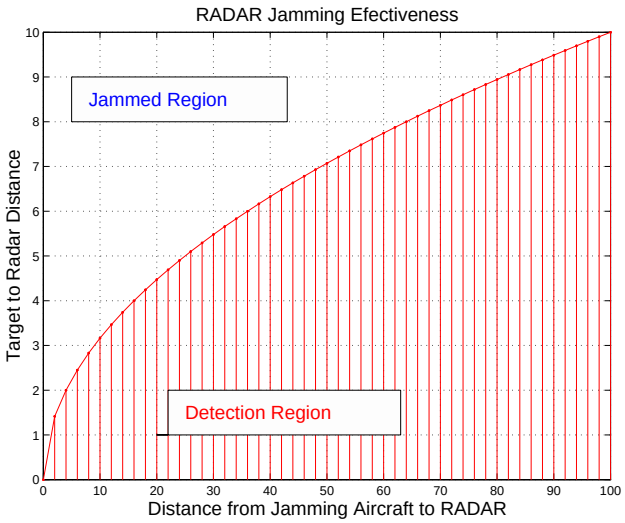

Fig. 3. Jamming Effectiveness

to effectively jam the RADAR, we need to have $\frac{1}{R_j^2} > \frac{1}{R_t^4}$ where R_t is the distance from RADAR to target and R_j is the distance from RADAR to jamming vehicle. That is, for effective jamming, the R_j can increase quadratically as R_t increases linearly.

As described in section II, the effect of jamming is to reduce the burn-through radius of the RADAR. If we suppose that we must fly a *strike aircraft* near a RADAR site to strike targets, then we may want to use a jamming aircraft to jam the RADAR to prevent detection of the strike aircraft. An abstraction of such a situation is shown in figure 4. In this figure we see the RADAR site as a dot inside concentric rings. The path of the strike vehicle is given by the line from the start to the destination. The outermost ring designates the nominal (un-jammed) RADAR detection radius. The innermost circle represents the minimum radius that will be required by the strike aircraft. The dotted ring will vary in size and indicates that the requirements on jamming are functions of strike aircraft location, and thus time. Therefore the jamming requirements are a time dependent EM power allocation problem for the jamming vehicle(s).

The last method in the list above is **False Target Generation**. This amounts to sending signals to the RADAR that would be expected if targets were in predefined locations.

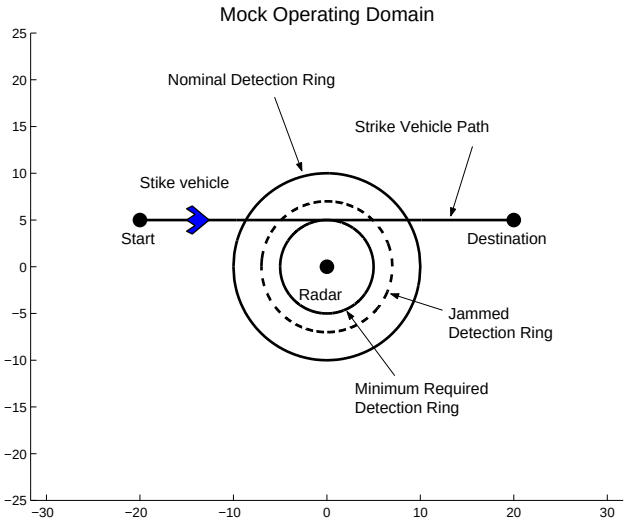

Fig. 4. Strike Aircraft Flying Near RADAR

For an aircraft to make a RADAR see multiple targets at ranges beyond the its own position, it simply sends delayed the signals back to the RADAR. This is done by using devices called *transponders* or *repeaters* which send back the type of signal expected by the RADAR. To insure that the signal structure expected by the RADAR is actually what is sent, devices called Digital Radio Frequency Memory (DRFM) can be used which record a digital representation of the signal to insure maximum fidelity of the signals transmitted back to the RADAR. If the structure of the signal can be anticipated by an aircraft, a signal can be sent in advance of the incoming RADAR illumination and cause the RADAR to *see* targets at closer range than that of the actual aircraft also. However, since many of today's RADAR systems are *pulse-to-pulse* agile, they are able to change their pulse characteristics preventing one from confidently anticipating pulse structure. In this case, the jamming aircraft would need to be closer to the RADAR than the false targets that are being created. In order to be believable, the range of the false target would need to be within the *burn-through-radius* of the RADAR, which in turn requires the jamming aircraft to be within this range. Thus, aircraft creating false targets would be vulnerable to threats.

It is also possible to make RADARs see targets at angles different from the line-of-sight (LOS) to the jamming aircraft. To achieve this, the jamming aircraft sends EM into a sidelobe of the RADAR. Since the RADAR assumes reflected energy is returning through its main beam, the angle to the perceived target is different from the LOS from the RADAR to the jamming aircraft. In order to cause this *angle* deception, the jamming aircraft must know the location of the main beam so that energy can be sent in to the same sidelobe consistently. Given the low gain of the sidelobe, the jamming aircraft must be able to supply

enough energy to overcome the attenuation. Also, robustness of sidelobe jamming of the EA vehicles to sidelobe notching and cancellation that might be done by RADARs is of concern.

The issue of sidelobe jamming requires the jamming aircraft to know its LOS with respect to the RADARs main beam and the lobe structure of the RADAR to maintain an angular orientation that will fool the RADAR. It also requires the jamming aircraft to maintain a distance from the RADAR that allow sufficient EM energy to enter the RADAR receiver. Thus, in the context of control, we have a path planning problem.

With the ability to generate false targets at ranges beyond the range of the jamming aircraft and within the main beam and sidelobes of the RADAR, the jamming RADAR can produce a large number of false target to confuse a RADAR system. The next issue, and the cooperative nature of this part of the control problem, is that of correlating the false target information sent to one RADAR by one jamming aircraft, with information sent by other jamming aircraft to different RADAR systems which overlap the same area. If this is not done, a RADAR system acting within an IADS could discard the track because it provides inconsistent information.

V. Cooperative Control of UAVs

Cooperative control of UAVs is an active area of research and a variety of applications, problem formulations and algorithms have resulted. A cooperative rendezvous problem has been addressed by McLain and Beard as a constrained optimization problem where multiple UAVs attempt to minimize accumulated exposure to RADARs while attempting to rendezvous at a specified location at the same time [5]. Their approach relied on Voronoi diagrams, and path refinement to generate *flyable paths* and path deviations were added to consume slack time and make vehicles arrive simultaneously. Nygard et al. addressed a Wide Area Search Munition (WASM) task by treating it as a capacitated transshipment problem (CTP) [6]. In order to optimally assign vehicles to tasks, a constrained linear program is solved. Schumacher et al. [7] addressed the WASM problem by combining variable-length path planning algorithms with iterative network flow to generate a complete assignment and path solution. Biologically inspired research from swarm behaviors has led to stability theorems and path planning algorithms applicable to UAVs [8]. Stochastic Dynamic Programming has been used to produce paths for cooperative search using UAVs [9]. The cooperative control areas just sited become formulations of a constrained optimization problem where one is attempting to derive algorithms that minimize time, fuel, threat exposure, or to maximize the performance, duration, coverage, etc.

Although the specific problems considered in the research mentioned above have no direct link to EA, the algorithms to perform a similarly formulated constrained optimization problem could be very similar. The motivation here, is to consider technology that could, with considerable additional development, be used on existing and future UAVs. More specifically, the desire is to apply existing algorithms and develop new ones, for generic, highly abstracted scenarios involving teams of unmanned Electronic Combat Air Vehicles (ECAVs) acting against networks of RADAR systems.

VI. UAV Role in EA

The investigation of use of multiple unmanned air vehicles (UAVs) to deceive RADAR systems is a relatively new area of study within the broader context of cooperative control and cooperative path planning. Use of small UAVs (tens to hundreds of pounds gross weight), military funding of larger UAV platforms, and potential use of unmanned decoy platforms to deliver EM has spurred interest in how multiple vehicles might be utilized for EA. With greater capabilities for autonomous operation emerging, cooperative and coordinated actions of groups of UAVs could have a synergistic effect.

Since UAVs can be smaller and have reduced safety considerations, they have the potential to change the complexion of the EA. By being smaller, the UAV may be more stealthy and less vulnerable to enemy weapons. Because they are smaller and unmanned they will likely be considerably cheaper alternatives to manned aircraft.

There are a number of tactics for performing EA using EW aircraft acting independently or in a loosely coupled way. However, it is conceivable that a variety of entities could be used to perform EA. UAVs could act with one another and within a larger framework. Since UAVs are cheaper, they may present a low cost part of EA within a ”system of systems” approach. Use of teams of UAVs doing stand-in jamming in close proximity to RADARs could be very effective if they are able to coordinate their activities and positions with each other and with other systems involved in EA.

To make teams of UAVs a low cost solution, cost associated with the UAVs themselves must be kept low. The drawback to having smaller EA assets with low unit costs is that the capabilities of each unit will be reduced. The amount of EM power produced by each vehicle, the frequency options, and the ability to direct the EM will likely be much less than that of conventional manned platforms. However, due to the quadratic benefit of range for jamming, UAV jamming may be of greater importance.

Intelligence Preparation of the Battlespace (IPB) will provide information regarding location of enemy assets [10] such as RADAR sites, however, there may be RADARs that are mobile which may *pop-up* without warning during a SEAD mission. The likelihood and number of these types of events would also be provided with the enemy assessment part of the IPB. These mobile sites are generally triggered to become active when they have been prompted by other RADARs. Part of the utility of unmanned vehicles is that they can be used, without placing people in harms way, as

decoys to cause RADARS to turn on, thus giving away their locations. Use of UAVs in this way could be choreographed into an EA plan to allow resources to exploit the opportunity to obtain accurate information.

UAVs could provide additional degrees of freedom for SEAD planners, however a larger solution space without guidance for optimal use could be no benefit or simply add to the *fog of war*. Therefore, tools for use of UAVs, as well as tools for all layers in a system of EA assets, would be required. Because solution to a complete EA problem could involve so many assets, the ensuing optimization problem would likely be too unwieldy to attack in its entirety. A set of integrated algorithms and heuristics would be needed to address the entire problem.

VII. Key areas

Within the branch of EW dealing with non-destructive, non-lethal SEAD there are two basic approaches. The first is what we will refer to as *deception* (sometimes called *technique jamming*). The second method involves EM energy as noise seen by the RADAR. We will refer to the second method as *EM jamming*. UAVs could provide a means for achieving many EA goals, however algorithmic solutions would need to be incorporated that are capable of working within the computational limits imposed by a UAV.

Both of the EA methods defined above assume that the locations and characteristics of the RADARs are known. There will most often be unknown or mobile RADARs that will complicate the EA problem. However, UAVs could play a role in information gathering for unknown RADARs and also take such factors into consideration when doing EA missions by having additional UAVs positioned. Determination of the location of RADAR sites could be determined using multiple vehicles to gather direction information. UAV decoys could be used to distract RADARs or cause unknown enemy EM assets to activate and reveal their location. By cooperatively positioning UAVs in orbits and fusing observations, the ellipse of error probability could be minimized.

In the remainder of this section this paper we describe some work done in the area of deception, and describe some noise jamming problem possibilities. At this point it should be noted that these two approaches as formulated here, may or may not have operational relevance. There may be better uses for assets positioned reasonably close to the enemy. However, regardless of operational relevance, these formulations provide a means for defining cooperative control problems which are pervasive for use of UAVs in EA.

A. Deception

For the deception, we consider two different problem formulations where Electronic Combat Air Vehicles (ECAVs) are used create *Phantom tracks* (RADAR target trajectories which do not really exist). In figure 5 we see a situation where the objective is to employ four ECAVs, using time

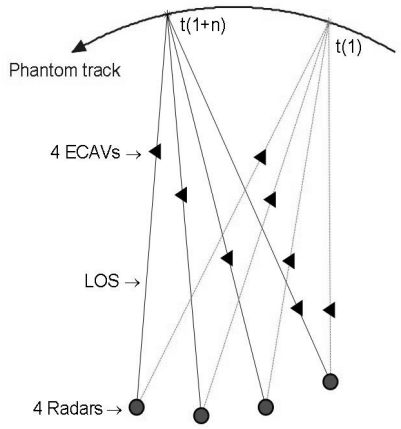

Fig. 5. Deception of 4 RADARs using 4 ECAVs

delay of the return radio frequency signal, to deceive four RADAR sites into believing that a Phantom aircraft exists at a range beyond the ECAVs. The ECAVs are assumed to be stealthy (unseen by the RADAR), each ECAV is able to direct a return signal to one of the RADARs that will not affect the other three RADARs, and the RADARs are assumed to correlate their information. The trajectory (track) of the Phantom is shown as a continuous path and the control problem is one of ECAV path planning where the geometry largely dictates the ECAV trajectories, i.e. the ECAVs are required to remain on the LOS between one RADAR and the Phantom. Two points on the Phantom path are noted at times $t(1)$ and n steps later at $t(n+1)$ to illustrate how the geometry influences the ECAV paths. To the extent that the velocity limits and dynamics of the ECAVs are observed, the ECAVs are free to position themselves on the LOS like beads on a string. This problem structure and these assumptions abstract the electronics involving RADAR and leave a tightly coupled path planning problem.

The geometry of one UAV and one RADAR with respect to a reference azimuth is shown in figure 6. The trigonometric relationships show the Phantom and ECAV angular rate and range rate in terms of velocity vectors. From the geometry of this figure, one can show that the RADAR can be induced to see a desired Phantom velocity vector by an infinite number of ECAV velocity vectors. If one assumes a constant ECAV speed, then the a desired Phantom velocity vector results in a uniquely determined angle, θ_E. If constraints are placed on the ECAV turn rate and velocity, there will be annular regions where the Phantom could fly within a defined time step.

In the first of the two approaches defined here, we desire an optimal combination of Phantom and ECAV trajectories, while in the second approach, we wish to find solution which is feasible. In both cases we assume that

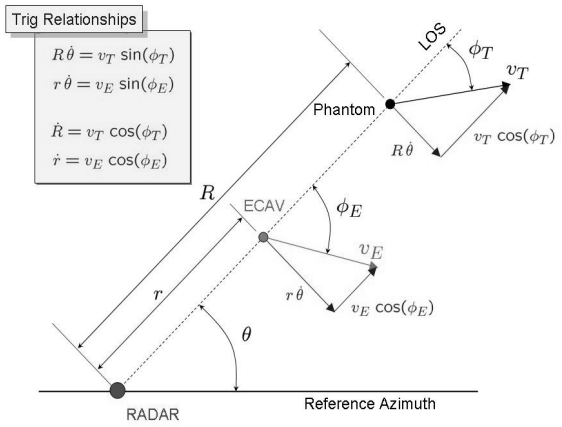

Fig. 6. Deception Problem Geometry

the necessary information is communicated without error or delay. However, for the feasible solution approach, the information that would need to be communicated is considerably less than that required for the optimal approach. Both approaches assume that velocity constraints exist for both the ECAVs and Phantom, and that the dynamics of the ECAVs impose turn rate restrictions. Both sets of results also assume that the ECAVs start at locations that result in a coherent Phantom track, i.e. one that is correlated for each RADAR, and that the ECAVs delay the RADAR signal by the proper amount of time to place the Phantom at the correct range.

1) Optimal Approach: The objective of the path planning control algorithm is to have each ECAV maintain a path on its own RADAR-Phantom LOS with the smallest cost possible. The approach to the path planning problem taken in this section of this paper is to determine what might be done to find optimal paths neglecting the issues relating to communication of information between ECAVs. Thus, each ECAV operates in a decentralized, but redundant fashion, using global information. To provide an optimal solution to the deception problem, we define a cost function that includes terms that penalize undesirable characteristics of both the Phantom track and the ECAV tracks. In qualitative terms, the approach defined in this section of this paper allows the ECAVs to negotiate a solution which produces *believable* Phantom tracks, is able to do so for a long period of time, and does not make excessive demands on the ECAV dynamics.

The qualitative requirements are put into a quantitative form using a multi-objective cost function. Physical and dynamics limitations are greatly penalized (soft constraints) and a additional terms are used to penalize undesirable behavior of the Phantom and ECAVs. To obtain the results described here, a receding horizon approach was taken where an optimal set of ECAV paths was computed for a prediction horizon of predefined length, and then *flown* for a fraction of that time (the control horizon).

To understand the rationale behind the cost function used let us first consider the geometry shown in figure 7. This figure shows three RADARs, the Phantom, and three ECAVs on the RADAR-Phantom LOS. It is desired that the RADARs be deceived into thinking that the Phantom flies through the waypoint on its way to the endpoint. Because constraints can sometimes make it costly to have the Phantom exactly follow prescribed paths or hit waypoints precisely, a *valid waypoint region* is defined. If the Phantom can be made to fly through these regions, this is more acceptable than constraint violation or extremely high costs [11].

The cost function used for this work contains a number of separate terms representing both local and global aspects of the problem. In mathematical terms, we define a *combined* cost function, J_C, which includes penalties due to the behavior of both the ECAVs and the Phantom. Using the nomenclature shown in figure 7 the cost is written as

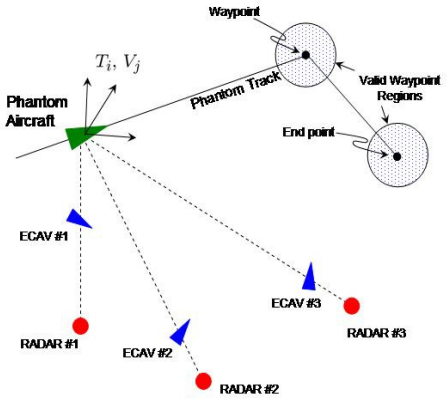

Fig. 7. Optimization Problem Geometry

$$J_C(\psi_i, V_j) = J_P(\psi_i, V_j) + \sum_k J_{E_k}(\psi_i, V_j) \qquad (1)$$

where J_P represents the costs associated with the Phantom track, J_{E_k} is the cost incurred by the k^{th} ECAV to maintain the Phantom, and each of the terms is parameterized by the Phantom Track, ψ_i, and the Phantom Velocity, V_j. The J_P part of the combined cost can be thought of as *global* because it's influenced by all the ECAVs. The J_{E_k} part of the combined cost can be considered *local* because it's determined by each ECAV and is driven by the individual ECAV paths.

To be evaluated, the cost function shown in equation 1 requires that permutations of speed and direction be *computationally flown out* and that this cost information be communicated. Based on the cost analysis, done by each

ECAV using the same data, the *best* Phantom path is chosen. Given this negotiated Phantom path, the ECAVs all fly their own calculated trajectory. More information regarding this work can be found in [11].

2) Feasible Approach: For this work, the objective was to attempt to determine what could be done if one was willing to settle for solutions which are feasible, but not necessarily optimal [12]. Such an approach would require less inter-UAV communication which might be better in some operational contexts. The objective of a feasible solution is to create the same type of coherent Phantom track described for the optimal approach above and depicted in figure 5, however only feasibility with respect to dynamic and velocity constraints are considered. As seen in figure 6

$$\dot{\theta} = \frac{v_T \sin(\theta_T)}{R} = \frac{v_E \sin(\theta_E)}{r}. \tag{2}$$

Given the *present* position of the Phantom, the *present* position and orientation of an ECAV, a maximum and minimum velocity magnitude and direction of the ECAV, and using the relationship shown in equation 2, one can calculate an annular region where the Phantom could *feasibly* be positioned within a given time step. In order to *move* a Phantom from an initial position to a waypoint or final destination, each ECAV communicates four numbers (minimum and maximum ECAV angle and velocity) with each other ECAV. Each ECAV then uses this information to calculate the intersection of the annular regions. By choosing the direction closest to the direct path to the waypoint (or destination), the Phantom moves in the desired direction.

Such a solution degenerates to a straight line path from start to finish if such a Phantom path is feasible for all the ECAVs. Figure 8 shows results of a simulation where four ECAVS are deceiving four RADARs into seeing a Phantom track moving from a starting point to a final destination. In figure 8 the Phantom Track and ECAV trajectories are shown and dotted lines are shown as LOS between the RADAR and Phantom for the start and final points of the track. For the first segment of the simulation, the Phantom trajectory is a sequence of small line segments forming an arc. However, once the ECAVs reach positions and orientations that allows them to induce a straight line Phantom trajectory to the destination, the Phantom trajectory becomes a straight line. Details of this work can be found in [12].

B. EM Jamming

EM Jamming is radiation, or re-radiation of EM, to prevent an adversary from effectively using the spectrum. Cooperative control of UAVs to support EM Jamming would amount to operating UAVs so that they are collectively able to raise the noise level seen by the RADAR above a required threshold. This would require the location, orientation and flight path of UAVs to be such that the needed EM can be delivered to a RADAR site.

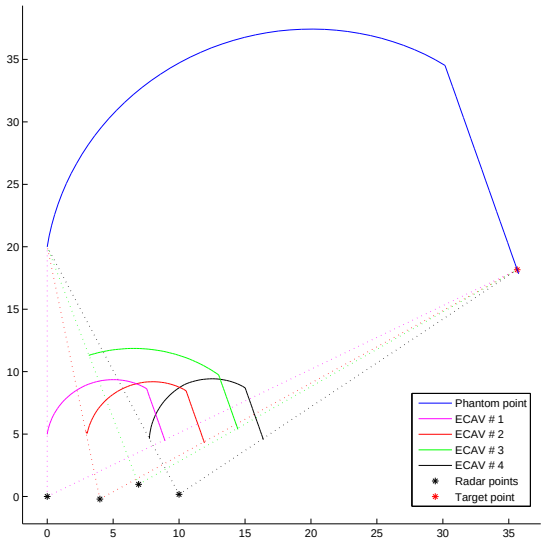

Fig. 8. Feasible Solution for Phantom Trajectory Generation

One could formulate this problem as separate path planning and resource allocation problems. Due to the fact that proximity is the dominant factor for effective jamming power, and given the possibility of numbers of UAVs, one could formulate the jamming problem as one of time dependent resource allocation for UAV positioning and an underlying path planning algorithm to maintain EM jamming power on a target. The need for a time dependent nature of the resource allocation stem from the fact that the assets to be protected will require ingress and egress protection as they move through an enemy IADs.

VIII. Conclusion

A brief background and operational context have been provided for the Electronic Attack problem. The application of UAVs for EA has been motivated and some technical challenges for implementation have been described. Issues related to cooperative control of groups UAVs have been highlighted within the context of some abstract EA scenarios. Relevant issues that have not been addressed include imperfect communications where only local information or corrupted information is available for decisions, planning and control. Also unaddressed is the fact that UAVs for EA will most often be part of a larger EA framework where multiple vehicles are utilized. However, a complete EA solution hierarchy utilizing many types of vehicles will make for a large optimization problem that will require decomposition into a number of smaller problems. Also left unaddressed in this paper is the plethora of research and development done in the area of RADAR electronics which are very important for a comprehensive treatment of

EA. The scenarios used are not meant to be of operational significance, but are instead intended to illustrate salient features of cooperative control of UAVs for EA.

REFERENCES

[1] "Jttp for joint supression of enemy air defenses," July 1995, http://www.dtic.mil/doctrine/jel.

[2] G. Stimson, *Introduction to Airborne RADAR*. Scitech, 1998.

[3] "Joint doctrine for electronic warfare," April 2000, http://www.dtic.mil/doctrine/jel.

[4] J. A. Tirpack, "The new way of electron war," *Air Force Magazine*, December 2004.

[5] T. McLain, "Cooperative rendezvous of multiple unmanned air vehicles," *AIAA Guidance, Navigation, and Control Conference*, August 2000.

[6] K. Nygard, P. Chandler, and M. Pachter, "Dynamic network flow optimization models for air vehicle resource allocation," *Proceedings of the Automatic Control Conference*, June 2001.

[7] C. Schumacher, P. R. Chandler, and S. R. Rasmussen, "Task allocation for wide area search munitions via iterative network flow," *Proceedings of the American Control Conference*, pp. 1917–1922, 2002.

[8] V. Gazi and K. M. Passino, "Stability analysis of swarms in an environment with an attractant/repellent profile," *Proceedings of the American Control Conference*, pp. 1819–1824, 2002.

[9] M. Flint, M. Polycarpou, and E. Fernandez-Gaucheand, "Cooperative control for multiple autonomous uavs searching for targets," *Conference on Decision and Control*, pp. 2823–2828, 2002.

[10] L. C. M. T. Satterly, L. C. D. Stubbs, M. G. D. Gilbert, M. C. L. Iler, and C. K. B. Glen, "Intelligence preparation of the battlespace - an airman's introduction," *Air and Space Power Chronicles - Chronicles Online Journal*, July 1999.

[11] M. J. Mears and M. R. Akella, "Deception of radar systems using cooperatively controlled unmanned air vehicles," *International Conference on Networking, Sensing and Control*, March 2005.

[12] D. Maithripala and S. Jayasuriya, "Radar deception through phantom track generation," *Proceedings of the American Control Conference*, June 2005.