Near-Neighbor Based Systems Engineering of Swarming Networks: A Case Study

Jerry A. Krill, Michael J. O'Driscoll, Kenneth W. O'Haver, and Eric R. Farmer
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road, Laurel, MD 20723-6099

Abstract. Traditional systems engineering is tailored to systems with complex subsystems having well-described physical and functional attributes and interfaces. Moreover, a network system generally features precisely defined communication signal and data protocols. We submit that development of swarming networks that do not exhibit such discrete linear attributes represents a new class of systems that can benefit from a new approach to systems engineering methodology. We will describe the new systems engineering concept of "near-neighbor interaction zones" for systems engineering processes and apply this approach to a case study of one such system, an automated swarming intrusion detection network to alleviate the monitoring burden on security operators. The result is a large-scale complex system that is potentially more tractable and efficient to develop and operate from a human cognition perspective.

Introduction

A system is described [Kossiakoff and Sweet, 2003] as "a set of interrelated components working together toward some common objective." As we know, the engineering of such systems becomes "interesting" when the system is complex with many components and functional interactions. The process for systems engineering (S.E.) is well defined and well used, e.g., [INCOSE Handbook]. However, the engineering of swarming systems requires a departure from classical S.E. The approach to S.E. of swarming emergent systems should reflect the nature of such systems. Therefore, we begin with a discussion of their characteristics.

This class of systems is analogous to swarming organisms in the natural world, as has been described, for example, [Johnson, 2004] related to ants that exhibit very simple behaviors and interactions and yet act collectively with intelligence in performing the functions of nest sustainment and replication. Johnson [2004] describes emergence as "solving problems by drawing on masses of relatively stupid elements, rather than a single intelligent executive branch." He describes "bottom-up" intelligence, or self-organization, and he discusses it in areas that run the gamut from slime mold to human brains and software. Whether investigating swarm cells, neurons, or zeros/ones, the important aspect in swarm logic is that the basic elements think and act locally but their aggregated behavior demonstrates a collective, beneficial effect. This local behavior not only motivated our conception of a swarming intruder network, but also motivated what we consider a novel system specification and design approach.

Human engineered systems also exhibit an analogous collective wisdom demonstrated vividly every day in events such as betting pools, the stock market, and jelly bean guessing contests where crowds are the basic norms. But for these crowds to be effective they have to have

certain characteristics: diversity of opinion, independence, de-centralization, and aggregation. In short, there must be a free exchange of ideas, with many conflicting views expressed, and the answer must be an aggregation of those views, not just a group consensus. This aggregation appears to arise from individuals engaged in dialog with their peers, their "near-neighbors."

Table 1 summarizes some distinct differences between the design of this type of system and the more traditional systems such as spacecraft and communication systems.

Table 1: Design Differences between Conventional Systems and Swarming Networks

Attributes	Conventional Systems	Swarming Networks
Control	Can be physically localized	Apparent and distributed
Predictability	Generally deterministic/linear	May appear ad hoc/nonlinear
Interfaces	Precise specification/protocol	Very simple/inferential
Design	Complex subsystems	Extreme component count
Reconfiguration	Discrete design features	Inherent/no explicit design
Scalability	Scale by x 2's with design modifications	Scales by x 10's without design modifications
Design hierarchy	Typically multiple levels (system to components)	Typically fewer levels

The following summarize behaviors of interest in swarming systems.

- Swarming – the ability of the system to focus in an ad hoc manner based on an input to any individual component
- Distributed Intelligence – whereas no single element possesses the information or orchestrates a response, a collection of system elements appears to respond intelligently
- Inferential Signaling without Protocol – the nontraditional conveyance of information that may consist of inferences from simple signals or behaviors, i.e., "body language" from near-neighbors
- Chaotic – the system seemingly behaves in a manner that borders on unpredictable or unstable
- Emergent – effects and behaviors are appearing at higher levels that are not explicitly evident in lower level components.

Relevant papers were presented at the INCOSE International Symposium held in Utrecht, Netherlands, in June 2008. Of specific interest to us was a panel on "How to Engineer the Emergent Behavior of a System of Systems." The panel's challenges included "how to understand the initiation mechanism of the emergent behaviors for a particular system architecture model so that the resident beneficial or harmful emergent behavior can be enhanced or mitigated with selected changes in the current system architectural model."

It boils down to the general question of coping with the conception and development of swarming emergent systems such as these when the theory does not exist. Is experimentation the only way, and with a systems of systems, would one be able to experiment sufficiently due to problems of complexity, scale, and economics to satisfy oneself of a reasonable level of understanding of the system from the standpoint of performance and risk?

We will propose a system model as the basis for a new tractable systems engineering approach to swarming systems. We will exercise the model and approach in a test case, a swarming network that is presently in exploratory development.

Test Case: Swarming Intruder Sensor Network

In part, to explore potential advantages of swarming networks, as well as the S.E. implications, the authors conceived of a swarming intruder detection and tracking sensor network [Krill et al., 2007]. This section describes the concept, top-level requirements, and interaction requirements. In the section that follows we will discuss a new "near-neighbor interaction in zone" approach to the S.E. of such a swarming system. This is our initial attempt to develop a simplified means of addressing these challenging entities.

Figure 1 illustrates the essential elements of the network. A large number of nodes, disguised here as "pebbles," is randomly distributed, e.g., air dropped or individually placed, with the condition that there is sufficient density so that each pebble is within sensor and communication range of its near-neighbors. The pebble field surrounds an installation, pipeline, or building to be protected.

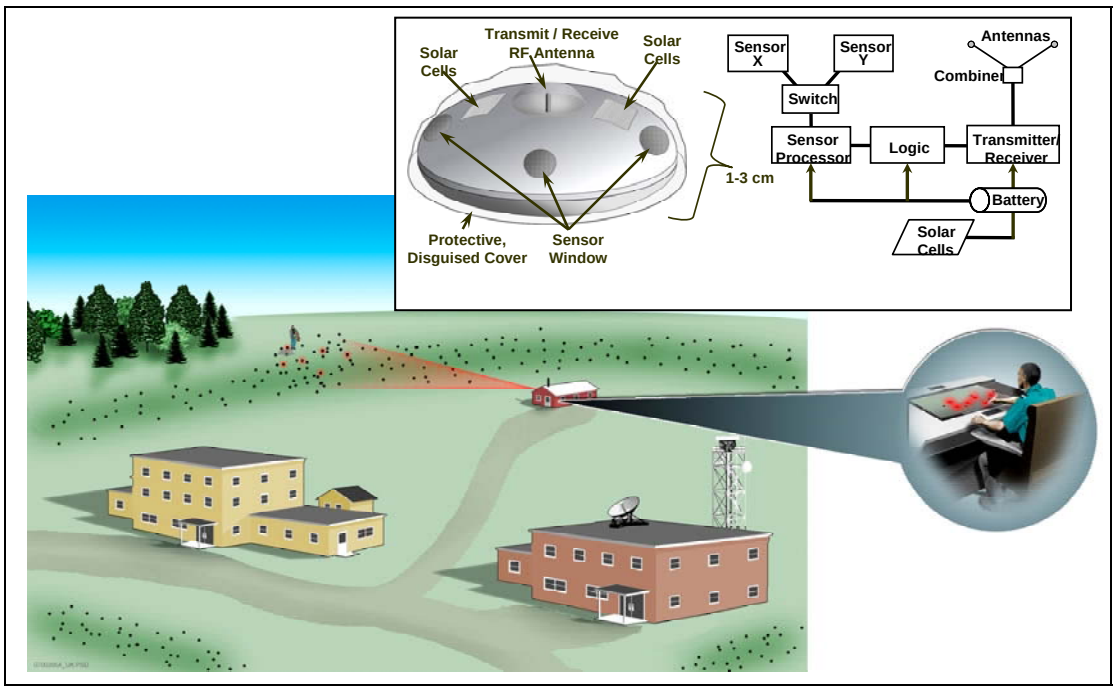

Figure 1. Elements of the Network

Each pebble is set to a "cold" sensor detection threshold for the requisite probabilities of detection (P_d) and false alarm (P_{fa}). An intruder entering the pebble field will be detected by the sensors of one or more pebbles' sensors as the intruder passes within their sensor detection ranges. A pebble making a sensor detection will emit a microwave "cue" tone of only sufficient power to be detected by near-neighbor pebbles. Those pebbles detecting the cue tone through their communication receivers will set their sensor detection thresholds to a more sensitive "cued" threshold so they are more likely to detect the nearby intruder. The "cued" pebbles that also detect the intruder, in turn, transmit cue tones to be received by their nearest neighbors. A cue tone will continue to be transmitted by a pebble only while the sensor detection continues and for several seconds after the detection. The pebble then resets to its cold sensor detection threshold if it was previously cued.

From a distance, e.g., several kilometers, a remote receiver with a directional antenna sweeps across the pebble field. If it detects sufficient power in the cue tone band via its antenna beam,

indicating that some minimum number of pebbles is emitting cue tones, the receiver makes a "detection" and alerts an operator. The operator observes the detection history on the display screen as shown in Figure 1. If the history appears to be consistent with an intruder approach path, the operator may alert security forces or cue video cameras to gain more information.

In this manner the field pebbles appears on the monitor to "swarm" around the intruder location. This swarming network is sufficiently automated that fewer operators would be required, for example, compared to operators continually monitoring a bank of video screens from a network of cameras.

Requirements. For this system, our key top-level requirements are:

- Provide a probability of intruder detection of 0.9 and probability of false alarm of 10^{-7}.
- Localize an intruder to within 100 meters.
- Alert an operator within 1 second of the first detection of signals by a remote receiver.
- Provide automatic scalability from tens of pebbles to millions.

Figure 1 shows a general design configuration for a pebble with one or more sensors and a communications monopole antenna to ensure full spatial coverage in a protective, perhaps disguised, cover. Several types of sensors could be used on different pebbles in the same field, for different fields, or even on the same pebble, including small microphones, infrared detectors, or video. Consideration could also be given to a new detection approach involving intruder blockage of a microwave illumination tone at a different frequency from communication tones as described in [Krill et al., 2007].

The cueing mechanism reduces false alarms and power consumption relative to an uncued system according to analysis [Krill et al., 2007]. The pebble block diagram is also shown in Figure 1. As the functionality of each sensor node is identical and since the communication of a detection does not require handshaking, the interfaces and functions are very simple per sensor node as identified in Table 2.

Table 2: Pebble Interface and Functional Requirements

Interface	**Functions**
Sensor Nodes	
Transmit cue tone upon detection Receive cue tone Receive command tone	Detect intruder Set/reset detection threshold Receive and transmit cues
Remote Monitor	
Receive cue tones via directive beam Transmit command tone via directive beam	Determine if adequate total power from sensors to declare intruder detection Locate intruder direction Change state of receiving nodes via command tone length or frequency

Because there is no handshaking protocol or modulated data and because the transmission power levels are tailored to limit detection range, the resultant loosely coupled system elements accommodate extreme scaling in pebble coverage area.

While working through the design requirements allocations and tailoring the interfaces, it occurred to us that such a swarming system can be designed using an approach that mirrors its near-neighbor behavior. As noted above, in nature, swarming instincts generally respond and

stimulate their near-neighbors. We therefore postulated that, rather than detailed design activities for all interfaces and functions, simple, near-neighbor "zones of influence" can be defined as the basis for the design of the system. As in nature, each type of element is influenced by and/or influences a specific neighborhood, but with little or no inherent coupling between neighborhoods. Our premise is that if we can define and design the requirements in these localized zones, the entire scalable system is specified. We have termed this approach "Near-Neighbor Based" systems engineering.

Near-Neighbor Based Interaction Zones

We view our swarming pebble network as being comprised of three interaction zones as illustrated in Figure 2.

- Zone Type 1: Near-neighbor signal cueing communications range (meters)
- Zone Type 2: Sensor detection range (meters)
- Zone Type 3: Remote monitoring and control from long (multi-kilometer) distances

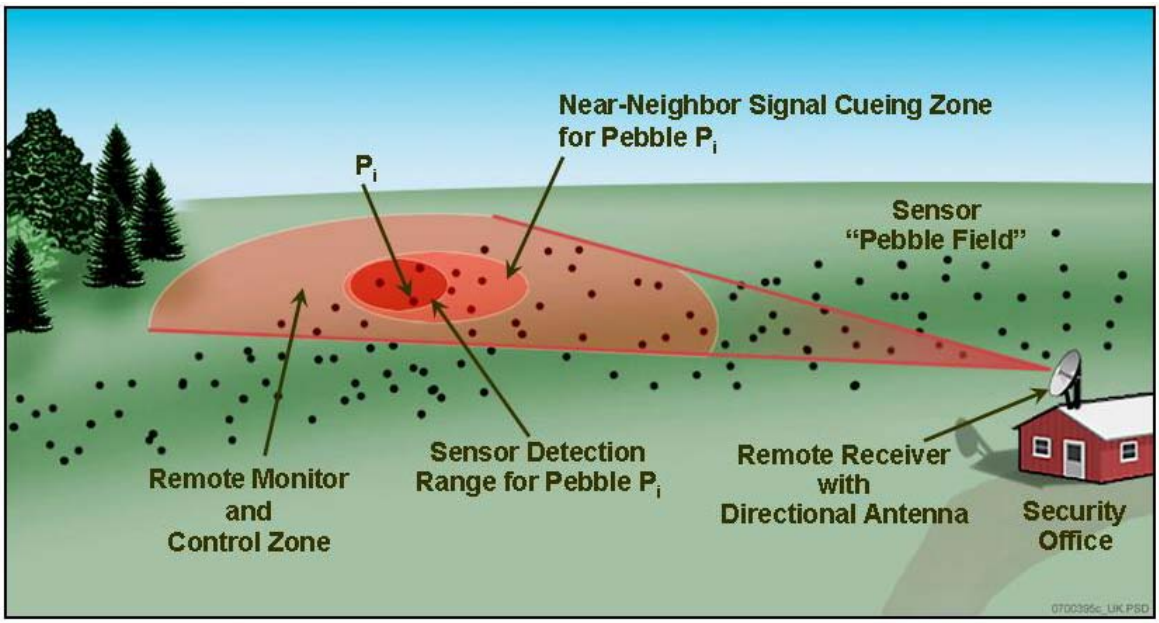

Figure 2. Near-Neighbor Based Interaction Zone

For Zone Types 1 and 2, we specify the behavior for nodes only between immediate neighbors and design to actually extinguish influence beyond the immediate neighbors. This is analogous to natural swarming in nature, and the extinguishing characteristic is essential to providing spatially rich emergence, which can then be geographically monitored within Zone Type 3.

By specifying only the details of activities within these "zones of influence," we can characterize the system. Further, as we shall see, simple modeling of the uncertainties within the zones can allow system design adjustments that ensure inherent stability within the swarming net. Thus, relatively simple modeling coupled with rather simple confirmation tests can yield results directly traceable to zone performance and, therefore, to total system performance.

We now describe the requirements for the interaction zones shown in Figure 2, based on analysis and experimentation to date [Krill et al., 2007, 2008].

For the case of cueing neighboring pebbles upon a cold detection by a pebble, the cue is accomplished by emitting a radio frequency (RF) tone that is then detected by a neighboring pebble. To prevent a "swarming instability" in which all pebbles are eventually cued and yield an excessive false alarm rate, cue tones last only a few seconds (we have initially selected 5 seconds) before turning off and will not be reinitiated unless another detection is made. We begin by assuming that this RF tone-based cueing system is designed to provide 12 dB or greater signal-to-noise ratio (SNR) out to a range of 10 meters. Signal detection theory can then be used to determine probabilities for detection and false alarms (according to classical "ROC" curves). For 12 dB or greater SNR, the probability of detection (P_d) is greater than 0.93 for a probability of false alarm (P_{fa}) of 10^{-4}. If we assume that the tone signal variation with range corresponds to free-space spreading, the design would then provide a 6-dB SNR at a range of 20 meters, which corresponds to a P_d of ~0.1 for a P_{fa} of 10^{-4}. For free-space propagation conditions, nearest neighbors will have a high P_d while the next closest neighbors will have a significant reduction in detection probability. More severe propagation conditions would further reduce the detection probability beyond the nearest neighbors. Coupled with the interfaces defined for each pebble transceiver, this analysis specifies the influence of neighbors. Table 3 indicates the simple results.

Table 3: Zone Requirements for Zone Type 1 Near-Neighbor Pebble Cueing

Communication tone detection	10 m (12-dB SNR)	20 m (6-dB SNR)
	$P_d > 0.9$; $P_{fa} = 10^{-4}$	$P_d < 0.1$; $P_{fa} = 10^{-4}$

The feasibility of the design parameters described above have been demonstrated by design analysis [Krill et al., 2007]. An RF tone-based signaling link that provides 12-dB SNR at 10 meters can be achieved with pebble design parameters (i.e., transmit power, antenna gain, noise bandwidth, integration time, propagation conditions, etc.) that are conducive to the small size, low cost, long battery life that the concept requires. We have also conducted propagation and connectivity experiments of pebble-to-pebble communications using commercially available wireless sensor modules to emulate the pebbles [Krill et al., 2008]. These experiments, which provide the basis for the propagation conditions assumed above, demonstrated free-space spreading for elevated modules and more severe attenuation with range for modules located on the ground.

For the case of sensor detection of an intruder, the detection could be accomplished by a number of means, including passive audio detection, passive infrared detection, or detection of blockage on an RF illumination signal [Krill et al., 2008]. We begin by assuming that a detection system is designed to provide 12 dB or greater SNR out to a range of 10 meters from the intruder location. As before, signal detection theory can then be used to determine probabilities for detection and false alarms. For 12 dB or greater sensor SNR, the "cold" probability of detection is greater than 0.93 for a P_{fa} of 10^{-4}. If the sensor has been cued, we assume that it lowers the detection threshold to increase the P_d. For example, for a 12-dB SNR, the detection threshold can be lowered to achieve a P_d of 0.995 for a P_{fa} of 10^{-2}. If the detection is increased to 20 meters, the same sensor system provides a 6-dB SNR, assuming that free-space spreading propagation conditions are in place. In this case, the cold P_d is 0.1 for a P_{fa} of approximately 10^{-4} and the cued P_d is 0.5 for a P_{fa} of 10^{-2}. These passive sensor detection results are summarized in Table 4.

Table 4: Example Requirements for Pebbles in a Passive Detection (Type 2) Zone

	Passive Detection at 10 m (12-dB SNR)	**Passive Detection at 20 m (6-dB SNR)**
Cold detection	$P_d > 0.9$; $P_{fa} = 10^{-4}$	$P_d < 0.1$; $P_{fa} = 10^{-4}$
Cued detection	$P_d > 0.99$; $P_{fa} = 10^{-2}$	$P_d < 0.5$; $P_{fa} = 10^{-2}$

Finally, Table 5 indicates the zone (Type 3) conditions for the remote monitor. From [Krill et al., 2008] a straightforward analysis showed that a remote receiver receiving the incoherent sum of five or more pebbles represents an acceptable likelihood of intruder presence.

Table 5: Requirements for Remove Monitor/Control Zone

Monitor probability of detection for at least five pebbles >0.9 for specified range region
With associated probability of false alarm of 10^{-4}
With localization of transmitting pebbles within 100 m CEP* of centroid

*CEP – Circular Error Probable

Coupled with the interfaces defined for each pebble transceiver (Table 2), Tables 3 to 5 specify the influence of neighbors.

Initial concerns were that propagation variations among pebbles in a field could cause a substantial deviation in zone detection ranges between pebbles. For example, experiments reported in [Krill et al., 2008] indicate that pebbles on the ground will exhibit rapid propagation loss beyond a few meters under normal propagation conditions, but elevated pebbles can exhibit free space (R^{-2}) propagation loss, which is the basis for the zone requirements described previously. For microwave tones propagation ducting conditions can occur, where guided wave conditions could increase propagation to lower loss than even free space [Krill et al., 2008]. Preliminary design analysis indicated that designing a signal strength measurement capability would allow pebbles to periodically automatically adjust receiver gain, receiver sensitivity, or transmit power to maintain the zone conditions described previously, essentially 12-dB SNR at 10 meters. This form of “automatic gain control” appears to provide an emergent design feature allowing the pebble field to maintain the requisite performance by adapting to propagation loss variations over space and time. It also allows for random placement over terrain.

Simulation of Swarming Network

On the basis of these zone conditions assuming the automatic gain control (AGC) feature, a simulation was developed to gain further first order insights into the swarming behavior. The simulation that was created to perform some initial investigations into the system performance is not unlike Mitch Resnick’s “Star Logo” simulation [Johnson, 2004] that mimics the behavior of slime mold, except that the sensors in our simulation are not allowed to move. Basically, an array of pebble sensors is modeled, each with a very simple rule set governing its behavior, such that the collective behavior could indicate “intrusions” that could be remotely monitored.

The simulation models the case of 20,164 pebble sensors distributed in an evenly spaced grid over 1 square kilometer (for a grid spacing of 7 meters). A mouse interface allows insertion of a moving intruder through the grid. At each time step, the state of each sensor is updated to reflect intruder detections, communication among nearby sensors, false alarms, etc. The result is effectively a cellular automaton with the mouse-controlled intruder as an additional external stimulus.

Each sensor's cued "alert state" is indicated by gray levels. On the simulation display each white pixel indicates a "cold" sensor that is not detecting or receiving, and each black pixel indicates a sensor that has detected an intruder and is emitting a tone to be received by nearby sensors that in turn respond by temporarily decreasing their detection threshold to the cued setting, indicated by the gray pixels.

At each time step, the process of updating the state of each cell in the automaton – that is, each sensor in the grid – consists of a single Bernoulli trial. The probability of "success" (i.e., detection or false alarm) for a sensor is determined by two factors: the current detection threshold state of the sensor ("cold" or "cued") and a unit step function (detection or false alarm) of range to the intruding target, if one exists. This detection range is fixed at 10 meters. Given the resulting probability of success, a uniform pseudo-random number in the unit interval determines whether the sensor has a detection or false alarm. In the event of a detection or false alarm, the detection threshold state of all sensors within communication range (also fixed at 10 meters) is lowered to the "cued" state.

Some performance parameters of the sensor are adjustable by slider controls. The default "cold" probabilities of detection and false alarm are 0.9 and 10^{-4}, respectively. In the "cued" state, with a lowered detection threshold, the default probabilities of detection and false alarm are 0.99 and 10^{-2}, respectively. The detection and communication ranges of each sensor are fixed at 10 meters, the effect being that the neighborhood of influence of each sensor is fixed to a subset of eight surrounding sensors.

Figure 3 shows by black and gray dots, pebbles currently detecting (black), those receiving a cue (light gray) but not yet detecting, and those that have detected (both cued and cold) within the cue tone persistence time (dark gray). The dashboard on the right allows the simulation user to adjust the key zone design parameters of cold and cued pebble communication tone detection and false alarm probabilities over one and several orders of magnitude, respectively. Also shown is a sliding adjustment of cue tone persistence time ("cued timeout") from zero to 5 seconds.

The simulation was useful in testing the stability of the network. Figure 3 illustrates a typical picture of the display with random false alarm detections for a pebble packing density of 7-meter separation. The lack of correlation (less than five pebbles detecting in a local area) indicates that a remote receiver with a directive antenna beam that scans over the pebble field would not receive the requisite signal level to expect an intruder.

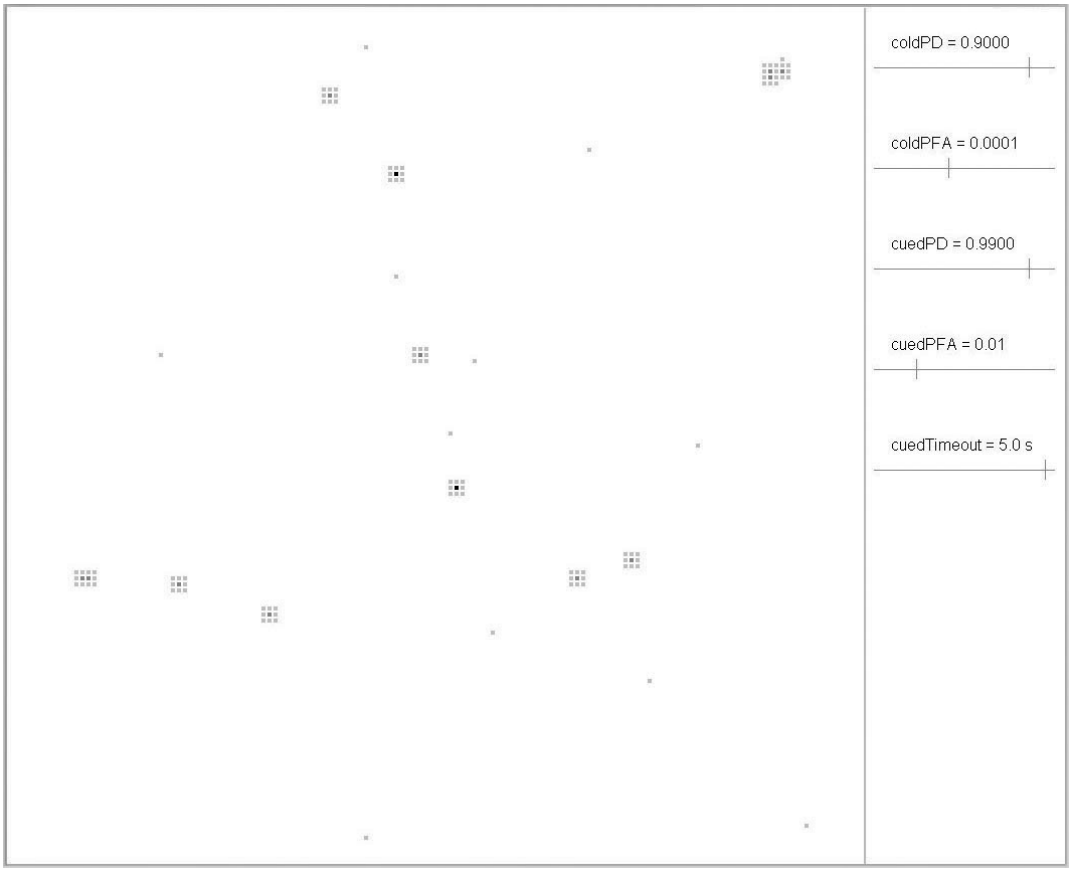

Figure 3. Simulation False Alarm Snapshot at Zone Requirements to First Order

Figure 4 illustrates a snapshot of an intruder moving through the sensor field after having entered the field some time ago. The sensors having detected the intruder leave a persistent trail of transmitting pebbles for a directive remote receiver to detect. If the remote receiver display retains the pebble transmission history and its beam directivity is sufficiently focused, then the track of an intruder could be followed.

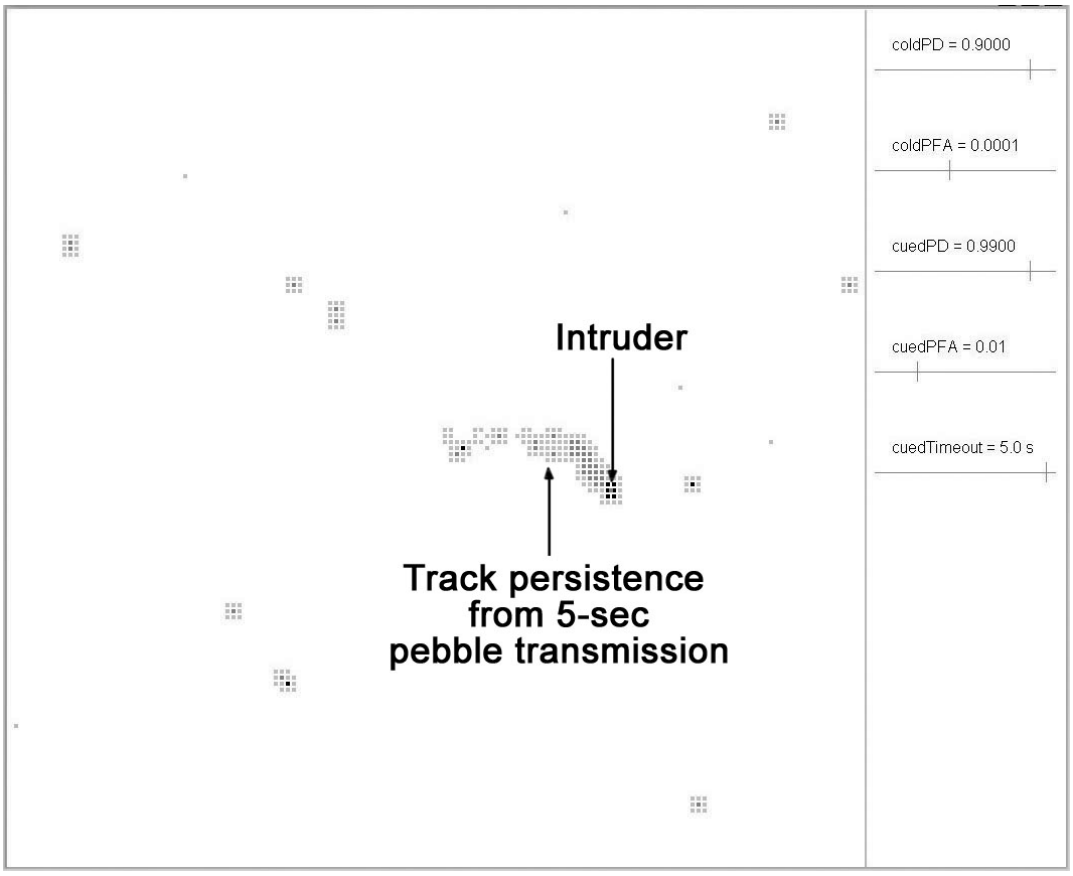

Figure 4. Simulation of False Alarms and Intruder Track for Nominal Zone Requirements

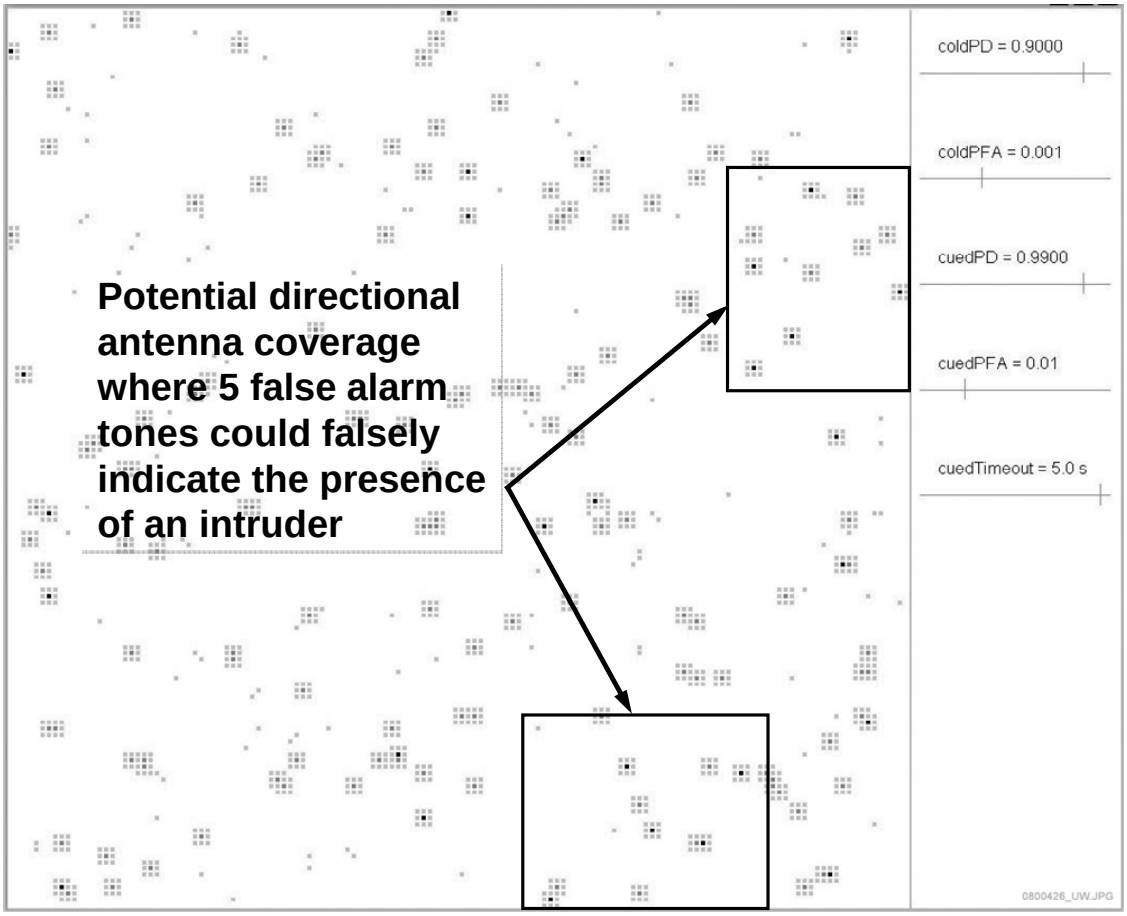

Figure 5. Simulation False Alarm Snapshot at 10 Times Higher Rate than Zone Requirement for Cold Detection

Figures 5 and 6 illustrate instabilities of the sensor field. Figure 5 shows the false alarms if the cold detection false alarm probability is increased by a factor of 10 from 10^{-4} to 10^{-3}. Enough individual false alarms occur that a directive remote receiver could be receiving a spatially correlated signal for a false intruder alert, as shown. Figure 6 is the case for which the cold detection false alarm probability is retained at the nominal 10^{-4}, but the false alarm probability for a cued detection is increased by a factor of 10 from 10^{-2} to 10^{-1}. Swarm "clouds" appear within seconds due to a high percentage of cued false detections. Moving these false alarm probabilities shown in Figures 5 and 6 back to their nominal value causes the sensor field to calm down to the picture of Figure 3 in a matter of seconds.

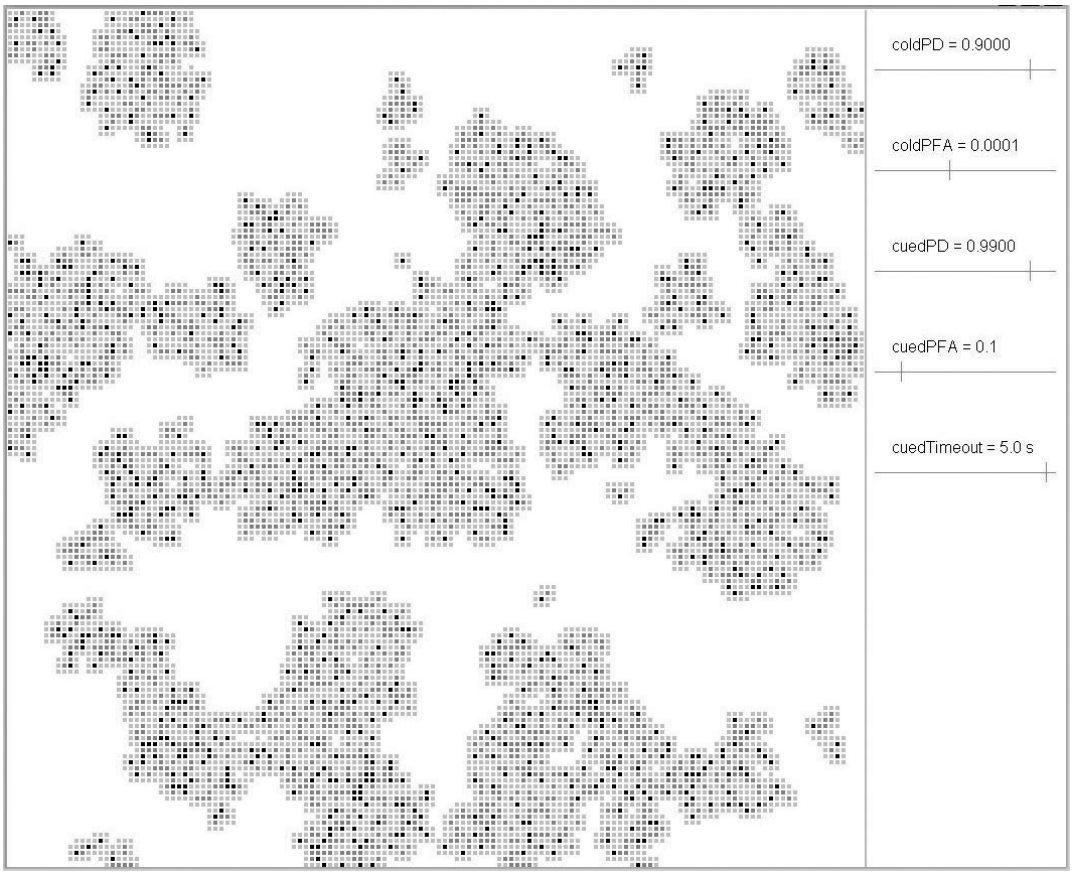

Figure 6. Simulation False Alarm Snapshot at 10 Times Higher Rate than Zone Requirements for Cued Detection

Other insights gained from the sensor net model include:

- The average separation between neighboring pebbles should not be so small that more pebbles than the nearest-neighbors can detect the cue tones. Otherwise, so many pebbles would be cued by a single cue tone that a "swarming instability" such as in Figure 6 could occur. On the other hand, too great inter-pebble distances approaching the communication zone range will provide insufficient inter-node interaction to respond to an intruder with sufficient cued detections. In other words, the model helps to verify the appropriate density of pebbles.
- Reducing the tone timeout from 5 seconds to 1 or 2 seconds cleans up the false alarm picture but further reduces the persistence of the track picture (Figure 4) at the remote receiver.

Summary

We have developed a specification and design approach for near-neighbor based systems engineering to advance the system engineering practice for swarming systems. We applied this approach to a new swarming network concept as a test case. Results for this test case indicate that the near-neighbor zone approach provides a tractable means to specify performance of the swarming network based on near-neighbor interactions. Straightforward analysis of these zones coupled with a statistical network model has allowed us to gain insights into such performance characteristics as network stability and response to an intruder. These insights coupled with specific field tests [Krill et al., 2008] have allowed us to specify the system

requirements and design. Planned continued development of this system will likely provide further insights into the sufficiency and benefits of the new approach.

Future Work

We intend to examine introduction of additional emergent features to the swarming intruder detection network. Additional features under our consideration, and key design issues, include:

- Kinetic response by pebble nodes – Pebble locomotion toward an intruder or transmission of tags or materials to "mark" the intruder for followup human inspection. Reaction distance and speed of response by the pebbles will impact network stability. For example, pebbles moving too quickly toward a detected intruder could expose patches of the sensor field to inadequate sensor density allowing a subsequent intruder to egress with lower sensor response performance.
- Diverse sensor types and performance zones – A diversity of sensor types (e.g., audio, infrared, optical) spread over a pebble field, each with a different detection range might provide better rejection of false alarms or provide provision, via correlation of detections from different sensors, to ensure that the intruder is appropriately identified as human (vehicle or on foot) versus, for example, a wild animal.
- Pebbles could be arrayed in concentric rings surrounding a protected site so that the outer ring provides an alert, the next ring in provides identification with a different suite of sensors, and, perhaps, an inner ring provides a response to inhibit the intruder, such as an audible alarm or nonlethal tear gas emission. In this manner such a "layered defense" swarming network would exhibit specialties in the pebble population not unlike insect hives and nests in nature.

For these features we plan to exercise the S.E. approach described in this paper. We will explore whether introduction of an increasing number of node types and behaviors can be addressed as a coupled superposition of coexisting swarming networks or whether all near-neighbor zone features must be addressed together to gain adequate insights into emergence stability and functional performance. We plan to report our findings as our systems engineering of swarming networks continues. This will include continued field testing of prototype elements as reported in [Krill et al., 2008] to validate dynamic behaviors in actual environments.

The question of the 2008 INCOSE panel, quoted previously, remains for the general case of more complex systems that exhibit emergent behavior such as a massive power grid, a MANET (Mobile AdHoc Network), or a complex defense system of systems such as the U.S. Army's Future Combat System (FCS). Emergent behavior for a power grid could take the form of propagating power variations as the network control mechanisms attempt to compensate for localized disruptions, resulting in grid power collapse. This appears to have occurred in the eastern United States in 1993, when not -understood events cascaded to cause this major disruption. For the MANET and FCS examples, our results for the pebble network indicate that local propagation outages, not easily modeled, can cause dissimilar behavior among system elements due to variations of information received by individual elements. Such dissimilar behavior among system elements might, in turn, lead to unwanted emergent responses. Our approach might provide an early means to anticipate such behavior and then lead to design measures, such as autonomy logic, to constrain unwanted behavior early in the development program. However, further investigation is required to address the value of generalizing the approach to such major systems of systems. In anticipation of considering our approach for more general problems, the following candidate heuristics are

offered for the general case of swarming, emergent systems.

- Design for local near-neighbor interaction zones.
- Create a statistical model to "tune" the inherent damping and amplified behavior by adjusting the near-neighbor design parameters.
- Conduct limited scope tests to verify key attributes of some behavior characteristics to ensure understanding of the environment.

Acknowledgment

The authors wish to thank Dr. Samuel Seymour for contributing the idea of a swarming "layered defense" as an additional network feature.

References

INCOSE 2006 Systems Engineering Handbook, Version 3, INCOSE-TP-2003-002-03, ed. C. Haskins.

Johnson, S. 2004. *Emergence*, Scribner.

Kossiakoff, A. and W. N. Sweet, 2003, *Systems Engineering*, Wiley.

Krill, J. A., M. J. O'Driscoll, K. W. O'Haver, and D. A. Day, "Swarming Network for Intruder Detection," 2007 Third International Conference on Intelligent Sensors, Sensor Networks, and Information Processing Conference, paper 1569058599, 3–6 December, Melbourne, Australia.

Krill, J. A., K. W. O'Haver, M. J. O'Driscoll, I-J Wang, and D. Lacanelli, "Prototype Design and Experimental Results for an Intruder Detection Swarming Network," 2008 Fourth International Conference, on Intelligent Sensors, Sensor Networks, and Information Processing Conference, paper 1569152080, 15–18 December, Sydney, Australia

Biography

Jerry A. Krill was appointed the Assistant Director, Programs at The Johns Hopkins University Applied Physics Laboratory in October 2005. Dr. Krill's expertise includes combat systems engineering, sensor and weapons networks, missile defense, over-the-horizon missile command and control systems, and microwave technology. Dr. Krill holds a Ph.D. in electrical engineering from the University of Maryland. He has served on studies for the Defense Science Board and Naval Studies Board. He holds 15 patents and has published over 100 articles and major documents.

Michael J. O'Driscoll has served in key management positions related to naval combat systems, command and control, and shipbuilding for 30 years. He retired from the Navy civilian sector as a member of the Senior Executive Service with the last post as Assistant Secretary of the Navy/RDA, Deputy Chief Engineer. Mr. O'Driscoll was a Senior Vice President/General Manager at Anteon and General Dynamics as head of the Combat Systems/Information Technology Group. Now in place at The Johns Hopkins University Applied Physics Laboratory, he is the Deputy Assistant Director for Advanced Concepts on the Director's Staff.

Kenneth O'Haver is a member of the Principal Professional Staff at The Johns Hopkins University Applied Physics Laboratory (JHU/APL). He received a Bachelor of Science degree from Virginia Tech and a Masters of Science degree from the Johns Hopkins University, both in Electrical Engineering. At JHU/APL, he leads research and development activities in

advanced radar system engineering and advanced technology development, including the areas of antennas, active phased arrays, digital receivers, advanced exciters, microwave subsystems and MMIC technologies, and power systems.

Eric R. Farmer is a senior mathematician at The Johns Hopkins University Applied Physics Laboratory. He received Bachelor of Science degrees in mathematics and computer science from Kansas State University, a Masters of Science in applied mathematics from the University of Illinois at Urbana-Champaign, and a Masters of Science in computer science from the Johns Hopkins University. He currently works in the Air and Missile Defense Department on sensor network modeling and simulation in large-scale parallel and distributed computing environments.