PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

Cooperative cognitive electronic warfare UAV game modeling for frequency hopping radar

Mark Rahmes, Dave Chester, Rich Clouse, Jodie Hunt, Tom Ottoson

Mark Rahmes, Dave Chester, Rich Clouse, Jodie Hunt, Tom Ottoson, "Cooperative cognitive electronic warfare UAV game modeling for frequency hopping radar
," Proc. SPIE 10640, Unmanned Systems Technology XX, 106400O (3 May 2018); doi: 10.1117/12.2291554

SPIE.

Event: SPIE Defense + Security, 2018, Orlando, Florida, United States

Cooperative Cognitive Electronic Warfare UAV Game Modeling for Frequency Hopping Radar

Mark Rahmes, Dave Chester, Rich Clouse, Jodie Hunt, Tom Ottoson
Harris Corporation, Space and Intelligence Systems, Melbourne, Florida 32904

ABSTRACT

In modern warfare concepts, the use of wireless communications and network-centric topologies with unmanned aerial vehicles (UAVs) creates an opportunity to combine the familiar concepts of wireless beamforming in opportunistic random arrays and swarm UAVs. Similar in concept to the collaborative beamforming used in ground-based randomly distributed array systems, our novel approach improves wireless beamforming performance by leveraging cooperative location and function knowledge. This enables the capabilities of individual UAVs to be enhanced, using swarming and cooperative beamforming techniques, for more-effective support of complex radar jamming and deception missions. In addition, a dedicated System Oversight function can be used to optimize the number of beamforming UAVs required to jam a given target and manage deception assets.

Keywords: Electronic Warfare, Optimal Game Theory, Decision Making, UAV Swarming.

1. INTRODUCTION

Multiple-input–multiple-output (MIMO) radar uses orthogonal signals to obtain the phase delay for each transmitting/receiving antenna pair and, thus, improve direction estimation accuracy. The relatively new MIMO Orthogonal Frequency Division Multiplexing (MIMO-OFDM) radar leverages recent advances in sampling technology. OFDM is a method for encoding digital data on multiple carrier frequencies. Increasingly, researchers have been exploring how MIMO-OFDM can improve dual-antenna radar performance over conventional single-antenna systems [1].

Here, we look at ways to apply cooperative game theory in a swarm of UAVs to jam and deceive a MIMO-OFDM radar. For this discussion, "cooperative" describes the ability of individual vehicles in a UAV swarm to work together to optimally jam or deceive a radar, while "cognitive electronic warfare (EW)" is defined as a priori noisy channel information obtained by eavesdropping on frequency hopping radar.

Electronic Counter Measures (ECM) are actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum, while Electronic Counter Counter-Measures (ECCM) are actions taken to ensure friendly use of the electromagnetic spectrum against EW. Jamming is an example of an ECM attack on a radar. Electronic Protection (EP) involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.

One of the most effective strategies to improve survivability of equipment and personnel is to implement a Digital Radio Frequency Memory (DRFM) deceptive jammer. A DRFM jammer can retransmit a manipulated replica of a received signal as the basis for its attack. The retransmitted signal, by appearing to be a legitimate signal, can fool the signal processing functions of the target radar.

The use of wireless communication techniques and network centric topologies with unmanned aerial vehicles (UAVs) within modern warfare concepts makes it possible to utilize new distributed beamforming applications. The objective of this research is to combine the concept of wireless beamforming successfully used in ground-based opportunistic random arrays with the concept of intelligent UAV swarms. Extensive research has already assessed the feasibility and advantages of opportunistic arrays for a single platform, with distributed beamforming techniques widely applied by many researchers. The use of UAV swarm concepts for a widely dispersed, wirelessly networked opportunistic array has the potential to realize significant performance gains over single platform-based opportunistic arrays. Among the major challenges are synchronization and localization, which result from the highly dynamic, mobile nature of the network topology [3].

Unmanned Systems Technology XX, edited by Robert E. Karlsen, Douglas W. Gage,
Charles M. Shoemaker, Hoa G. Nguyen, Proc. of SPIE Vol. 10640, 106400O
 · doi: 10.1117/12.2291554

2. SYSTEM MODEL

An enhanced multi-UAV, intelligent swarm system is dynamic and flexible, enabling it to respond to emerging conditions that could impact network performance. Its ability to dynamically adjust individual parameter weightings to account for changing conditions ensures that UAV positioning decisions account for both the immediate needs of a given network node and the overall needs of the network. These conflicting needs form the basis for applying a game-theory-based scenario in which each UAV is alternately pushed or pulled over time to new positions until reaching a steady state or Nash Equilibrium.

A high-level, multi-UAV system block diagram is presented in Figure 1. As shown, individual parameter weights are initially optimized through training. Once the parameter weights are determined, the system uses them to support control decisions that optimize UAV positioning. Q-Learning can be used to optimize weights for each input parameter.

A System Oversight function can be used to determine the optimal number of UAVs required to participate in jamming at a given distance. One or more of the UAVs in the swarm may be better suited to performing a task other than jamming or deception. System Oversight uses weighted criteria to drive decisions for each UAV regarding what tasks would be optimal for the overall swarm.

An innovative game-theory-based decision algorithm, which we refer to as Genetic Linear Optimization (GLO), can be created that combines genetic algorithms (GA) and linear optimization. Currently, the use of GA is a very popular approach to optimizing characteristic values for a given situation, and it can play an important role in the development of test scenarios to optimize values across multiple degrees of freedom. In addition, the use of game theory enables analysts to develop models that better predict actual behavior. In the genetics portion of the GLO algorithm, an iterative process keeps track of distance to target and recalculates signal strength as a function of distance.

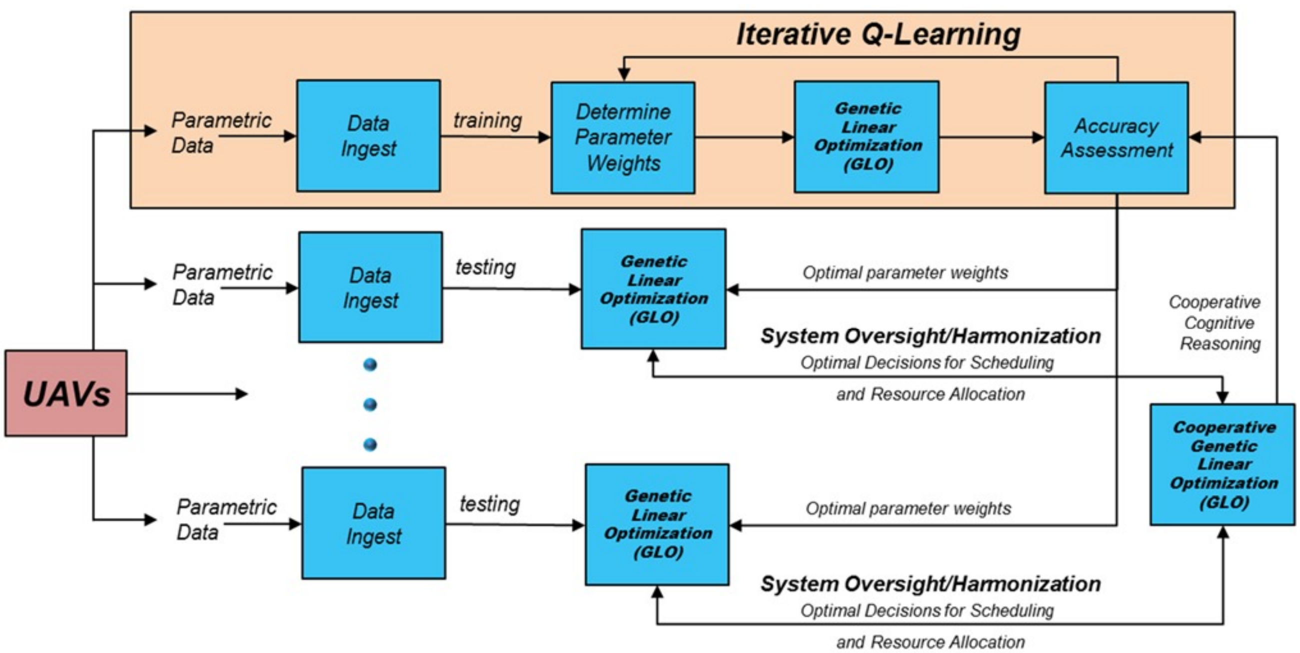

Figure 1. System Block Diagram

3. GAME THEORY

Three games can be modeled in the EW environment. The first of these is the two-player decision matrix or Electronic Order of Battle (EOB), as shown in Figure 2.

	Jam	Deceive	Fire Control Radar	Detect and Track With Radar	Update TDS	RF Comms	Collect Sigint	Eaves drop
Jam (Responsive Spot Noise)		1		1	1			
Deceive (False Targets)	1		1			1	1	
Fire control Radar		2		2	2			
Detect and Track With Radar	2		2			2	2	
Update Tactical Data System (TDS)	3		3			3	3	
RF Comms		3		3	3			
Collect Sigint		4		4	4			
Eavesdrop								1

Figure 2. Example Electronic Order of Battle

The second game to be modeled is concerned with determining which function to choose based on electronic signal inputs received. In Figures 3 and 4, we illustrate a game architecture with two one-sided game scenarios, each of which requires that choices be made in the rows and that input parameters be entered in the columns.

The third game to be modeled (and perhaps the most significant) involves decisions made by a radar jammer or deceiver as to the frequency band on which to operate. We model the knowledge of the correct next frequency to jam based on eavesdropping information on frequency hopping radar as a function of signal to noise ratio.

To validate the enhanced performance of an intelligent UAV swarm in jamming and deception, we conducted two modelling experiments. In Experiment 1, we modeled the performance of a UAV swarm in jamming a frequency hopping radar. In Experiment 2, we modeled the performance of a UAV swarm in deceiving a frequency hopping radar. In each, we used linear optimization based on its widely acknowledged usefulness as a mathematical procedure for determining optimal allocation of limited resources.

Linear optimization is also particularly useful for solving game theory problems and finding optimal strategies. In a classic game theory scenario, a conductor must choose from a set of actions, the consequences of which depend on either certain states about which the conductor is not completely informed (i.e., subjective uncertainty) or on the result of random, independent processes (i.e., objective uncertainty) [6]. The “expected utility” forms the basis for a prediction of what the conductor will choose in an uncertain environment.

The use of probabilistic predictions and game theory is an essential element of many decision-making applications, characterized by the need to compute expected utilities for mutually exclusive objectives to optimize performance. The Nash Equilibrium is synonymous with objective function or value of the game in an integer linear program. For each of the two modeling experiments, we used a primal-dual interior-point algorithm, which must be feasible for convergence. The primal standard form, which is used to calculate optimal tasks and characteristics, is [8]:

$$\begin{gathered} minimize\ (f * x)\ s.t. \\ A * x = b \end{gathered} \tag{1}$$

$$x \geq 0$$

The dual problem, which is used to calculate optimal parameters, is:

$$\begin{gathered} maximize\ (b' \ * y)\ s.t. \\ A' \ * y + s = f \\ s \geq 0 \end{gathered} \tag{2}$$

Since we know the optimal direction decision based on detected channel information from the frequency hopping radar, we can find the associated parameter (column), given the decision (row).

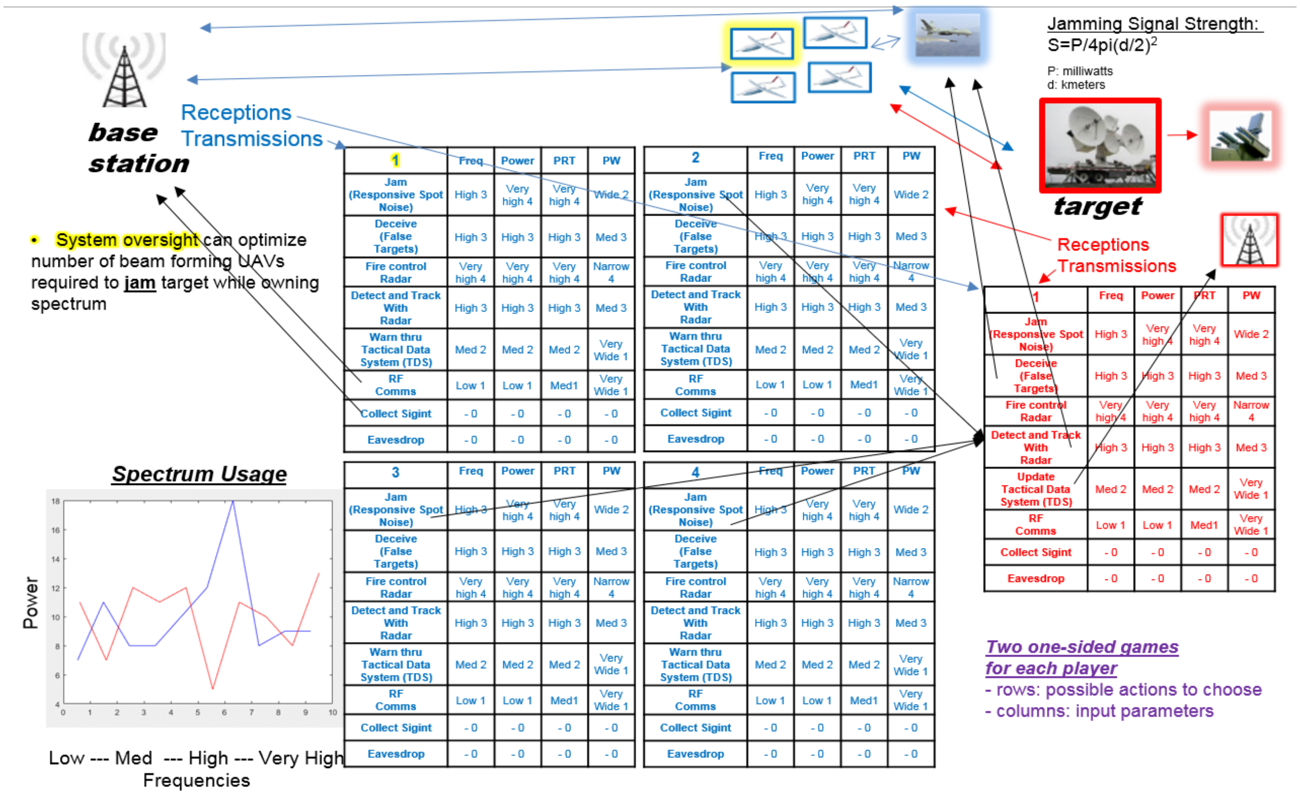

Figure 3. Modeling Experiment 1: Jamming

Figure 4. Modeling Experiment 2: Deception

4. SIMULATIONS

We modeled the interaction between a radar and a jammer or deceiver as a Markov Decision Process. A Markov game is characterized by an action space, immediate reward for each player, and a state space with the transition probabilities. The decision epochs are at the end of the time slot, and the effect takes place in the beginning of the next time slots [2]. We used subset summing of the feasible regions in a linear program to decide which frequency bands each UAV would jam or deceive. The associated reward matrix uses rows as the decisions for each band and columns for the channel state information. Figure 5 shows an example of cooperative UAVs jamming a frequency hopping radar. In our scenario we have four UAVs such that each can jam one channel.

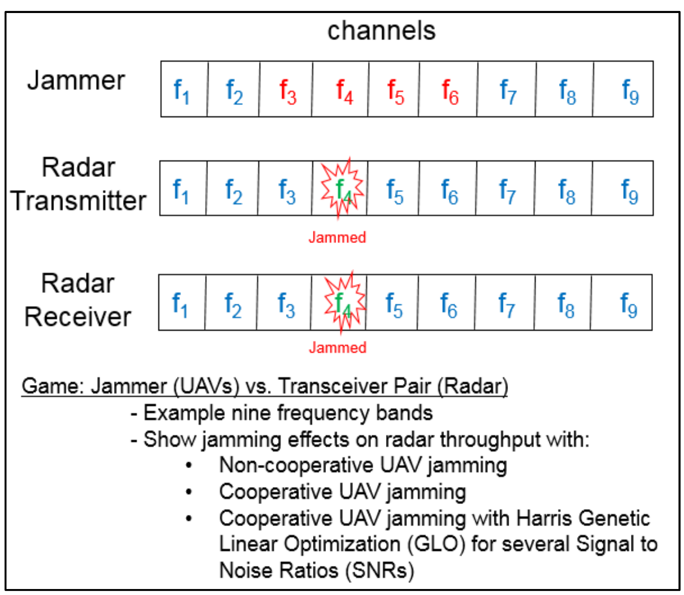

Figure 5. Cooperative UAV Jamming vs. Frequency Hopping Radar

If the jammer knows the strategy of its opponent (i.e., radar), is can devise a more-effective attack strategy. The strategies of both the jammer and the radar depend on their specific hardware and computational capabilities. For instance, if the transmitter and jammer are each equipped with a single radio, they can transmit on only one channel per slot. In such a single-channel scenario, i.e., K = 1, the transmitter can only evade the jammer by adapting its transmission rate [2]. However, when multiple channels are available, the optimal transmitter strategy is to hop from channel to channel to evade the jammer. In response, the jammer would also switch channels to find the transmitter. When the jammer is aware that the transmitter may switch channels, a naive jammer attack strategy would be to randomly choose a channel, with equal probabilities in each time slot [2]. As the jammer sequentially cycles through (or sweeps) all the K channels, it can jam one channel in each slot. The sweep jammer can also randomize its hopping pattern each time it successfully jams the transmitter or completes one sweep cycle to make its sweep patterns unpredictable. For the transmitter, hopping is uniform in that each time the transmitter decides to hop, it chooses a channel with equal probability [2].

We consider a more-sophisticated jammer attack strategy in which the jammer acquires, by eavesdropping, noise-corrupted knowledge of the transmitter's Radar Channel State Information (CSI), which includes transmission rate, power, and channel frequency. We further consider a proactive jamming attack, in which each UAV jammer continuously jams one radar channel every T seconds. At a given range, each UAV can jam one radar frequency band every T seconds. UAVs cooperate to ensure that each one jams a different radar band or, in some cases, the same band, e.g., when more power is needed for maximum effectiveness.

For our simulation, we use nine frequency bands and four UAVs. We model the performance with three different signal-to-noise ratios (SNRs) to account for noisy channel information obtained through eavesdropping on the frequency hopping radar. The model is a form of cooperative game theory for a swarm of UAVs that have jamming capability.

We then compare cooperative game theory performance and UAV cooperation without game theory. Cooperation consists of ensuring that each UAV jams or deceives a different frequency band. Non-cooperative performance is modeled as each UAV randomly jamming or deceiving one of the nine possible frequency bands of the frequency hopping radar.

Deceptive jamming is a standard technique for an intelligent target to spoof a radar system. Specifically, the target first intercepts the radar's transmitted signal and then broadcasts it with a controlled delay. Given that the deceptive broadcast pulse is usually stronger than the direct reflection detected by the receiver, the radar system will register an additional *false detection*. This false detection can confuse the tracker, resulting, for example, in a waste of weapons for a ground combat system. In modern radar system design, despite efforts to refine anti-jamming countermeasures, the ability to effectively distinguish a deceptive jammer from a legitimate signal remains an important area of research [7].

In assessing deception performance, it is important to consider the number of consecutive deception frames. This metric was chosen based on the extensive body of research on countering DRFM-based jamming using sophisticated processing to recombine multiple frames, which enables the validity of a radar contact to be checked and a determination to be made of the real target vs. false targets [4], as shown in Figure 6. Therefore, the larger the number of consecutive deception frames, the better the performance of the deception jammer, as a function of time. This is apparent in that the longer a radar contact is accepted as valid, the more likely it is that opposing forces will choose to act on that false information.

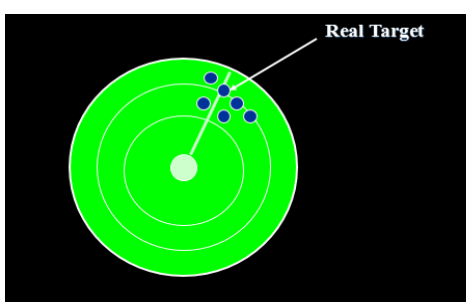

Figure 6. Multiple False Targets

Basically, DRFM signals serve as an effective jamming source that can cause the radar operator to wrongly interpret the data or accept misleading information from the radar. DRFM is applied to cause the radar to lose its tracking on the target. DRFM is a device with high-speed sampling digital memory for storage and recreation of RF signals to deceive radars. In a DRFM, the input RF is first down-converted in frequency and then sampled with a high-speed analog-to-digital converter. The samples are stored in memory and can be manipulated in amplitude, frequency and phase to jam the radar signal. The stored samples are later recalled from memory, processed by the digital-to-analog converter, up-converted and transmitted back to the radar. After uniform phase quantization applied to the signal by the DRFM, the jamming signal is transmitted back to the radar with an increasing delay. For example, in a range gate stealer system, DRFM is used to delay the signal linearly to create a constant range false target [5].

The performance results are shown in Figure 7 for jamming scenarios and in Figure 8 for deception. Jamming performance is measured as one minus the radar throughput, with lower throughput indicating a higher jamming success rate.

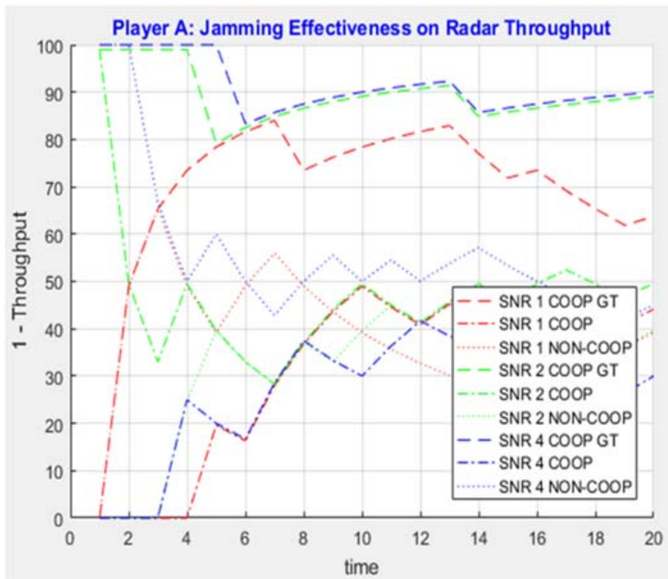

Figure 7. Jamming Effectiveness

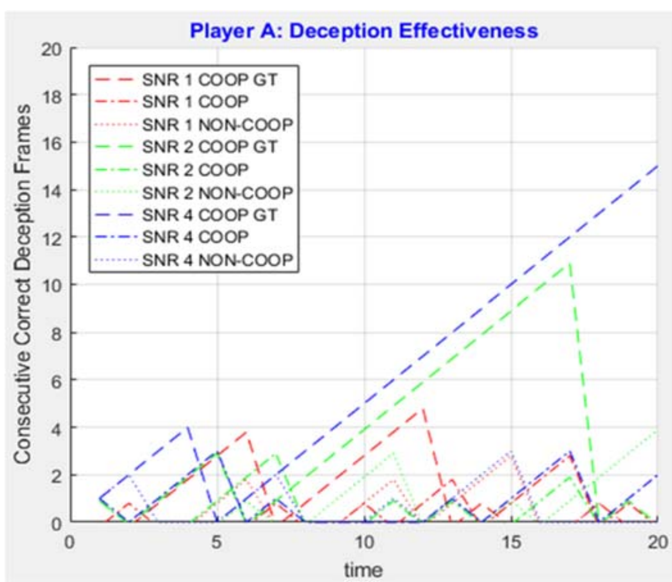

Figure 8. Deception Effectiveness

As expected, the higher the SNR, the better the performance. And, clearly, the cooperative game theory approach (i.e., COOP GT) performs better than cooperation alone or non-cooperation (i.e., COOP and NON-COOP, respectively).

System oversight of system processing can help determine the best task for each UAV at a given time. For example, the closer a jamming UAV gets to its target, the less power it needs to accomplish its jamming mission. This creates an opportunity for a UAV to multi-task, supporting other important functions, such as communicating situational awareness or updating tactical data link information.

It is essential to determine how much power would be required for jamming or deception at a given distance. The single most important factor in that determination is free-space path loss (FSPL), which is the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction. We model FSPL signal attenuation using the inverse square law:

$$S = P/(4 \pi d^2) \tag{3}$$

where S is the power spatial density in watts per square meter. P is the equivalent isotropically radiated power in watts referenced to 1 meter.

5. CONCLUSION

An innovative, self-forming, self-organizing, cooperative, autonomous system of distributed UAVs can be realized wherein each UAV acts cooperatively. This will enable a multi-UAV network to jam or deceive a radar target in a way that is more resilient, resulting in enhanced levels of performance. We have simulated the UAV tasks based on decisions from game theory, with each vehicle working cooperatively to achieve optimal performance. A cooperative System Oversight engine was also implemented to ensure that the entire system functions optimally. This results in overall enhanced system performance.

REFERENCES

[1] K. Han and A. Nehorai, "Joint frequency-hopping waveform design for MIMO radar estimation using game theory," 2013 IEEE Radar Conference (RadarCon13), Ottawa, ON, 2013, pp. 1-4.

[2] Hanawal MK, Abdel-Rahman MJ, Krunz M. Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems, 2014.

[3] Kocaman, Ibrahim. Distributed beamforming in a swarm UAV network. Diss. Monterey Ca. Naval Postgraduate School, 2008.

[4] Y. Li, X. Jia, Y. Chen and C. Yin, "Frequency agility MIMO-SAR imaging and anti-deception jamming performance," 2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS), Beijing, 2014, pp. 1-4.

[5] C. M. Kwak, "Application of DRFM in ECM for pulse type radar," 2009 34th International Conference on Infrared, Millimeter, and Terahertz Waves, Busan, 2009, pp. 1-2.

[6] Roy, O. (2010). Epistemic Logic and the Foundations of Decision and Game Theory. Journal of the Indian Council of Philosophical Research, 27(2), pp. 283–314.

[7] X. Song, P. Willett and S. Zhou, "Jammer detection and estimation with MIMO radar," 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, 2012, pp. 1312-1316.

[8] Wayne Winston. (2003). Operations Research Applications and Algorithms 4th. Edition.