Proceedings of the 2019 Winter Simulation Conference
N. Mustafee, K.-H. G. Bae, S. Lazarova-Molnar, M. Rabe, C. Szabo, P. Haas, and Y.-J. Son, eds.

A DISTRIBUTED AGENT-BASED FRAMEWORK FOR A CONSTELLATION OF DRONES IN A MILITARY OPERATION

Alem H. Fitwi
Deeraj Nagothu
Yu Chen

Department of Electrical and Computer Engr.
Binghamton University
Binghamton, NY 13850, USA

Erik Blasch

Air Force Office of Scientific Research
875 N. Randolph Street
Arlington, VA 22203, USA

ABSTRACT

A seamless communication capability is important in military operations. Likewise, enhanced security, increased capacity, and robust communication mechanisms are vital for humanitarian and disaster-response operations. Often, a system of wide-band satellites is employed for real-time exchange of information and over-the-horizon control, but the communications are prone to denial of service (DoS) attacks, and delayed redeployment. Hence, a swarm of drones could be deployed in mission-critical operations in times of urgency for a secured and robust distributed-intercommunication which is essential for survivability and successful completion of missions. In this paper, a distributed-agent-based framework for secure and reliable information exchange between drones in a constellation is proposed. The framework comprises a mechanism for path planning simulation and estimation, a flexible network architecture for improved client-server(C/S) and peer-to-peer (P2P) connectivity, as well as agents for identity authentications and secure communications. The framework has been simulated and verified with results showing promise.

1 INTRODUCTION

An *agent* is a computer program that can act autonomously and individually in computer simulations; whereas a *model* refers to the abstracted representation of objects, environments, or processes. Hence, agent-based modeling (ABM) is the process of creating a representation for real-world problems or businesses where a collection of autonomous decision-making agents interact with one another. The agents can individually assess their status and decide based on a set of predefined rules (Bonabeau 2002). The agents can be leveraged and applied for simulating a multitude of real-world problems including a fleet of drones in a mission (Shen et al. 2008). Hence, an agent-based framework provides simulation functionality for a swarm of drones in a military or civilian operation for such roles as high-altitude surveillance in times of emergency (Palaniappan et al. 2016; Wu et al. 2017).

Unmanned aerial vehicles (UAVs), also commonly known as drones, have found a multitude of civil and military applications since 2007 due to their mobility and low cost (Chen et al. 2017; Chen et al. 2018). The UAVs can operate in hostile territories to reduce losses which make them suitable for military operations. However, military forces that currently operate based on assured information communication systems are likely to face the danger of service disruption. Their communication system often relies on wide-band satellites and satellite-based high-altitude UAVs. Many methods are capable of perpetrating denial of service attacks on space vehicles because satellite communications (SATCOM) are well-documented and methods for wide-band communications assessments are researched (Tian et al. 2008; Shen et al. 2014). That is, SATCOM systems can be jammed and rapidly replacing them in orbit is not an easy task due to the limited number of launching sites or vehicles. Even with a replacement method, providing a timely response would still be next to impossible. One solution is to design new satellites

capable of supporting advanced extra high-frequency systems to overcome possible jamming efforts (Wilgenbusch et al. 2013; Bi et al. 2015; Zeng et al. 2016). Methods for jamming assessment simulation include agent swarms with game theory (Wei et al. 2007), frequency hopping (Shen et al. 2012), and signal-interference-to-noise ratio (Li et al. 2016). Using the performance assessment of the communication could provide information to a swarm of drones to meet a timely response.

With the incorporation of strong security countermeasures, UAVs can be effectively deployed for ubiquitous wireless coverage in an area devoid of communication networking infrastructures, for communication relaying, and for information garnering and dissemination. UAVs are applicable for search-and-rescue missions, for disaster-stricken areas where the communication infrastructures have been destroyed, and in urgent situations during interruptions (Zeng et al. 2016; Roder et al. 2018). However, many drones cannot be deployed for military use because they have some security and energy limitations. These drawbacks could be addressed through the introduction of agents capable of performing security and identity authentication, integrity checking, encryption validating, path planning, and information collating (Blasch et al. 2010). An additional consideration is route planning for multi-drone deployment (Chakrabarty et al. 2010; Zeng et al. 2016), which can leverage mulitple ad-hoc networks (MANETS) (Han et al. 2006; Han et al. 2009; Gupta et al. 2016). Currently, there is a trend in developing flying ad-hoc networks (FANETS) (Oubbati et al. 2017). The FANET agents could be fixed, semi-mobile or fully mobile. Agents can run in each drone and are capable of interacting based on defined and learned rules. They are self-controlled applications or mobile codes that can travel and communicate via a specially established local area network (LAN) or over the Internet. Also, they can perform predefined activities by frequency-hopping from one drone to another or via network-based interaction with each other. Mobile-agents were initially built for a distributed computing paradigm (Alami-Kamouri et al. 2016; Mahmoodi et al. 2014; Dadhichet al. 2010). Hence, the swarm interaction capabilities could be leveraged to enable the distributed deployment of drones for ubiquitous wireless communication coverage, connectivity relaying, and collaborative information garnering.

This paper is on agent-based modeling and military applications of a fleet of drones. A new distributed-agent-based framework for a constellation of drones is proposed. It runs on a hybrid of peer-to-peer (P2P) and client-server (C/S) network architecture with reduced protocol overheads for fast and bandwidth-efficient communication (Mustafee et al. 2017). A group of drones are flown over the area that needs urgent and secure wireless connectivity coverage and relaying information using a framework capable of supporting route optimization for energy saving and effective coverage. The agents interact with one another as peers and perform several functions. That is, the agent in each drone communicates with agents on other drones in P2P mode (in C/S mode with the control center) to collect data relevant to route optimization and routing. Optimal inter-drone distance for energy saving and increased bandwidth capacity is computed using convex optimization. The objective function is the free space path loss equation, which is a function of distance and carrier frequency, while the constraints include the area to be covered, the height, and the inter-drone distance. For optimal positioning of the drones, a semi-ellipsoid or semi-sphere is generated based on the serving area. The results demonstrate a successful simulation using the framework along with a programmable flight simulation tool on the Linux platform. Also, the python-based agent can scan and detect burned in ready-only drone-IDs, drone-IP Address, drone-MAC address, and system calls made. Brief attributes of the installed applications runtime system programs and applications along with any modifications are validated by the agents to ensure authentic and authorized exchange of information. To prevent confidentiality and integrity attacks, the agents also perform data encryption and hashing and report any abnormality discovered to peers and the command and control (C2) center server. The agent securely authenticates peer drones, enciphers the communication, and authorizes inter-drone accesses. It also collates information and images for quicker and insightful understanding.

The remainder of this paper is organized as ensues. Reviews of previous works germane to agent-based modeling, drones, path planning, and military applications are presented in Section 2. Then, the proposed framework is presented in Section 3. Section 4 presents the simulation models and results followed by the conclusive remarks presented in Section 5.

2 AGENT-BASED MODELS

Agent-based modeling (ABM) is considered a bottom-up approach, in contrast to conventional top-down models. A bottom-up approach captures the generative nature of system properties like that of UAVs (McCune et al. 2013). ABM shows the interactive behavior between the agents, predicts the results, and calibrates the model for better performance.

2.1 Related Work

A drone constellation, or commonly known as the swarm of drones, is collectively an active research topic for many applications including military and civilian operations. For the general purpose, the drones are used for area surveillance for infrastructure security (Semsch et al. 2009, Cruise et al. 2018). Many authors have addressed the complex problems of urban surveillance with occlusions due to tall buildings or vegetation as well as timeliness. Recently, a commercial application of package delivery through UAV network is promoted. UAVs are still not robust for extensive uses due to their short battery life, payload limitation, and limited onboard computational power. To accommodate these limitations and aiming for higher efficiency with the available architecture, path planning and vehicle routing problems are solved extensively using multi-objective evolutionary algorithms (Dunik et al. 2015). Peng and Mohseni (2014) presented an environmental simulation to dynamically incorporate data into a running application while simultaneously using the application to detect the presence of a puff cloud (toxic environment). In the case of military applications, an occlusion avoidance algorithm supports area survey, collects critical information about locations, and improves strategic planning as compared to the satellite-based imagery (Wei et al. 2014). Multi-UAV constellations have also been in use with a military convoy; however, the optimized topology is not transparent which requires simulations.

Algorithms for path following and collision avoidance are developed based on the sensors from the drones, and a real-time calibration due to changes in the environment is required. These limitations entail the requirement of Dynamic Data Driven Application System (DDDAS) (Darema 2004) for dynamically managing the onboard sensors and improving performance. Methods for video support include model fidelity analysis (Blasch et al. 2005), target tracking (Dunik et al. 2015), graphical methods (Liu et al. 2017), and multisource analysis (Hammoud et al. 2018).

2.2 Dynamic Data Driven Applications Systems (DDDAS)

The DDDAS framework combines the models and data to facilitate the analysis and prediction of physical phenomenon. Figure 1 shows the defined DDDAS feedback loop (Blasch 2018b). Blasch (2018a) defines the DDDAS as an adaptive framework with a sensor reconfiguration loop and a data assimilation loop. These loops use the real-time input from the test-bed sensors, and the framework recalibrates the sensor input for the error which in turn reconfigures the physical model for more accurate data collection. Many DDDAS examples explore the use of kinematic modeling in support coordinated multi-UAV control which utilizes models for optimizing sensor placement (Yang et al. 2013).

For the current proposed DDDAS application, the UAV's neighboring distance provides an input to recalibrate path planning for optimal peer-to-peer connectivity. The distance can also be quickly determined from the uncertainty quantification of the UAV positions (Tian et al. 2012).

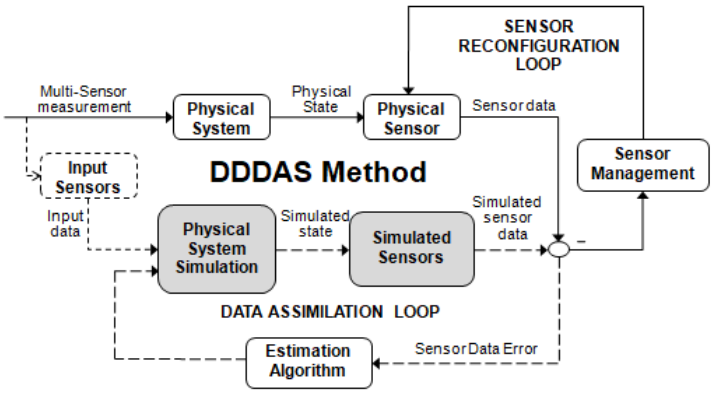

Figure 1:Dynamic data driven application system framework.

2.3 Agents

Agents are self-controlled mobile programs that can move via a network. The software agents can jump from one node to another to carry out tasks according to the set of rules defined in the code in each node and can be designed to interact with other agents. Agents were initially built for a distributed computing paradigm and could be applied in information retrieval, mobile computing, e-commerce, and network management because they can make complex problems appear simpler. But, their mobility from one network to another and from one system to another, and their interactive nature have made them a target for security attacks (Alami-Kamouri et al. 2016; Mahmoodi et al. 2014; Dadhich et al. 2010). In this paper, multifunction and secure agents are proposed which are configured on each drone. If the agent happens to fail during a mission due to various reasons, it is immediately replaced by the server in the ground control via Secure Shell (SSH) access to an agent platform on the drone.

Similar redundant applications of agents are used in honeypot deployment in Network Intrusion detection system or Industrial controls-based system (ICS). Nagothu et al. (2017) deployed a web-crawler agent based on a high-interaction simulation to collect web data and map user-interaction with the unique website behavior with client's system. Besides, Fitwi et al. (2019) developed a method based on agents for secure communication between smart grid sensors and a covey of drones.

3 THE PROPOSED AGENT-BASED FRAMEWORK FOR UAV SWARMS

Various systems for military deployment require data driven methods, such as information fusion (Blasch et al. 2012). This section provides the detailed presentation of design considerations, components, and functions of the framework. Route optimization of a covey of drones for elongating battery life, effective inter-communication, communication and device security, and information collating are the major aspects detailed.

3.1 Route Optimization

The deployment of drones seeks safety and robustness. The implementation of appropriate flight route planning can significantly shorten the communication distance. Maintaining an optimal inter-drone distance is essential for high-capacity performance. However, determining the inter-distance optimal for both high-capacity performance and energy saving is not a trivial task. Increasing the drones' altitude leads to an increased possibility of having a line of sight (LoS) links with ground stations but causes more free space path loss. Hence, a trade-off between altitude and path loss is quite important. Likewise, the drones' inter-distance must be varied only within the minimum allowable distance that avoids a possible collision and the maximum range of the Wi-Fi technology in use.

The minimum inter-distance for two drones fitted with Wi-Fi technologies to operate efficiently may not matter if they are on different frequencies. They could fly side by side in the closest possible proximity. But if they can't be separated by spectrum allocations (which is not often the case), some minimum inter-distance must be maintained. It's a good practice to place Wi-Fi access points (e.g., drones) at least 10ft away from each other. This ensures that the path loss between them is at least 50dB, big enough to negate the spectral mask of adjacent channels. With the possible channel adjacency and collision avoidance in mind, the minimum inter-drone distance is set at 10ft plus the longest body span of the drones. The maximum inter-drone distance is equal to the maximum range supported by the Wi-Fi.

Similarly, the heights of raised topographies or mountains are considered while computing the hovering altitude. Hence, the framework is designed to incorporate a convex optimization technique which is solved using a standard convex optimization method called CVX (http://cvxr.com/cvx/), to compute the optimal altitude and inter-drone separation to achieve energy-conscious maximum coverage.

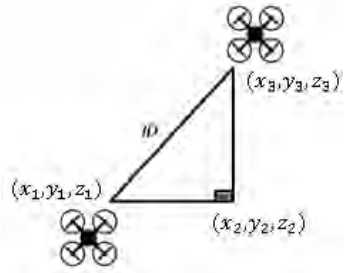

Figure 2: Inter-drone distance calculations.

Figures 2 and 3 illustrate how the inter-drone distance (ID) and the optimal traffic paths are computed using Eq. 1. The agents in each drone interact with one another via the network and exchange information about their position coordinates (x, y, z) and then compute inter-drone distances and the optimal route. Figure 3 demonstrates how five drones could be deployed to provide an important ubiquitous connectivity coverage in an identified serving area where an operation is underway.

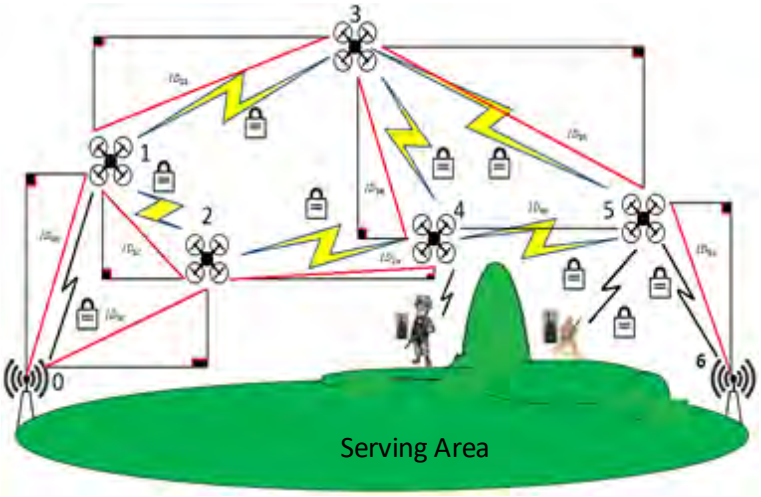

Figure 3: Route optimization.

UAVs can relay communication beyond a mountain, which is an obstacle to LoS. Figure 4 portrays a semi-ellipsoid shape placed over an elliptical area after the objective function in Eq. 2, derived from the free space path loss (FSPL) and Friis transmission formula, was optimized using the ellipsoidal area and inter-

drone distance constraints in Eq. 2 through Eq.4. Eq.1 computes the inter-drone distance (*ID*) in terms of the coordinates of the drones' current positions. In Eq. 2, d is the ID from different heights (h), f_c is the carrier frequency which is 5GHz in our case, and c is the speed of light in free space.

$$distance(ID) = \sqrt{(x2 - x1)^2 + (y2 - y1)^2 + (z2 - z1)^2} \tag{1}$$

$$FSPL(dB) = 20log_{10}\left(\frac{4\,\pi d f_c}{c}\right) \tag{2}$$

$$AreaofSemi\_Ellipsoid\ (S) = \left(\frac{2\,\pi}{3}\right)((ab)^{1.6} + (ah)^{1.6} + (bh)^{1.6})^{\frac{1}{1.6}} \tag{3}$$

$$DroneSpan + \ 10ft \leq ID \leq WiFi\ \max range \tag{4}$$

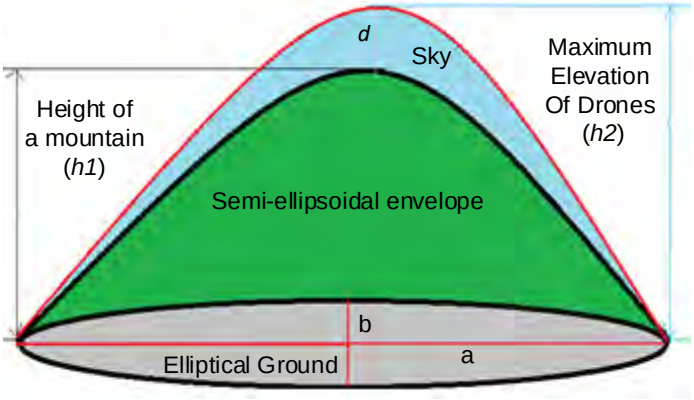

Figure 4: Semi ellipsoid envelope.

Flight time is continuously recorded for the estimation of the remaining battery power. The drones start flying back to ground when "there is just enough power for the return trip" signal is produced by the agents installed in each one of them based on the best route computed. Then, other drones take over following the broadcast of an updated signal to the database (DB), where a sample is provided in the experiments and result analysis section of this paper and in Yang et al. (2012). The broadcast starts before a drone begins its trip back to ground-based on an average drone speed of 50mph so as to fill the gap just in time.

3.2 Enhancing the Security

Drones are vulnerable to availability, integrity, and confidentiality attacks. They have several security weaknesses that could be exploited to inflict substantial attacks. Fitwi et al. (2019) stated that cache-poisoning and buffer overflow are common problems in some drones, which could cause DoS or the disconnection of drones from the controllers. Hence, to remedy these problems, the framework supports security countermeasures.

Availability ensures that information or services are accessible to authorized parties. A DoS attack on a drone denies legitimate users access to it, degrades its performance, or interrupts the standard functionality of the drones. In the proposed framework, a security measure that enforces the scrutiny of incoming requests is made to ensure that it is coming from an authentic drone in the mission or from the command center. An agent is designed to have access to an encrypted database (DB) of unique drones' IDs, media access control (MAC) addresses, system program attributes, and application program attributes of all drones in the mission. Hence, the agent on a drone receiving a request performs an identity and security authentication

of the incoming request in comparison to the initial status stored in the DB. It can also stop any unauthorized access or superfluous applications that could potentially result in a DoS attack in collaboration with the command center server. The server gets a periodic report of resource utilization by current processes helpful to identify processes that avariciously consume resources which could lead to a potential DoS attack.

Secondly, a measure against possible *integrity* attack is enforced by the framework. An information integrity measure is meant to prevent unauthorized tampering of information by illegitimate parties. That is to say, information has value only if unauthorized users do not tamper it. In this paper, integrity also refers to the drone device security/authenticity. The agents are capable of computing hashes to check the integrity of information exchanged and the authenticity of the source drone. The authenticity of the sending drone is proved by comparing the hash of the ID, and system attributes on the request and those initially stored on each drone by the server at the start of the mission.

Thirdly, the agents are equipped with a capability to protect the *secrecy* of communication. As far as confidentiality is concerned, information is the most valued asset. Hence, every communication is encrypted using the standard Advanced Encryption Standard (AES) to protect the privacy of the information. The Diffie-Hellman protocol is incorporated as part of the framework for key management.

3.3 Parallel Processing and Collating of Images

The agents have high versatility and high-level of abstraction that makes them suitable for parallel complex data acquisition. In the proposed system, the framework creates an enabling situation for concurrent information processing and collating. That is, simultaneously garnered surveillance data or images are put together onto multiple viewing monitors. They provide a panoramic view of a larger area; where the divided boundaries are much like that of surveillance cameras. In this paper, we did experiment on the collation of images captured in parallel by two different drones where the collation is done based on morphological image processing and semantic segmentation. Figure 5 portrays a sample result of our simulation where two images with common area were preprocessed and collated. Once detected, the intersection area is first removed from one of the images and collated at the boundary line that provides continuous and smooth view. It works fine with slight misalignment with high quality images but suffers a bit higher misalignment with lower quality images.

Figure 5:Collation of images captured by two drones with intersecting area.

In this paper we employed a simple but efficient technique for collating images captured by multiple drones in the same mission. But, in the future, we aspire to incorporate a more robust, machine learning (ML) based method capable of handling complex images to equip the agents with the capability of detecting germane boundaries so as to seamlessly collate average quality images captured by more than one drones in a mission into a single whole smooth view important for a quick understanding of the situations or scene (Chen et al. 2016). Besides, using context fusion, the agents enable drones to easily exchange surveillance information for image fusion (Zheng et al. 2018) about the target's boundary lines and approaching aerial or ground vehicles (Wu et al. 2011).

4 EXPERIMENTS AND RESULT ANALYSIS

Following theoretical modeling and analysis of the framework, we have created an experimental setting for simulation and verification of the proposed system practicability. A fleet of drones were simulated and deployed using a programmable open flight simulation tool. The required information like coordinates were collected and route optimization was performed by the help of the agents. A sample of generated initial drones' status loaded to each drone (a member of the mission) just before the start of the mission in lightweight format (JSON) is portrayed in Figure 6. A summarized version of all the simulations carried out is presented to verify the results.


```
#Drone_1
{"unique_ID": "f49d3e5f52fa13806323845a1fdc03615533a34539a308bece07ef66",
"MAC_ADD": "55cdd3c7d2082adec6f5539d1925a505331070dd09d9301bd2962184",
"App_attrib": "c6680dfe105bc8bb8b006f6fe918f992d2c549270bc6e0d58e3519cb",
"Sys_attrib": "b6e83f700d1267056c411402c860f6a384b63ab132f914e32e7371e7"}
#Drone_2
{"unique_ID": "8b43aa958b363914200cbec07a3f5b05c031ea27d9182c9644c4b560",
"MAC_ADD": "e2d81de55e603ae1289b907ed28a802b2dd463cdaffc8003ba557ee5",
"App_attrib": "b37238eeaa0521a4b8b74d66d5993cbc2e26a51176947df5636a14f7",
"Sys_attrib": "be666a11b079d65d847d05c698eaa50823964ccb93569ca77ee95795"}
#Drone_3
{"unique_ID": "a8b823a6739d3f3e30f00c532abc0d99b8abbffe73c3d8f0165428ef",
"MAC_ADD": "862a5718082b7183bfb61abad1289abdbd0ac20adcb3e2ca901cc2c9",
"App_attrib": "3070f04dab31c2f45992c2a850c6657e647eaf142c5592006867c084",
"Sys_attrib": "cb02dd66c31bde35da8782eb9c03f744263d3ba35e423379e25032b7"}
#Drone_4
{"unique_ID": "67fad5e78486dd0488dbbd56b2d62fac7d0b9256d2d7544b97c255e8",
"MAC_ADD": "eb38fec39cde4b4cb473d9973476f868d8d729fa60183dd7e4466fe6",
"App_attrib": "42df43535f23024adababd7241f14a725905fd0d7ac689d257d02365",
"Sys_attrib": "6f108721cc39445059f8104cac875b5a901a67eb04b506b827f02b60"}
#Drone_5
{"unique_ID": "bc35615d06ea8fe4b63b348ebb2d3be11dc56a9c38faccee1e8908b6",
"MAC_ADD": "2ac1645a4781107b75c12f4d79740206d099022c83cbed1250fcd076",
"App_attrib": "47ee80b948ae0d82f811ba12e047f6a5996dc701ca4b552dd989780a",
"Sys_attrib": "b3cfc0a416b89dd4f517cabc54b4959e2f3f5c418597ae862c997f04"}
```


Figure 6: Drone to drone Hashed Message exchange for Authentication.

The agents play a very pronounced role in the proposed model in terms of creating a collaborative environment and ensuring a secure and authentic exchange of information. Each agent in a drone is a program delegated by the server sitting in the ground control station to continuously perform system scanning and to monitor any malicious activities in every drone in the mission. They perform identity and security authentications based on the set of policies put in place. The agent deployed in each drone is said to be the client-agent; whereas the one running in the server at the control room is the server-agent. The server-agent in collaboration with the client-agents collects the IDs, MAC addresses, application attributes, and system attributes just before the start of the mission. Then, it hashes and dispatches them to every drone in a lightweight file format. A sample of the initial database of five drones' attributes vital for request-source authentication, and integrity checking is presented in Figure 6. It is generated in JSON format in order for it to be storage and bandwidth friendly. Exchanging the whole list of applications and their attributes, and operating systems and their attributes makes the comparison and checking process slower. Hashing and converting them to JSON format is more efficient as it is faster and more resource friendly.

The simulation testbed includes the MATLAB's Mobile Robotics Simulation Toolbox. The path optimized algorithms were tested in Jmavsim (https://dev.px4.io/en/simulation/jmavsim.html) and a simple Quad Simulator running PX4 autopilot system and Quad Ground Control (QGC) (http://qgroundcontrol.com/)as ground control station. Work on swarming algorithms have been previously proposed and discussed in the literature, but for deployment of an isolated air-gapped network for communication purposes in case of emergency protocol involves re-aligning the drones in a pattern to increase the bandwidth of the network and its reliability on the formation. Using the LIDAR sensors on the drones, the path between the neighboring drones is calculated, and the algorithm optimizes the distance between the drones. We simulated a swarm of agents with random initial states in MATLAB, and the

distance is calibrated using the (*x, y, z*) co-ordinates of the agent. For each iteration, the linear and the angular velocity is incremented to align the swarm of both in close proximity. Once the UAVs converge within an optimal distance, the swarm leader is responsible for following the waypoint, and the remaining UAV uses the path following algorithm to track the leader. The leader-follower approach reduces the computation on all the UAVs, and when required a new leader can be assigned for faster mission switching.

Figure 7(a) represents the simulated model of the swarming drone with random initial states in the *x-y* plane. This inter-agent distance is maintained by constantly analyzing the co-ordinate placement and simulating the error correction in form of changes in velocity and angular velocity. The sensors are used to calculate the distance between the neighboring drones and travel toward that direction. The "blue" line in Figure 7(b) indicates the path travelled to reach the final state as a coordinated swarm from the initial state. The drone separation is maintained such that convergence is encouraged by separation optimized.

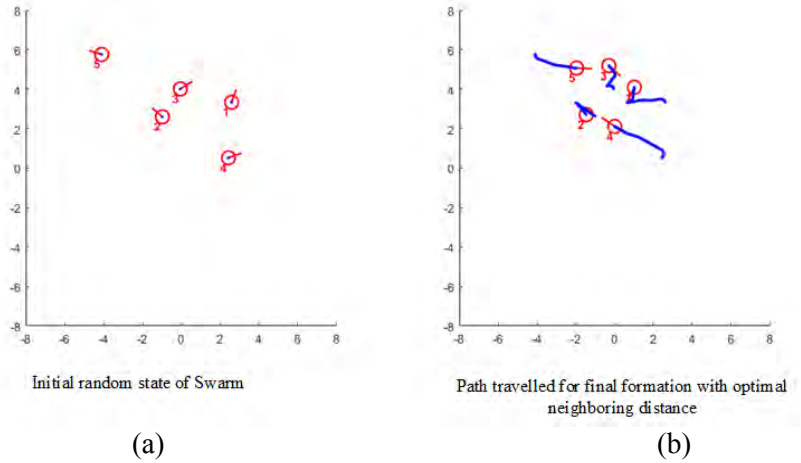

Figure 7: Simulation of Swarm UAV in XY plane.

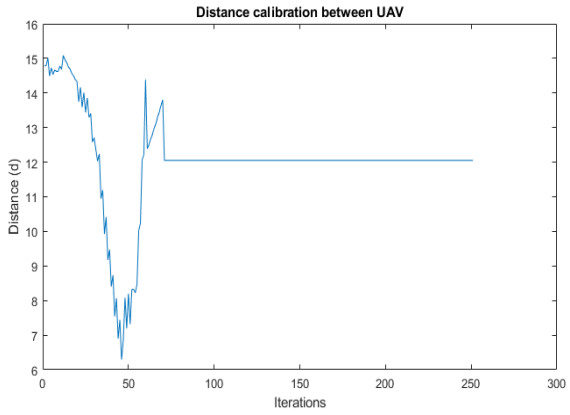

Figure 8: Distance between simulated agents 1 and 2.

The distance between two of the simulated agents is plotted in Figure 8. It can be seen that the error correction algorithm maintains the threshold distance between the swarm.

The implementation of Multi-UAV in an open-source platform following the path optimizing algorithm is shown in Figure 9. With two drones, one acts as the master and the other follows the master drone. The mission uploaded included an area survey, which includes a sweep search both horizontally and vertically. Future methods will support mobile and fixed multi-source sensing (Zulch et al. 2019).

Figure 9: Two drones in survey mission area in Quad Ground Control (QGC).

5 CONCLUSIONS

Military disaster response operations cannot rely only on assured wide-band satellite-based communication systems because well-documented communications present opportunities for jamming. When such disasters happen, timely replacing the satellites into orbit is difficult. As a result, there is a pressing call for easy replacement of communications in such times of emergency.

In this paper, we have introduced an aerial agent-based new framework that supports a secure deployment of a covey of drones for urgent response operations. It provides optimized, secured and robust distributed connectivity and relaying vital for continued operation and mission accomplishment. The framework supports mechanisms for route optimization, for secure and authentic communication, and concurrent information processing. Successful simulations were carried out by integrating our framework with an open unmanned aerial vehicle (UAV) flight simulating software on Linux and Windows environments. The simulation results validate the theoretical model estimations to support further testing such as scalability with multiple UAVs, variations in security protocols, and coordinated sensor fusion.

ACKNOWLEDGMENTS

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Government.

REFERENCES

Alami-Kamouri, S., G. Orhanou, and S. Elhajji. 2016. "Overview of Mobile Agents and Security". *International Conference on Engineering & MIS (ICEMIS)*, September 22nd – 24th, Agadir, Morocco, IEEE, 1-5.

Bi, S., C. K. Ho, and R. Zhang. 2015. "Wireless Powered Communication: Opportunities and Challenges". *IEEE Communications Magazine* 53(2015):117-125.

Blasch, E. 2018a. "DDDAS Advantages from High-dimensional Simulation". In *Proceedings of the 2018 Winter Simulation Conference*, ed. by M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, 1418-1429. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Blasch, E., E. Bosse, and D. A. Lambert. 2012. *High-Level Information Fusion Management and Systems Design*. Norwood, MA: Artech House.

Blasch, E., E. Lavely, and T. Ross. 2005. "Fidelity Score for ATR Performance Modeling". In *Proceedings of the SPIE 2005 Conference on Algorithms for Synthetic Aperture Radar Imagery XII*, May 19th, Orlando, FL, 383-394.

Blasch, E. P., P. Maupin, and A. L. Jousselme. 2010. "Sensor-based Allocation for Path Planning and Area Coverage using UGSs". In *Proceedings of the IEEE 2010 National Aerospace & Electronics Conference*, July 14th-16th, Fairborn, OH, 361–368.

Blasch, E., S. Ravela, and A. J. Aved. 2018. *Handbook of Dynamic Data Driven Applications Systems.* Heidelberg, Germany: Springer.

Bonabeau, E. 2002. "Agent-based Modeling: Methods and Techniques for Simulating Human Systems". *Proceedings of the National Academy of Sciences*99(suppl 3): 7280-7287.

Chakrabarty, A. and J. Langelaan. 2010. "Flight Path Planning for UAV Atmospheric Energy Harvesting using Heuristic Search". In *AIAA guidance, navigation, and control conference,* August 2nd-5th, Toronto, Ontario Canada, 8033.

Chen, H.-M., E. Blasch, K. Pham, Z. Wang, and G. Chen. 2016. "An Investigation of Image Compression on NIIRS Rating Degradation through Automated Image Analysis". In *Sensors and Systems for Space Applications IX* 9838:983811.

Chen, N. and Y. Chen. 2018. "Smart City Surveillance at the Network Edge in the Era of IoT: Opportunities and Challenges". In *Smart Cities*, edited by Z. Mahmood, 153-176. Cham: Springer.

Chen, N., Y. Chen, E. Blasch, H. Ling, Y. You, and X. Ye. 2017. "Enabling Smart Urban Surveillance at the Edge". In *2017 IEEE International Conference on Smart Cloud (Smart Cloud)*, November 3rd-5th, New York, NY, 109–119.

Cruise, R., E. Blasch, S. Natarajan, and A. Raz. 2018. "Cyber-physical Command Guided Swarm". *DSIAC Journal* 5(2):24–30.

Dadhich, P., K. Dutta, and M. Govil. 2010. "Security Issues in Mobile Agents". *International Journal of Computer Applications* 11(4):1–7.

Darema, F. 2004. "Dynamic Data Driven Applications Systems: A New Paradigm for Application Simulations and Measurements". In *International Conf. on Computational Science,* edited by M. Bubak, G. D. van Albada, P. M. A. Sloot, and J. Dongarra, 662-669, Berlin, Heidelberg: Springer.

Dunik, J., O. Straka, M. Simandl, and E. Blasch. 2015. "Random-point-based filters: Analysis and Comparison in Target Tracking". *IEEE Transactions on Aerospace and Electronic Systems*51(2): 1403–1421.

Fitwi, A., Y. Chen, and N. Zhou. 2019. "An Agent-Administrator-based Security Mechanism for Distributed Sensors and Drones for Smart Grid Monitoring". In *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII* 11018: 110180L.

Gupta, L., R. Jain, and G. Vaszkun. 2015. "Survey of Important Issues in UAV Communication Networks". *IEEE Communications Surveys & Tutorials* 18(2): 1123-1152.

Hammoud, R., S. Cem, and E. Blasch. 2018, April 3. "Multi-source Multi-modal Activity Recognition in Aerial Video Surveillance". *US Patent* 9, 934, 453.

Han, Z., A. L. Swindlehurst, K. J. R. Liu. 2009. "Optimization of MANET Connectivity via Smart Deployment/ Movement of Unmanned Air Vehicles". IEEE *Transactions on Vehicular Technology*, 58(7): 3533 – 3546.

Liu, K., S. Wei, Z. Chen, B. Jia, G. Chen, H. Ling, C. Sheaff, and E. Blasch. 2017. "A Real-time High Performance Computation Architecture for Multiple Moving Target Tracking based on Wide-Area Motion Imagery via Cloud and Graphic Processing Units". *Sensors* 17(2): 356.

Mahmoodi, M. and M. M. Varnamkhasti. 2014. "A Secure Communication in Mobile Agent System". *arXiv preprint arXiv:1402.0886*.

McCune, R., R. Purta, M. Dobski, A. Jaworski, G. Madey, A. Madey, Y. Wei, and M. B. Blake. 2013. "Investigations of DDDAS for Command and Control of UAV Swarms with Agent-based Modeling". In *2013 Winter Simulations Conference (WSC)*, edited by R. R. Hill and M. E. Kuhl, 1467–1478.Washington, DC: Institute of Electrical and Electronics Engineers, Inc.

Mustafee, N., S. Brailsford, A. Djanatliev, T. Eldabi, M. Kunc andA. Tolk. 2017. "Purpose and Benefits of Hybrid Simulation: Contributing to the Convergence of its Definition". *Proceedings of the Winter Simulation Conference (WSC),* edited by W. K. V. Chan and A. D'Ambrogio, 1631-1645, Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

Nagothu, D. and A. Dolgikh. 2017. "iCrawl: A Visual High Interaction Web Crawler". In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, Aug 28th-30th, Warsaw, Poland, 91–103.

Oubbati, O. S., A. Lakas, F. Zhou, M. Güneş, and M. B. Yagoubi, 2017. "A Survey on Position-based Routing Protocols for Flying Ad hoc Networks (FANETs)". *Vehicular Communications* 10: 29-56.

Palaniappan, K., M. Poostchi, H. Aliakbarpour, R. Viguier, J. Fraser, F. Bunyak, A. Basharat, S. Suddarth, E. Blasch, and R. M. Rao 2016. "Moving Object Detection for Vehicle Tracking in Wide Area Motion Imagery using 4D Filtering". In *2016 23rd International Conference on Pattern Recognition (ICPR)*, December 4th-8th, Cancun, Mexico, 2830–2835.

Peng, L. and K. Mohseni. 2014. "Sensor Driven Feedback for Puff Estimation using Unmanned Aerial Vehicles". *International Conference on Unmanned Aircraft Systems (ICUAS),* May 27th-30th, Orlando, FL, 562-569.

Roder, A., K-K. R. Choo, and N-A. Le-Khac. 2018. "Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom3 Drone As A Case Study". *arXiv preprint arXiv:1804.08649*.

Semsch, E., M. Jakob, D. Pavlicek, and M. Pechoucek. 2009. "Autonomous UAV Surveillance in Complex Urban Environments". In *Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology Vol. 02*, September 15th-18th, Washington, DC, 82–85.

Shen, D., G. Chen, J. B. Cruz, and E. Blasch. 2008. "A Game Theoretic Data Fusion Aided Path Planning Approach for Cooperative UAV ISR". In *2008 IEEE Aerospace Conference*, March 1st-8th, Big Sky, Montana, 1–9.

Shen, D., G. Chen, K. Pham, E. Blasch, and Z. Tian. 2012. "Models in Frequency-Hopping-based Proactive Jamming Mitigation for Space Communication Networks". In *Sensors and Systems for Space Applications V* 8385: 83850P.

Shen, D., G. Chen, G. Wang, K. Pham, E. Blasch, and Z. Tian. 2014. "Network Survivability Oriented Markov Games (NSOMG) in Wideband Satellite Communications". In *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)*, October 5th-9th, Colorado Springs, CO, USA, 6C2-1.

Tian, Z., E. Blasch, W. Li, G. Chen, and X. Li. 2008. "Performance Evaluation of Distributed Compressed Wideband Sensing for Cognitive Radio Networks". In *11th International Conference on Information Fusion*, June 30th-Jul 3rd, Cologne, Germany, 1–8.

Tian, X., Y. Bar-Shalom, G. Chen, E. Blasch, and K. Pham. 2012. "A Unified Cooperative Control Architecture for UAV Missions". In *Signal Processing, Sensor Fusion, and Target Recognition XXI* 8392:83920X.

Wei, M. G. Chen, J B. Cruz, L. S., Haynes, K. Pham, and E. Blasch. 2007. "Multi-Pursuer Multi-Evader Pursuit-Evasion Games with Jamming Confrontation". *AIAA Journal of Aerospace Computing, Information, and Communication* 4(3):693-70.

Wei, S., L. Ge, W. Yu, G. Chen, K. Pham, E. Blasch, D. Shen, and C. Lu. 2014. "Simulation Study of Unmanned Aerial Vehicle Communication Networks Addressing Bandwidth Disruptions". In *Sensors and Systems for Space Applications VII* 9085: 90850O.

Wilgenbusch, R. C. and A. Heisig. 2013. *Command and Control Vulnerabilities to Communications Jamming.* Fort Macnair DC: National Defense University Press.

Wu, R., B. Liu, Y. Chen, E.Blasch, H. Ling, and G. Chen. 2017. "A Container-based Elastic Cloud Architecture for Pseudo Real-time Exploitation of Wide Area Motion Imagery (WAMI) Stream". *The Journal of Signal Processing Systems* 88(2): 219-231.

Wu, Y., E. Blasch, G. Chen, L. Bai, and H. Ling. 2011. "Multiple Source Data Fusion via Sparse Representation for Robust Visual Tracking". In 14th I*nternational Conference on Information Fusion*, July 5th-8th, Chicago, IL, 1–8.

Yang, C., L. Kaplan, and E. Blasch. 2012. "Performance Measures of Covariance and Information Matrices in Resource Management for Target State Estimation". *IEEE Transactions on Aerospace and Electronic Systems* 48(3): 2594–2613.

Yang, C., L. Kaplan, E. Blasch, and M. Bakich. 2013. "Optimal Placement of Heterogeneous Sensors for Targets with Gaussian Priors". *IEEE Transactions on Aerospace and Electronic Systems* 49(3): 1637-1653.

Zeng, Y., R. Zhang, and T. J. Lim. 2016. "Wireless Communications with Unmanned Aerial Vehicles: Opportunities and challenges". *IEEE Communications Magazine* 54:36-42.

Zheng. Y., E. Blasch, and Z. Liu, 2018. *Multispectral Image Fusion and Colorization*. Vol. 481. Bellingham, WA: SPIE Press.

Zulch, P., M. Distasio, T. Cushman, B. Wilson, B. Hart, and E. Blasch. 2019. "ESCAPE Data Collection for Multi-Modal Data Fusion Research". In *2019 IEEE Aerospace Conference*, March 2nd-9th, Big Sky, Montana, USA, 1–10.

AUTHOR BIOGRAPHIES

ALEM H FITWI is a PhD candidate in the Department of Electrical and Computer Engineering at the Binghamton University. He has been working as a Graduate Assistant for Data Science and Analysis using SAS & MySQL. He has extensive pragmatic professional experiences in Networking, Network Security, Data Center construction and management, Power plant and Smart Grids construction, and enterprise software development. His current research interests include Internet of Drones (IoD), Privacy, Machine Learning, Blockchain Technology, Network Architecture for IoDs, and Network Security for IoT/IoD. His email address is afitwi1@binghamton.edu.

DEERAJ NAGOTHU is a PhD student in Electrical and Computer Engineering Department at the Binghamton University. He has been working as a Graduate Course Instructor for the course Network Computer Security since 2016. His current research interests are visual layer attacks on IoT networks, Multimedia Forensics, Network Security in IoT domain, Applications of UAV framework and Blockchain architecture. His email address is dnagoth1@binghamton.edu.

YU CHEN is an Associate Professor at the Binghamton University-SUNY. He received the Ph.D. in Electrical Engineering from the University of Southern California(USC) in 2006. His research interest lies in Trust, Security and Privacy in Computer Networks,focusing on Edge-Fog-Cloud Computing, Internet of Things (IoTs), and their applications in smart andconnected environments. His publications include over 150 papers in scholarly journals, conference proceedings, and books. His email address is ychen@binghamton.edu.

ERIK BLASCH is a Program Officer at the Air Force Office of Scientifc Research (AFOSR). He received his BS from MIT, six MS degrees, and PhD from Wright State University. He has compiled 800+ papers, 5 books, 27 patents, and 30 tutorials. He is a recipient of the Military Sensing Society Mignogna data fusion award, past president of the International Society of Information Fusion, AIAA Associate Fellow, SPIE Fellow, and IEEE Fellow.His email address is erik.blasch.1@us.af.mil.