Presented at 2009 IEEE International Conference on Technologies for Homeland Security (HST 2009), Waltham, MA, May 11-12, 2009

Demonstration of Swarming Control of Unmanned Ground and Air Systems in Surveillance and Infrastructure Protection

John A. Sauter[a], Robert S. Mathews[a], Kris Neuharth[a], Joshua S. Robinson[b], John Moody[b], and Stephanie Riddle[c]

[a]TechTeam Government Solutions, 3520 Green Court, Suite 250, Ann Arbor, MI 48105, voice 734-302-5660, fax 734-302-5661, email [john.sauter, robert.matthews, kris.neuharth]@newvectors.net

[b]Augusta Systems, 3592 Collins Ferry Road, Suite 250, Morgantown, WV 26505, voice 304-599-3200, fax 304-599-3480, email [jrobinson, jmoody]@augustasystems.com.

[c]NAVAIR, 48150 Shaw Road, Bldg. 2109 Suite S211-21, Patuxent River, MD 20670, voice 301-342-8475, fax 301-757-2747, email stephanie.riddle@navy.mil.

Abstract—*The emergence of new risks to homeland security requires a greater reliance on innovative remote sensing and monitoring systems deployed on Unmanned Vehicles (UxVs) for protecting borders and critical infrastructure. Robust autonomous control technologies that can reliably coordinate these sensors and platforms are needed. We describe a class of algorithms based on digital pheromones that enables robust, complex, intelligent behavior. These algorithms have been implemented on a variety of UxVs and sensor platforms and demonstrated in surveillance and infrastructure protection applications. The algorithms autonomously adapt to a rapidly changing environment as well as failures or changes in the composition of the sensor assets. They can support mixed manned and unmanned teaming environments. An Operator System Interface (OSI) enables a single operator to monitor and manage the system. We describe the results from various tests and the challenges faced in implementing these algorithms on actual hardware.*

1. INTRODUCTION

The emergence of new global security risks threatens military and civilian installations. The entire international infrastructure for the production, storage, and transportation of material goods, energy, and information needs to be protected. The sheer number, variety, and size of these facilities preclude the use of conventional security approaches for protection. Unmanned remote sensing and monitoring systems offer a promising means to extend protection to more areas with limited human resources. Current unmanned systems typically require multiple operators for each platform. Future systems will require a single operator to monitor and manage dozens of platforms. This requires the development of innovative technologies in autonomous control, coordination, communication, and operator interfaces.

We describe a class of stigmergic algorithms based on digital pheromones for autonomous control. Examples from natural systems [1] show that stigmergic systems can generate robust, complex, intelligent behavior at the system level even when the individual agents are simple and non-intelligent. Digital pheromones are modeled on the pheromone fields that many social insects use to coordinate their behavior. In this paper we describe the use of digital pheromones to control and coordinate the actions of unmanned sensor systems in surveillance and facility protection. These swarming algorithms are designed to autonomously and dynamically adapt to a rapidly changing threat as well as failures in the system and changes in the composition of the sensor assets. They cooperate seamlessly with human patrols and monitoring personnel to create a comprehensive, coordinated security system.

In the following sections of this paper we introduce the surveillance and security problem and the requirements it places on the control system. We briefly discuss the pheromone algorithms used and the concepts behind the Operator System Interface. Finally we describe the results of tests of these algorithms in support of surveillance and security applications and offer some observations and conclusions.

2. DESCRIPTION OF THE PROBLEM

The need to cope with increasing security risks is placing more demands on security systems and personnel. Advanced sensor suites can support all aspects of the security task including Finding, Fixing, Tracking, Targeting, Engaging, and Assessing (F2T2EA). But the sheer number and size of the areas to be protected makes it economically infeasible to completely protect every asset with a full suite of security sensors. Similarly manning all these sensors is problematic. Having humans monitor all the video cameras and sensor feeds required to protect a wide area 24-7 is prohibitively expensive. In the future successful security systems will need to make better use of scarce sensor assets and rely less on human monitoring of raw sensor feeds. Autonomous mobile sensor platforms can take over the dull, dirty, and dangerous aspects of surveillance and facility security maximizing the sensor area covered and reducing reliance on human operators. Intelligent coordination and control of

those platforms maximizes their effectiveness by better managing limited sensor assets to protect against an intelligent adversary.

Facility Protection Example

In a typical configuration, aerial sensors on towers, tethered balloons, and Unmanned Aerial Vehicles (UAVs) provide broad area coverage in the vicinity of the protected area, pipeline, or border. Ground sensors or intrusion detection sensors may be deployed around the outside perimeter of a protected area to signal breaches. Visible/IR cameras and radar sensors may be used to identify and track intruders. Human, animal, and Unmanned Ground Vehicle (UGV) patrols cover the area inside the protected area. They provide a rapid response capability to further identify, interdict, or deter an intruder.

A trip from a ground sensor indicates a potential intruder. Ground sensors provide an approximate location and potentially a target type (such as biped or vehicle). Additional information must be obtained from the nearest sensor with the ability to more accurately measure location, heading, and speed and make a more positive identification of intruder type. Other sensors may be necessary to positively identify the intruder as friendly or enemy and to continuously track the intruder. Multiple simultaneous intrusions from different directions with sabotage, subterfuge, and concealment make the scenario even more complex as the sensors need to rapidly adapt and coordinate to complete multiple competing tasks with varying priorities. Finally lethal and non-lethal weapon systems (unmanned and manned) may need to be deployed to deter or neutralize the threat.

Surveillance Sensor and Platform Constraints

The sensors and platforms place a number of requirements on the software that controls them.

Multiple types of sensors and sensor capabilities — Surveillance systems include optical (visible and infrared spectrum), seismic, acoustic, and radar sensors. Additionally Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) sensors may be deployed to detect specific types of hazards. Each sensor type has different resolution, detection, and location capabilities, varying performance capabilities for different targets in different terrain and weather conditions, and different requirements for optimal acquisition (distance, speed, orientation, time-on-target, etc.). Sensor fusion algorithms may require the coordinated configuration of multiple sensors maintaining specific orientation or temporal constraints.

Multiple types of sensor platforms and platform capabilities — Sensors may be deployed on mobile ground, air, or marine vehicles or located on fixed or pan-tilt platforms (such as surveillance cameras). The platforms have varying capabilities for speed, altitude, mobility, endurance, and different restrictions for operating in adverse weather and terrain.

Varying communications capabilities — Sensor data must be processed and important time-critical data communicated quickly to a base station. Coordination among the nodes also requires communications. Sensor platforms have varying communication capabilities and power constraints and may not always be in constant contact with the network. The swarming algorithms may need to configure mobile nodes in the swarm to ensure that persistent and timely communication links are maintained to all the sensors in the network. Errors and delays in communications must be accommodated.

Safety Constraints — Collision with other UxVs or entities in the air or on the ground must be avoided. Additional safety factors must be incorporated in the design of the algorithms when hardware methods alone are insufficient.

Hardware Errors and Failures — Errors in the sensors, GPS, and navigation can lead to a host of problems and possible collisions. Partial or catastrophic failures in any element of the system must be accommodated by the network to ensure continued, if not degraded, operation.

Energy Usage — The conservation of energy is critical to small distributed platforms that are required to be on station for extended periods of time. Turns and climbs consume more energy decreasing the effective range and time on station for the UxV. The swarming algorithm needs to consider the energy cost in making its decisions about how to control the movement of UxV sensor platforms.

Whatever deployment of sensor nodes is used, the system must be capable of dealing with a determined, intelligent, and ever adapting adversary intent on identifying and exploiting the weaknesses in the system. They will utilize all forms of Camouflage, Concealment, Deception & Obscurants (CCD&O) to bypass security barriers. If greater autonomy is given to the security system for monitoring and identifying potential intruders then it must be capable of adapting to multiple intrusion strategies.

3. APPROACHES TO SURVEILLANCE AND INFRASTRUCTURE PROTECTION

Military security systems have been given increased attention over the years. The Air Force Integrated Base Defense Security Systems (IBDSS) is meant as a replacement for the Tactical Automated Security System (TASS). The Joint Force Protection Advanced Security System (JFPASS) integrates access control and perimeter security for military installations. IBDSS and JFPASS are primarily architectures that bring together a wide variety of security sensors and platforms and provide the operator with a common operating picture from these various sensors. It enables, but does not duplicate the vision for a swarming security system described in this paper.

Several researchers have investigated approaches to build collaborative security systems using autonomous unmanned vehicles. Harbor [2] describes the use of UAVs and UGVs in route protection, reconnaissance, and perimeter protection

scenarios. Carroll [3] describes the Remote Detection Challenge and Response (REDCAR) initiative for Integrated Base Defense that includes unmanned platforms equipped with audio, non-lethal, and lethal deterrent mechanisms under operator control. Gray [4] describes how Integrated Swarming Operations can best be used for force protection to achieve the Air Forces Integrated Base Defense (IBD) Objectives of "See First, Understand First, and Act First."

A swarming security system must be able to direct the right sensors and platforms, to the right locations, with the right orientation to support all the elements of F2T2EA. In this effort we describe a class of algorithms using digital pheromones based on insect models [5-8]. They have been used to support a variety of surveillance functions including path planning and coordination for unpiloted vehicles [9, 10], positioning multiple sensors [11], surveillance, target tracking and trailing [12], and maintaining line of sight communications in mobile ad hoc networks [13]. Swarming systems based on digital pheromones can generate robust, adaptive, intelligent behavior at the system level even when the agents are simple and individually non-intelligent.

This paper describes the use of digital pheromones in realistic scenarios relevant to surveillance and security. In particular we demonstrate these capabilities using hardware appropriate for security systems: Pan, Tilt, Zoom (PTZ) cameras, ground sensors, small UGVs, and UAVs.

4. THE SWARMING ALGORITHM

A digital pheromone represents information about the system and its environment. Different "flavors" of pheromones convey different kinds of information. There are five primary flavors of pheromones involved in the control of the sensor platforms:

1. *Uncertainty* pheromone attracts a sensor to areas that need to be searched. This pheromone represents the level of the uncertainty about an area. High uncertainty attracts sensors that can reduce the uncertainty about the presence or absence of intruders in that area.
2. *Sensor Request* pheromones are deposited by a sensor that detects a possible intruder but needs other sensor assets to complete the identification task. Different request pheromones recruit specific sensor capabilities to the tasks of identifying and tracking the target.
3. *Target Tracking* pheromone is deposited by a sensor while tracking a particular target of interest. Normally one sensor is dedicated to tracking a target's location, heading, and speed.
4. *No-go* pheromone is deposited in areas that represent no-fly zones for UAVs or no-go zones for UGVs.
5. *Vehicle Path* pheromone is deposited along the planned path for each vehicle.

These pheromones are deposited on a gridded map representing a region of space. New deposits of the same pheromone flavor are added to previous deposits of the same flavor. Each cycle a certain fraction of the pheromone at each cell in the grid is propagated to each of the neighboring cells in the map and a certain fraction of the pheromone is removed or *evaporated* using standard equations [12]. Regular deposits followed by propagation and evaporation lead to a persistent and stable pheromone field. These two pheromone maintenance operations enable the propagation of information and help ensure that only current information is maintained in the map.

The swarming algorithm plans the areas to be covered by its onboard sensor(s). Each sensor has a footprint that identifies what area of the space it covers. The algorithm evaluates different potential paths against the following high-level objectives:

1. Move quickly to areas where there is the most need for my sensor: highest Uncertainty or Sensor Requests requiring my sensor capabilities.
2. Conserve energy (platform dependent).
3. Stay away from other vehicles and their planned paths and from no-go zones.

These high level objectives are translated into a more precise Cost to Benefit formula that drives swarming decisions [14].

5. THE OPERATOR SYSTEM INTERFACE

The Operator System Interface (OSI) was developed to evaluate techniques for enabling a single operator to monitor and manage multiple sensor platforms of different types in a surveillance application. The OSI is a geospatially based control and display system providing a visual representation of the location and status of all the entities in the system. The OSI displays advisories, cautions, and warnings; system status; time-stamped events; imagery from PTZ cameras and the cameras aboard the UAVs and UGVs; and a scalable bird's-eye view of the area of interest. This bird's-eye view includes the real-time position of all UxVs, ground sensors, PTZ cameras, and human patrols as well as targets as they are located and identified (see Figure 1). The OSI also provides audio cues when events occur, such as system health issues or intruder detections. The OSI is designed with human factors in mind, such that the operator needs to perform a minimal set of tasks to maintain the swarm and to configure the interface itself.

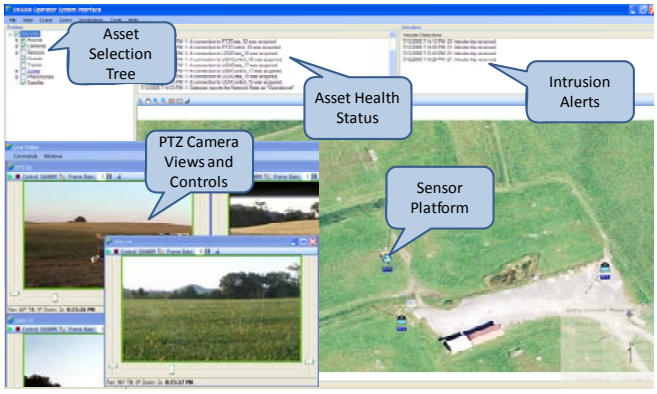

Figure 1. Operator System Interface

The user has considerable flexibility in configuring and customizing the OSI. The asset selection tree governs what information is placed on the display. Right clicking on

entities in the map-based display window provides a list of commands and information that are available for that unit. Simple drop-down menus allow users to quickly get to all functions without having to navigate through many menu layers. To take control of a particular camera, the operator clicks on its icon and a pop-up window allows the user to control the camera's pan, tilt, zoom, and frame rate parameters. The mouse and mouse wheel can be used to center, zoom in or out, and/or drag the displayed area. The OSI also includes a "goal-based" zoom capability that allows the operator to quickly scale the display to show all entities or areas of interest. Currently different communities use different symbology sets for their interfaces. The user can switch the OSI to display MIL-STD-2525B, MIL-STD-1787C, MIL-STD-1477C, and a custom designed symbol set.

6. SURVEILLANCE FLIGHT AND GROUND TESTS

An initial test of the swarming system was held at NASA's Wallops Island test range in July 2007. Two AAI Aerosonde Mk 4.1 UAVs (Figure 2) performed aerial surveillance. The UAVs were equipped with a Canon PowerShot S80 color camera to capture high resolution still images.

Figure 2. AAI Aerosonde Mk 4.1 UAV.

Figure 3. Pioneer 3-AT ground robot

Four modified Pioneer 3-AT robots were used for the ground vehicles (Figure 3). They can move at 3 kph, carry 30 kg of payload, and operate for 3-6 hours. The UGVs were equipped with 8 fore acoustic proximity sensors, GPS, digital compass, video camera, and a simulated target confirmation sensor.

Both the UAV and the UGV were equipped with an Augusta Systems SensorPort payload computer utilizing a 1.4 GHz, low voltage, Pentium-M processor module running Windows XP Embedded on a 1 GB Compact Flash. A MeshNetworks WMC6300 2.4 GHz subscriber card providing a 1.5 Mbps (6 Mbps burst rate) ad-hoc mesh network supported communications of command and control and imagery data with the ground stations. A single laptop on the MeshNetwork is used as a "payload control station" for monitoring the vehicles and providing manual control in emergencies. A second laptop was used for the OSI.

Augusta Systems developed the software to interface the swarming algorithms with the other system components including the cameras, the MeshNetwork communications network, the autopilot, the robot microcontroller, the GPS, and the payload control station. NewVectors developed the swarming algorithms operating on the payload computer and software for visualizing the pheromones and status of the swarming algorithms on the payload control station.

For the test the two Aerosonde UAVs were responsible for surveillance over a 2.5 km by 1 km playbox, while the UGVs were responsible for a smaller 250 meter by 75 meter portion of that playbox (see Figure 4). Four targets were placed within the UGV playbox and two targets just outside that playbox but still within the UAV playbox.

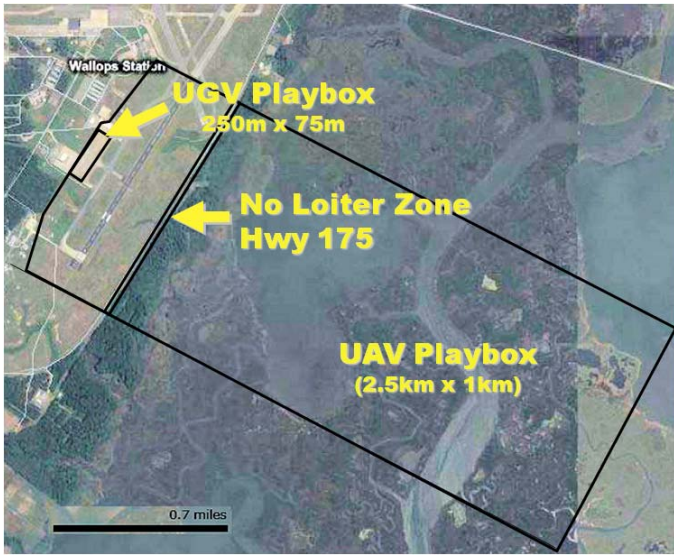

Figure 4. UAV and UGV playboxes.

Both the UAVs and UGVs executed the swarming algorithm described above. When the UAV identified a friendly target its location was designated with a box and the image sent to the OSI. When the UAV detected an unknown target it deposited Sensor Request pheromone at the detected target's location. This attracted the UGVs which possessed the necessary target identification sensor: an RF receiver detecting an RF transmitter embedded in the targets. UGVs needed to be within 6-8 feet of the target to pick up the RF signal to identify the target. Once a UGV identified a target it was reported to the OSI and the rest of the swarm so that further sensor hits on that target would be ignored. The UAV's ground projection of target location was within 50 meters of the actual location, a function of GPS error and UAV avionics error. Since the Sensor Request pheromone would propagate and the UGVs would survey around the location estimate they were still able to locate the actual target despite the location error.

On the day of the demonstration all six UxVs were successfully launched, but payload communications with one of the UAVs failed. Without any human intervention the second UAV automatically adapted to the missing UAV and surveyed the area by itself. However, due to the size of the UAV playbox that had to be covered by the one remaining UAV and the need to stay 200m away from the edge of the UGV playbox due to NASA safety constraints, the UAV missed the targets in the UGV playbox. Still, without the

expected help of the UAV, the UGVs' normal swarming activity brought them within the requisite range of 6-8 feet to find and identify three out of the four targets placed within the 200,000 square foot playbox. Finally, prior to the demonstration, the acoustic collision detection sensors on the UGVs started generating spurious contacts. The sensors were turned off for the demonstration so the collision prevention function of the swarming algorithm was entirely responsible for guaranteeing that no two robots collided during the demonstration further demonstrating the robustness of the algorithm to hardware failures.

7. PERIMETER PROTECTION TESTS

A second test and demonstration was held the following year adding ground sensors, human patrols, and fixed ground and aerial PTZ cameras, but without the UAVs, to evaluate a suite of sensors for perimeter protection. A Hostile Environment Airfield Protection (HEAP) OPerational SITuation (OPSIT) scenario was used. In this scenario an airfield is to be protected against penetration by hostile forces through the employment of a distributed, intelligent, and largely autonomous base perimeter protection system comprised of unattended sensor systems, unmanned vehicles, and an advanced network infrastructure. The system needed to be capable of complementing the limited number of personnel available for patrolling and monitoring the security of the base's perimeter.

Perimeter Test Hardware

The Pioneer 3 ground robots were updated with new motors and control software running on an Asus EeePC – a small form factor laptop PC. With the new motors and control software speeds were increased from 3 kph to 29 kph. They were outfitted with either Axis 213 (Figure 5) or 215 PTZ cameras. A SensorPort computer hosted Augusta Systems' EdgeFrontier communications software and the swarming control logic. The same 2.4 GHz MeshNetwork communications system was employed for inter-swarm and base station communications. Two robots were used in the demonstration.

A moored balloon carrying an Axis 213 PTZ camera was also planned for the demonstration, but an accident during testing destroyed the camera and it was not used for the final test.

Figure 5. Axis 213 and 232D PTZ cameras

Two fixed ground PTZ cameras provided additional surveillance capabilities. One of the fixed PTZ cameras was an AXIS 232D (Figure 5), a network dome color camera that outputs motion JPEG and MPEG-4 video with full PTZ control over an IP network. It features an 18x optical zoom and autofocus lens. It is capable of continuous 360^o pan and 90^o tilt operation. The second fixed PTZ camera was a Pelco Spectra III. It is a dome color camera with 16x optical zoom, autofocus lens with full 360^o pan and 90^o zoom. Status and commands are sent through an RS-422 link and video is transmitted over coaxial cable to an Axis 241 video server that served as a frame grabber and gateway to an IP network for transmitting the images to the Sensor Port control station.

A Crane MicroObserver ground sensor network was used for perimeter intrusion (Figure 6). Twenty MicroObserver 1045 acoustic and seismic sensors were wirelessly connected to the MicroObserver gateway. This in turn communicated over an IP network with the SensorPort control computer. The ground sensors were placed roughly 12 meters apart since each had a reliable detection range of 6 meters. The

Figure 6. Crane MicroObserver gateway and 1045 acoustic and seismic sensor

system is capable of creating tracks from multiple sensors, but this requires a higher density of sensor nodes and it can be confused when multiple intruders are involved. Instead the swarming algorithm just listened to individual sensor trips and relied on the PTZ cameras to track targets.

Finally human patrols were outfitted with a Garmin GPS tracking system that communicated wirelessly to a base station connected to a laptop computer. Though not under swarming control, the human patrols were integrated into the swarming logic. The reported location of a patrol was broadcast to the autonomous swarm entities that would deposit Vehicle Path pheromone at those locations in their pheromone maps. The propagation radius estimated the ground area visible to the human patrols so that other sensors would avoid duplicating the human surveillance activity. In this way the swarm was able to easily coordinate its autonomous surveillance tasks with available human patrols.

The UGVs, PTZ cameras, and ground sensor gateway were each connected to the SensorPort computers running the communications and swarming control software. Figure 7 shows the architecture of the systems and the communications links among the components.

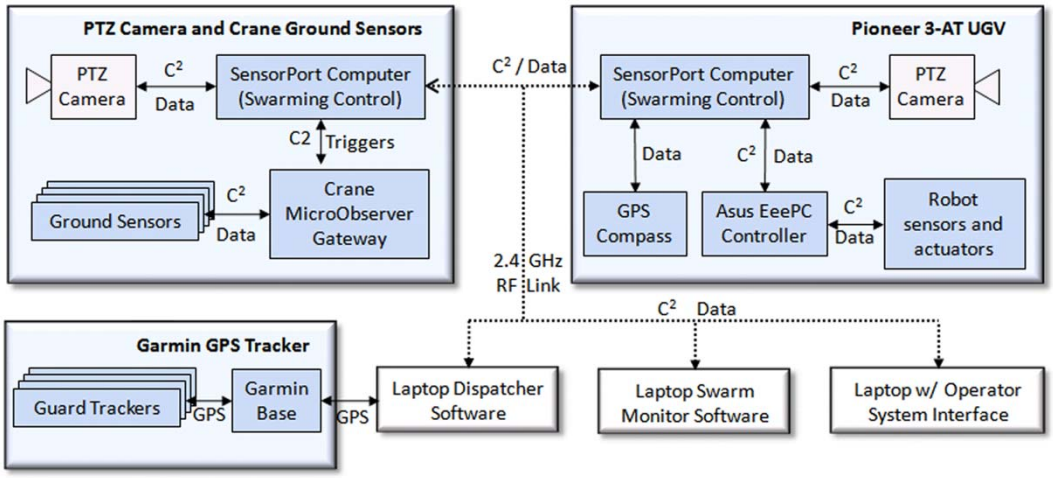

Figure 7. UGV, Ground Sensor, PTZ Camera Architecture for Perimeter Protection Demonstration

Perimeter Protection Demonstration

Multiple test scenarios were created by varying the number of intruders, direction of intruder approach, and intruder tactics. The goal of each scenario was for the system to effectively prosecute the intruders by detecting and then tracking them for a period of time long enough to consider them neutralized.

Figure 8 depicts the testing grounds, in which the various assets used in the tests are shown. A single row of ground sensors runs along the west and north sides of the field, which is approximately a rectangle with dimensions of 80 meters by 150 meters. The two PTZ cameras are located on the south side of the field and the ground robots roam within the yellow shaded area.

The ATR function was partially simulated in this demonstration. Each intruder is equipped with a GPS tracking unit, which transmits the location of the intruder at any time to the PTZ cameras, but not to the collaborative control software. Intruders can either be detected by a legitimate trip of a ground sensor or by a PTZ camera when the GPS coordinates overlap with the current view of one of the PTZ cameras. A *Sensor Request* message is sent by a ground sensor or PTZ camera when an intruder is detected. Once the swarming algorithm directs a PTZ camera to begin tracking an intruder, the camera uses the GPS coordinates to actually track the intruder through its pan range. An intruder is considered neutralized either when a guard dispatched to prosecute the intruder comes within a prescribed short distance of the intruder or the intruder has been tracked continuously for a prescribed period of time.

It is possible for a camera to lose the target being tracked when it leaves the field of view of the camera. In such cases the swarming algorithm causes another camera to pick up the target and resume tracking it to the completion of the target's prosecution. This phenomenon was observed in some of the demonstration tests.

Since intruders can only enter the protected area from outside the perimeter, Uncertainty pheromone deposits were made at the perimeter and propagated into the protected area at a speed roughly equal to the speed of an intruder on foot. As a sweep was made of an area, the Uncertainty pheromone was cleared out from the field of view of the sensor. However, new Uncertainty pheromone would immediately begin to propagate back into that area from the adjacent regions representing possible intruders just beyond the range of the sensor moving into the previously surveyed area. Thus the Uncertainty pheromone maintained an accurate representation of where potential intruders could still be hiding based on the history of sensor sweeps in the area.

Energy conservation is critical in persistent surveillance and patrol applications. All nodes in the network were designed to minimize energy usage. Ground sensors operate with only the acoustic sensors powered on. When the acoustic sensor trips, the seismic sensor is activated to further classify the intrusion and eliminate acoustic false alarms. For the UGVs energy usage was minimized by adjusting the swarming algorithm to keep the UGV stationary until it was needed elsewhere such as supporting the tracking of multiple intruders in an area.

Intrusion Test Results

Eighteen separate tests were performed. Each test involved between one and five intruders, entering from different angles or employing different strategies to try to confuse or thwart the swarming algorithm.Figure 8 shows some of the tests and the timeline of sensor trips and tracking activity. Different intruder strategies were employed including tripping a UGS sensor then retreating to penetrate elsewhere (DT.003), walking along the UGS field (DT.008 to fool location attempts), penetrating and retreating, two intruders pentrating together then splitting into different directions, etc. Two of the tests included five intruders entering the perimeter from multiple angles one of them bypassing the UGS field entirely. In this scenario all five intruders were detected, tracked and neutralized within one minute of the first intruder detection event by one of the UGS.

Table 1 has a summary of all the test results. The table shows which side or corner the intruders entered (N, NW,

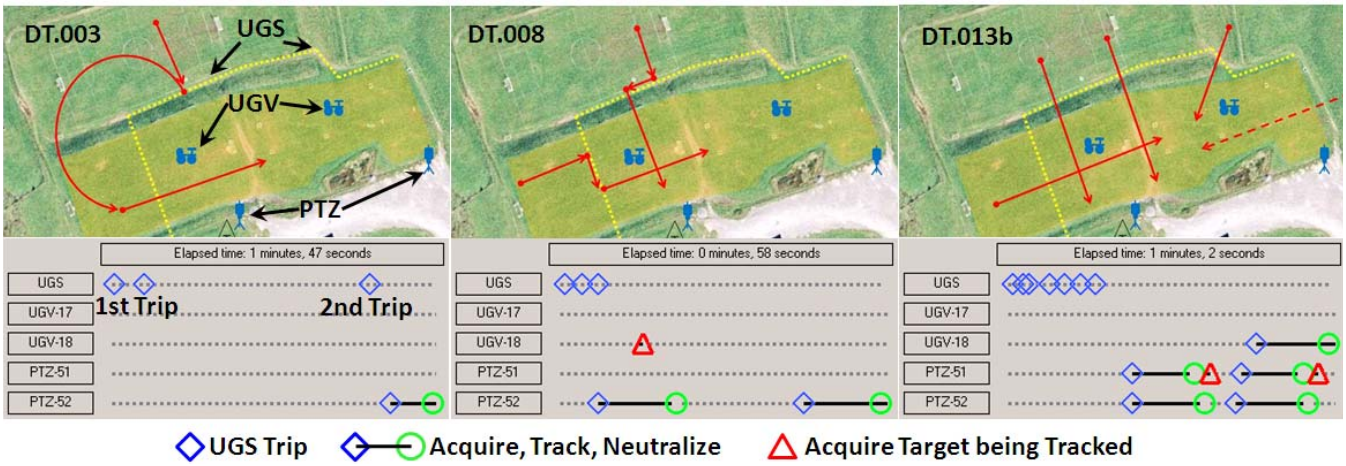

Figure 8. Example Intruder Strategies and Timelines of Sensor Activity

W, SW, or E). Three neutralization methods were used. The first required the camera to track the intruder until a guard arrived. The other two only required the camera to track the intruder for either 30 seconds (T30) or 15 seconds (T15) before the intruder was considered neutralized. The total time from when the first intruder was detected entering the perimeter until the last intruder was neutralized is listed in the table. DT.001 and DT.003 were similar except that the UGVs were not present in DT.001. Other identical runs are marked as "a" and "b". Those marked with an "*" include at least one intruder that entered the field from the east, bypassing the UGS's entirely. That intruder was only detected by the normal surveillance activities of one of the four cameras. The number of intruders tracked and neutralized by each UGV or PTZ camera is also listed in the table. An "n+" indicates the number of intruders that the sensor successfully tracked until neutralized and an "n-" indicates the number of intruders that the sensor started to track but lost until another sensor found the intruder again.

Overall, the system performed well during operational testing: all intruders were detected, tracked, and neutralized within two minutes with a minimum of human intervention. In the tests in which there was one more intruder than available tracking cameras, the swarming algorithm successfully multiplexed the tasks among the available cameras to detect and track all five targets until prosecution. The swarming algorithm demonstrated its effectiveness in coordinating the sensors under its control to ensure that all intrusion attempts were thwarted.

Table 1. Summary of Test Results

Test	Intruder Strategy	Num Intruders	Test End	Time (m:ss)	UGV-17	UGV-18	PTZ-51	PTZ-52
DT.001	Trip N, retreat, penetrate W	1	Guard	1:42	<na>	<na>	1+	
DT.002a	Penetrate N	1	T30	0:45		1+		
DT.002b	Penetrate N	1	T15	0:27	1+			
DT.003	Trip N, retreat, penetrate W	1	T15	0:21				1+
DT.005	Trip NW, follow UGS S, penetrate SW	1	T15	0:31		1+		
DT.006	Trip NW, follow UGS S, no penetration	1	T15	0:29	1+			1-
DT.007	Penetrate N and W	2	T15	0:58	1+	1+		
DT.008	Trip N and W, follow UGS, then penetrate	2	T15	0:58				2+
DT.009	Penetrate N and W then retreat	2	T15	0:45	1+	1+		
DT.010	Two penetrate N, one penetrate W	3	T15	1:03	1+	1+		1+
DT.011*	Penetrate N, W, and E*	3	T15	0:53		1+		2+
DT.012*	Two penetrate N, one penetrate W and E*	4	T15	0:59	2+		1+	1+
DT.013a*	Three penetrate N, one penetrate W and E*	5	T15	1:58	1-, 1+	1-, 1+	1+	1-, 2+
DT.013b*	Three penetrate N, one penetrate W and E*	5	T15	1:02		1+	2+	2+
DT.015a	Two (together) trip N, split along UGS, penetrate	2	T15	0:42				2+
DT.015b	Two (together) trip N, split along UGS, penetrate	2	T15	0:50	1-	2+		1-
DT.017	Two penetrate N 30 seconds apart	2	T15	0:58			1-	2+
DT.018*	Two penetrate E* 30 seconds apart	2	T15	0:56	1+		1+	

* These runs include one or two intruders entering the perimeter from the east while bypassing the UGS field
Times for DT.001 and DT.003 were from the second penetration of the intruder

8. CONCLUSION

Previous work demonstrated the versatility and adaptability of the swarming algorithms for controlling multiple air and ground vehicles. This research demonstrated the capabilities of this software in controlling a wider range of sensor platforms in more advanced scenarios. The ability to control PTZ cameras and merge data collected from ground sensors was demonstrated. Additionally the ability to seamlessly accommodate and cooperate with any number of human patrols was demonstrated in the facility protection scenario. The algorithms demonstrated an ability to easily handle the addition or removal of entire nodes as well as accommodate the errors in communications and noise common in sensors while still effectively accomplishing their overall mission. The OSI demonstrated how one person could monitor, visualize and help manage multiple diverse swarming sensors building a common operating picture over a large area. In summary the onboard digital pheromone swarming algorithms successfully coordinated the behaviors of multiple air and ground sensors in a realistic surveillance and security applications.

9. ACKNOWLEDGMENTS

This paper is based on work supported by NAVAIR with Augusta Systems as the prime contractor. NAVAIR Public Release 09-212. Distribution: Statement A – "Approved for public release; distribution is unlimited." The views and conclusions in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Department of Defense, or the US Government.

REFERENCES

[1] Parunak, H.V.D., *Go to the Ant: Engineering Principles from Natural Agent Systems.* Annals of Operations Research, 1997. **75**: p. 69-101.

[2] Harbour, J.L., Bauer, S.G., Bruemmer, D.J., Carroll, D.M., Pacis, E.B., Mullens, K.D., and Everet, H.R., *Enabling Technologies for Unmanned Protection Systems*, in *SPIE Proc. 5804: Unmanned Ground Vehicle Technology VII*. 2005: Orlando, FL, www.inl.gov/adaptiverobotics/dynamicautonomy/pubs/spie_2005_5804-66_carroll.pdf

[3] Carroll, D.M., Mikell, K., and Denewiler, T., *Unmanned Ground Vehicles for Integrated Force Protection*, in *SPIE Proc. 5804: Unmanned Ground Vehicle Technology VII*. 2005: Orlando, FL, www.nosc.mil/robots/pubs/spie5422-50.pdf

[4] Gray, R., *Integrated Swarming Operations for Air Base Defense: Applications in Irregular Warfare*. 2006, Naval Postgraduate School: Monterey, CA. p. 91, http://handle.dtic.mil/100.2/ADA451371

[5] Dasgupta, P. *Distributed Automatic Target Recognition Using Multiagent UAV Swarms*. in *Fifth International Joint Conference on Autonomous Agents and Multiagent Systems*. 2006. Hakodate, Japan

[6] Gaudiano, P., Shargel, B., Bonabeau, E., and Clough, B.T. *Swarm Intelligence: a New C2 Paradigm with an Application to Control of Swarms of UAVs*. in *8th ICCRTS Command and Control Research and Technology Symposium*. 2003. Washington, DC

[7] Payton, D., Daily, M., Estowski, R., Howard, M., and Lee, C., *Pheromone Robotics.* Journal Autonomous Robots, 2001. **11**(3): p. 319-324.

[8] Sauter, J.A., Matthews, R., Parunak, H.V.D., and Brueckner, S.A. *Performance of Digital Pheromones for Swarming Vehicle Control*. in *Fourth International Joint Conference on Autonomous Agents and Multi-Agent Systems*. 2005. Utrecht, Netherlands: ACM, www.newvectors.net/staff/parunakv/AAMAS05SwarmingDemo.pdf

[9] Parunak, H.V.D., Purcell, M., and O'Connell, R., *Digital Pheromones for Autonomous Coordination of Swarming UAV's*, in *First AIAA Unmanned Aerospace Vehicles, Systems,Technologies, and Operations Conference*. 2002, AIAA: Norfolk, VA, www.newvectors.net/staff/parunakv/AIAA02.pdf

[10] Payton, D., Daily, M., Estowski, R., Howard, M., and Lee, C., *Pheromone Robotics.* Journal Autonomous Robots, 2001. **11**(3): p. 319-324.

[11] Parunak, H.V.D., Brueckner, S., and Odell, J.J., *Swarming Coordination of Multiple UAV's for Collaborative Sensing*, in *Second AIAA "Unmanned Unlimited" Systems, Technologies, and Operations Conference*. 2003, AIAA: San Diego, CA, http://www.newvectors.net/staff/parunakv/AIAA03.pdf

[12] Sauter, J.A., Matthews, R., Parunak, H.V.D., and Brueckner, S.A., *Effectiveness of Digital Pheromones Controlling Swarming Vehicles in Military Scenarios.* Journal of Aerospace Computing, Information, and Communication, 2007. **4**(5): p. 753-769.

[13] Parunak, H.V.D. and Brueckner, S.A. *Stigmergic Learning for Self-Organizing Mobile Ad-Hoc Networks (MANET's)*. in *Third International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS'04)*. 2004. Columbia University, NY: ACM, http://www.newvectors.net/staff/parunakv/AAMAS04MANET.pdf

[14] Sauter, J.A., Matthews, R.S., Robinson, J.S., Moody, J., and Riddle, S. *Swarming Unmanned Air and Ground Systems for Surveillance and Base Protection*. in *AIAA Infotech@Aerospace 2009 Conference*. 2009. Seattle, Washington