UAVSim: A Simulation Testbed for Unmanned Aerial Vehicle Network Cyber Security Analysis

Ahmad Y. Javaid
EECS Department
University of Toledo, Ohio
ahmad.javaid@rockets.utoledo.edu

Weiqing Sun
ET Department
University of Toledo, Ohio
weiqing.sun@utoledo.edu

Mansoor Alam
EECS Department
University of Toledo, Ohio
mansoor.alam2@utoledo.edu

***Abstract* – Increased use of unmanned systems in various tasks enables users to complete important missions without risking human lives. Nonetheless, these systems pose a huge threat if the operational cyber security is not handled properly, especially for the unmanned aerial vehicle systems (UAVS), which can cause catastrophic damages. Therefore, it is important to check the impact of various attack attempts on the UAV system. The most economical and insightful way to do this is to simulate operational scenarios of UAVs in advance. In this paper, we introduce UAVSim, a simulation testbed for Unmanned Aerial Vehicle Networks cyber security analysis. The testbed allows users to easily experiment by adjusting different parameters for the networks, hosts and attacks. In addition, each UAV host works on well-defined mobility framework and radio propagation models, which resembles real-world scenarios. Based on the experiments performed in UAVSim, we evaluate the impact of Jamming attacks against UAV networks and report the results to demonstrate the necessity and usefulness of the testbed.**

***Index Terms* - cyber security; testbed; unmanned aerial vehicles; UAV network; network simulation.**

I. INTRODUCTION

Use of various unmanned systems has increased worldwide to reduce the risk involved in some tasks, e.g., deep sea exploration missions, aerial surveillance, food and medicine supply during crisis, etc. Developing these remotely controlled unmanned systems has been a focus in the past decade for several countries. Unmanned Aerial Vehicles, UAVs, are one of the most important unmanned systems being used by various defense agencies in the US. In addition, UAVs are being used in several civilian, agricultural and research applications. Development of low-cost, smaller, more reliable and more efficient UAVs has promoted their use in various difficult tasks. Number of UAVs in the US has increased from 50 to 7000 over the last decade [1]. Several work and studies have proved the importance of using multiple UAVs and enhancement in quality of the information gathered [2]. Another work has demonstrated how use of satellite based UAVs as traffic routers in sensor networks increases system availability and performance [3].

Cyber security for UAVs has recently drawn attention primarily because of the increase in cyber-attacks against these systems in the past 5 years. One of these recent incidents from 2011 forced the US Military to recall their Predator model drones from Afghanistan due to the presence of a key-logger malware in an Air Force base PC [4]. Another recent attack involved capture of the UAV video feed using cheap equipment and software in 2007 [5]. Lack of attention to the security of these unmanned systems until recent past is clearly proved after the discovery of these vulnerabilities.

However, there is not much work on the development of any cost-effective UAV network (UAVNet) simulation testbed, which would be helpful in testing various security measures, possible system vulnerabilities, attacks, etc. Some available testbeds require hardware to function and thus, require significant investment. At the same time, traditional network simulators are insufficient due to unique requirements of UAVNets. Even two closely related types of networks, MANETs (Mobile Ad-hoc Networks) and WSNs (Wireless Sensor Networks) are quite different in terms of coverage area, power requirement, transmission mechanism, etc. [6]

These recent attacks and unavailability of any software based simulation testbed served as a major motivation for this work. The catastrophic impact of losing control over these systems further necessitates in-depth research in this area. It should also be noted that most UAV applications are time sensitive and the communication channel plays a very important role in the timely delivery of information.

The rest of the paper is organized as follows. Section II describes the related work in the area of UAV testbed development. Section III details the testbed requirements and Section IV presents the design, architecture and operation of our testbed UAVSim. Section V presents the attack analysis and results, and the paper is concluded in Section VI.

II. RELATED WORK

Several works have been done in this area and many of them are promising for simulation of a single UAV. Most of these works model a single UAV instead of simulating behaviors of several UAVs while communicating with each other. Some works deal with simulation in an enclosed lab environment or a controlled open area but the focus still remains the operation instead of security. Some of these works are still premature to perform the attack simulation as they focus on improving the system instead of studying the cyber security impact. Some of these works are discussed here.

A software based simulation system using Matlab/Simulink [7] and FlightGear [8] were initial attempts

978-1-4799-2851-4/13/$31.00 ©2013IEEE

and later, using these two together, a visual simulator was made [9]. Some GUI based simulators were designed which included actual hardware to mimic real UAVs [10] while one of them used a right-angle robot to mimic an unmanned vehicle [11]. Another recent work involves use of JSBSim and FlightGear for finding vulnerabilities of the auto-pilot system [12]. All of these works are focused on single UAV simulation.

Another work, focused on simulation of a swarm of UAVs, LaBRI involves deployment of actual UAVs on a field for specific applications and check their survivability [13]. More software based network simulation systems were developed for a swarm of UAVs [14], [15], but these involved use of laptops or other hardware as UAVs. Two more important simulation testbeds for such swarms of UAVs were also developed, SPEEDES (Synchronous Parallel Environment for Emulation and Discrete Event Simulation) [16] and C3UV (Center for Collaborative Control of Unmanned Vehicles) [17]. SPEEDES simulates a swarm of UAVs on a high performance parallel computer in order to match the actual speed and communication rate of the network and C3UV testbed focuses on the fact that information acquisition through collaborative sensing and control are highly coupled. Two related works in the area of network security simulation are also quite different due to the unavailability of wireless security analysis through simulation considering the mobility of nodes. One of them, ARENA, was proposed in 2007 and includes multi-level attack simulation in the network but does not focus on all layers as well as individual modules of vital network components [18], such as UAV in our case. The other one, Ordered Scenario based Network Security Simulator, was proposed in 2005 and has the same limitation of simulating only wired components [19]. Apart from the mobile wireless component modeling capability in UAVSim, UAV models have also been defined in detail. Further, attacks targeting different layers can be defined, launched and tested in UAVSim.

III. Testbed Requirements

In this Section, we discuss the requirements to be fulfilled by a testbed like UAVSim, limitations involved and few assumptions made during the development of the testbed.

A. Security Analysis Testbed Requirements

The testbed should fulfill some of the basic requirements in order to be used as a cost-effective method of simulating UAVs and various security related events/incidents. Such a testbed should –

- allow use of various models of UAV irrespective of the scenario being simulated;
- allow testing of security measures (hardware or software) in place and check their impact on system components and overall performance;
- have an interactive and easy to use GUI;
- provide intuitive options for customized result analysis as per user's requirements;

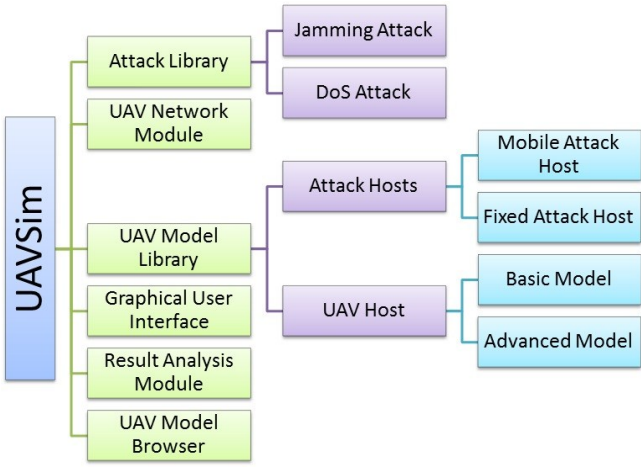


Fig. 2: Architectural design of UAVSim

- be compatible with the UAV models developed in other popular software and provide an interface to directly import these UAV models into the testbed;
- treat UAV as a network of components which replicates the component communication behavior;
- allow users to slow down the simulation speed and gain valuable insights during the simulation;
- allow users to simulate different mission scenarios through the use of different mobility models/paths.

B. Limitations and Assumptions

During our security experiments, we assume that the attacking host is at least as capable as the UAV in the system. This is advantageous in two aspects, first, we will be prepared for attacks from our own compromised systems and second, it allows us to evaluate the attack strength of attackers less powerful than us. Also, due to the non-availability of any historical data for these systems, the analysis requires data generation through experiments using different scenarios in order to ensure correct analysis. Therefore, we rely on experimentally generated data in order to gain insights into the security of the system.

IV. UAVSim Design and Development

A. Base Simulator – OMNeT++

Developing a testbed from scratch when existing network simulators can be used as a base for the testbed development would not be economical. Therefore, we selected OMNeT++ as the base simulator for our testbed. It is open-source, has a very good network animation module and supports mobile host simulation [20]. OMNeT++ has a separate mobility framework called INET which has extensive modules for wireless simulation using various mobility and radio propagation models [21]. We have used OMNeT ++ 4.2.2 and *inet* 2.0 for our development. The network is defined in NED (Network Description) files which import libraries required for the simulation. Each simulation project has a configuration file, named as *omnetpp.ini* by default. This file contains all network parameters. In UAVSim, the GUI sets the various

parameters and users don't need to edit or create this file. Advanced users can still directly edit this configuration file.

B. UAVSim Design

Figure 2 shows the architecture of UAVSim and its major modules. The six core modules of UAVSim are discussed in this Section in detail.

1) UAV Model Library

UAV model library contains all the UAV models as well as the mobile and fixed attack host models. The basic UAV model uses the architecture presented in [6] which captures the basic functionalities of a UAV. It depicts the UAV as a combination of six components – Data Acquisition Module, AHRS (Altitude and Heading Reference System), NAV (Navigation) System, Control Module, Data Logging Module and the Telemetry Module. This model can also be used for wireless attack hosts, based on the assumption that they are equally capable. However, it will be a waste of computing resources with the aim in defining the modules being detection and testing of lower layer attacks. This model is shown in Figure 3. It should be noted that the communication module is not shown here as it encompasses all the sub-modules.

Basic properties of a UAV such as speed, mobility, etc., are defined for each of the models and users are allowed to change some of them. Advanced users will also be allowed to modify the default values and other parameters. All defenses against various attacks will have to be defined in the C++ code files. The advanced UAV model allows communication between the UAV components as well as changes in the parameters related to each one of them.

2) UAV Network Module

This module defines various network parameters of the UAVNet, such as the number of radio channels, communication protocol, and transmission range. Similar to other modules, some advanced parameters are not allowed to be changed by the basic user. Several parameters defined in this module use base wireless networking packages and other mobility related packages are imported from inet 2.0.

3) Attack Library

The Attack module contains all the attack libraries. It can help designers prioritize system aspects to address and hence, improve the overall system security. Based on the threat model proposed in [6] we selected two most important attacks for UAVs – DDoS and Jamming. These attacks pose huge threat and are quite damaging in terms of compromising availability of the system. A brief description of these attacks and their implementations follows.

i) DDoS Attacks

The DDoS (Distributed DoS) attack aims at network congestion in order to make the host appear unavailable to other hosts in the network, mostly, due to the increase in response time. This attack has been implemented using a number of attack hosts, which can be defined by the user based on the total number of UAVs in the network. We have used the traditional way of transmitting spoofed packets to a single host in order to launch this attack. All of the attack hosts behave like regular UAV hosts and are assigned the IP addresses of the same range in order to make them

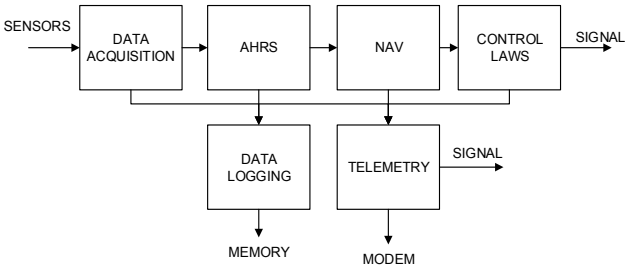


Fig. 3: Simple UAV block diagram [6]

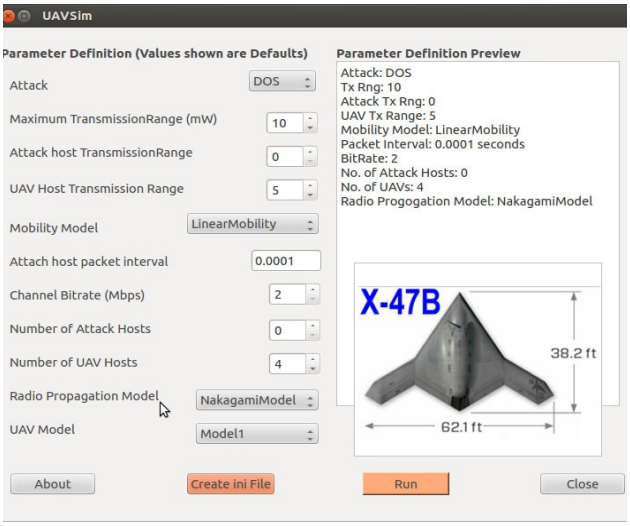


Fig. 4: The simple graphical user interface of UAVSim which includes less number of options

indistinguishable from other trusted UAVs. By default, we use 30 hostile hosts, and this number was calculated after several calibration experiments done by the authors.

ii) Jamming Attacks

Jamming involves transmission of noise in the mission area in order to block all the communications. The noise usually spans over all the frequencies and prevents all the communication. This attack can't be handled by most of today's wireless devices and is relatively easier to launch. This attack is implemented by creating a program in NED language which enables sending random signals to all the hosts in a round robin fashion over different frequencies.

4) Graphical User Interface

This is one of the most important components of UAVSim. It was specifically developed in order to allow basic users to change parameters and run the simulation using specific values. It has been shown in Figure 4. The GUI makes the testbed easy to use and removes any technical expertise required. Parameters not shown in the GUI are assigned default values. While the simulation is running, it shows the real-time network behavior, which makes it easy to visualize. The attack hosts and UAVs are represented using different icons to help the user distinguish between them. Currently, another GUI for advanced users is under development and other advanced options need to be changed in the configuration file manually.

5) Result Analysis Module

This module enables users to see results graphically according to various output parameters and gain valuable insights. The result analysis interface computes and displays results data such as time and average loss. With the accumulated data of several experiments, the module can display graphs of results.

6) UAV Model Browser

This module allows users to use other models developed in FlightGear flight simulator. This module converts the browsed xml file into a UAV model based on the parameter description in the xml file. It also allows the user to save the model in the UAV model library. Different industrial and research models can be tested by simply generating their model files using this module.

V. Attack Analysis and Results

Although a lot of analysis for DDoS and Jamming attack were performed, only the jamming attack results are presented here. Using the testbed, we analyzed the effect of changing different parameters. Average loss and average round trip time were calculated by averaging them over all the hosts in the network. These quantities were chosen as they represent the reliability and availability of time-sensitive networks. Some of the default parameters are defined in Table I.

TABLE I. Default Values of Some Parameters

Parameter	Value
Simulation time limit	300 seconds
Radio propagation model	Nakagami model [22]
Packet interval for UAVs	0.05 seconds [23]
Packet interval for attack hosts	0.0001 seconds
Number of UAV hosts	10
Number of attack hosts	30
Mobility model	Linear mobility
UAV transmission power	5 Watts
Attack host transmission power	10 Watts

A. Jamming Attack

We have 6 UAV hosts where 3 hosts use 5 GHz band and the others use 10 GHz band. Two hosts in each group are communicating with the third host. For jamming attacks, we evaluated the effect of transmission range and number of attack hosts on the system.

1) Effect of Transmission Range

The transmission range of attack hosts was varied from 0 to 10W while the regular UAV host transmission range was fixed at 5W. Figure 5 shows the result graph. It is clear that the average loss increases rapidly when the communication range is increased up to the range of UAVs and becomes almost constant once the range of attack hosts is more than that of the UAV host. Another important observation here is that loss in regular host remains in the range of 50-60% i.e., increased transmission range of attack host does not have much effect on it once the attack is launched.

2) Effect of Increasing Number of Attack Hosts

Effects of increasing number of attack hosts were evaluated while keeping the transmission range constant for each simulation. We consider two cases: Case I, where the communication range of the attack host is 10W and that of regular UAV host is 5W. Case II, where the communication ranges for the attack host and regular UAV host are 5W and 10W, respectively. We can see from Figures 6 and 7 that the average loss varies almost linearly with the increasing number of attack hosts while round trip time increases exponentially as the number of attack hosts increase in the network.

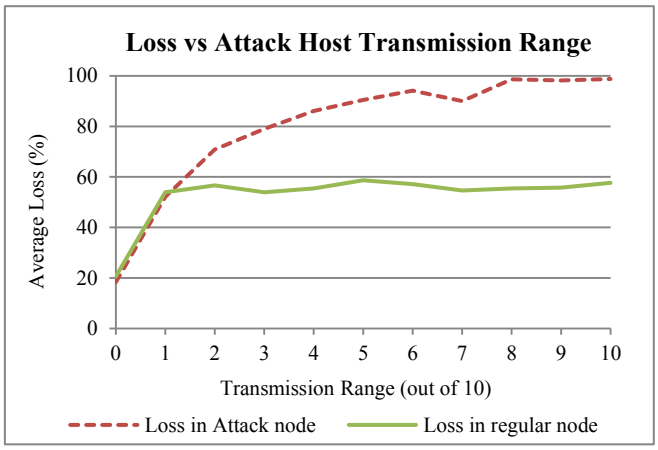
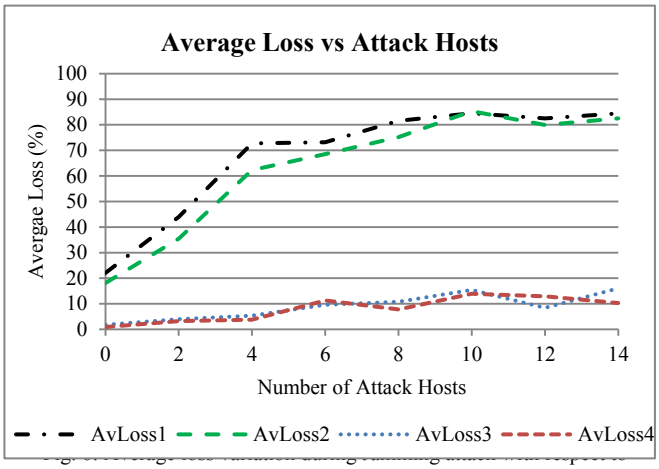


Fig. 5: Average loss variation with increasing transmission range of attack hosts while UAV host range is fixed at 50% (or 5)



number of attack hosts, first two losses for Case I and the other two for Case II

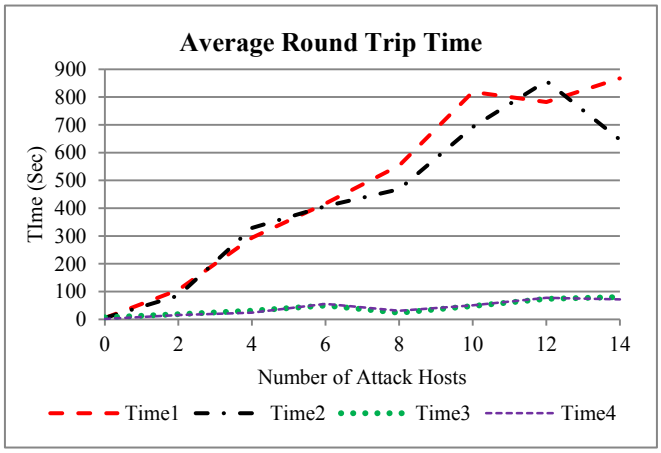


Fig. 7: Average round trip time variation during Jamming attack with respect to number of attack hosts, first two times for Case I and the other two for Case II

B. Analysis

In this Section, we discuss the insights gained from the analysis of attack simulation result graphs, which further prove the capability of the testbed.

- An increase in the number of attack hosts result in an increase of the average data loss and packet round trip times for all the simulations.
- The number of attack hosts required to launch a jamming attack varied under different simulation conditions.
- With the increase in the number of attack hosts, the average packet loss increases linearly and the round trip time increases exponentially, from 1.6 sec to almost 14 minutes.
- The average loss quickly became 99.9% for simulations of 10 sec while it decreased for longer simulations of 300 sec. This shows that during an attack, the system could not work for the first few seconds and may take some time to start communicating again.

VI. Conclusions and Future Work

In this paper, we present the UAVSim testbed developed for security experiments of UAV networks in a cost-effective manner. The UAVSim allows users to specify different UAV models and different attacks as well as generate results graphically. Simulations were performed to analyze the impact of the DDoS and Jamming attack against the UAV network in UAVSim. Results from the analysis of jamming attack demonstrate the capability of the testbed to simulate the UAVNet. It is also shown that the testbed can be used for evaluating attacks and various mitigation measures. From a research perspective, UAVSim is a novel attempt to simulate the communication behavior of a UAVNet and the impact of attacks on the communication channels of this network rather than focusing on simulation of a single UAV. For the future work, we plan to incorporate new protocols, advanced attacks and test various defensive techniques in the UAVSim.

VII. References

[1] Bumiller E. and Shanker T., “War Evolves with Drones, Some Timy as Bugs”, NY Times, June 19,2011, Last accessed on April 27, 2013. http://www.nytimes.com/2011/06/20/world/20drones.html

[2] Dixon, S. R. and Wickens, C. D., “Automation Reliability in Unmanned Aerial Vehicle Control: A Reliance-Compliance Model of Automation Dependence in High Workload”, Human Factors: The Journal of the Human Factors and Ergonomics Society, 48: 474-486, Fall 2006.

[3] Puchaty, E.M.; DeLaurentis, D.A., "A performance study of UAV-based sensor networks under cyber-attack," System of Systems Engineering (SoSE), 2011 6th International Conference on, vol., no., pp.214,219, 27-30 June 2011.

[4] Charles Arthur, “SkyGrabber: the $26 software used by insurgents to hack into US drones”, Guardian, Dec 17, 2009. http://www.guardian.co.uk/technology/2009/dec/17/skygrabber-software-drones-hacked

[5] “Computer virus infects drone plane command center in US”, Associated Press, Guardian, October 9, 2011. http://www.guardian.co.uk/technology/2011/oct/09/virus-infects-drone-plane-command

[6] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, M. Alam, “Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System”, Proceedings of Conference on Homeland Security Technologies 2012, Boston, MA, November 2012.

[7] Peng Lu; Qingbo Geng, "Real-time simulation system for UAV based on Matlab/Simulink," Computing, Control and Industrial Engineering (CCIE), 2011 IEEE 2nd International Conference on, vol.1, no., pp.399,404, 20-21 Aug. 2011.

[8] Zhang, Jingsha; Geng, Qingbo; Fei, Qing, "UAV flight control system modeling and simulation based on flightGear," *Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on*, vol., no., pp.2231,2234, 3-5 March 2012.

[9] Yin Qiang; Xian Bin; Zhang Yao; Yu Yanping; Li Haotao; Zeng Wei, "Visual simulation system for quadrotor unmanned aerial vehicles," Control Conference (CCC), 2011 30th Chinese , vol., no., pp.454,459, 22-24 July 2011.

[10] Jianan Wu; Wei Wang; Jinhong Zhang; Bodong Wang, "Research of a kind of new UAV training simulator based on equipment simulation," Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on , vol.9, no., pp.4812,4815, 12-14 Aug. 2011.

[11] Jun Yang; Huimin Li, "UAV Hardware-in-loop Simulation System Based on Right-angle Robot," Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2012 4th International Conference on, vol.1, no., pp.58,61, 26-27 Aug. 2012.

[12] Alan Kim, Brandon Wampler, James Goppert, and Inseok Hwang, “Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles”, Proceedings of Infotech @Aerospace 2012 Conference, California, 19-22 June 2012.

[13] Timothy X Brown, Sheetalkumar Doshi, Sushant Jadhav and Jesse Himmelstein, “Test Bed for a Wireless Network on Small UAVs”, in Proc. AIAA 3rd ``Unmanned Unlimited'' Technical Conference, Chicago, IL, 20-23 Sep 2004.

[14] Joshua J. Corner and Gary B. Lamont, “Parallel simulation of UAV swarm scenarios”, Proceedings of the 2004 Winter Simulation Conference, pp 355-363.

[15] Stephen Hamilton, J. A. “Drew” Hamilton Jr. and Colonel Timothy Schmoyer, “Validating a network simulation testbed for army UAVs”, Proceedings of the 2007 Winter Simulation Conference, WSC 2007, Washington, DC, USA, December 9-12, 2007.

[16] S. Chaumette, R. Laplace, C. Mazely and R. Miraulty, “SCUAL, Swarm of Communicating UAVs at LaBRI: an open UAVNet testbed”, 2011 14th International Symposium on Wireless Personal Multimedia Communications (WPMC), France, 3-7 Oct 2011.

[17] Pereira, E., Sengupta, R., Hedrick, K., "The C3UV Testbed for Collaborative Control and Information Acquisition Using UAVs", to appear at the 2013 American Control Conference, Washington DC, USA, June 2013.

[18] Kuhl, M.E.; Kistner, J.; Costantini, K.; Sudit, M., "Cyber-attack modeling and simulation for network security analysis," Simulation Conference, 2007 Winter, vol., no., pp.1180,1188, 9-12 Dec. 2007.

[19] Yun, JooBeom, Park, EungKi, Im, EulGyu and In, HohPeter, “A Scalable, Ordered Scenario-Based Network Security Simulator”, Book Chapter, Systems Modeling and Simulation: Theory and Applications - Lecture Notes in Computer Science, Baik, Doo-Kwon, Springer Berlin Heidelberg, 2005-01-01, pp 487-494.

[20] OMNeT++ Community Site (2013), OMNeT++ Discrete Event Simulation System. http://www.omnetpp.org

[21] INET Framework - an open-source communication networks simulation package for OMNeT++, http://inet.omnetpp.org

[22] Rhattoy, A. and A. Zatni, “The Impact of Radio Propagation Models on Ad Hoc Networks Performances”, Journal of Computer Science 8 (5): 752-760, 2012, ISSN 1549-3636.

[23] Pengcheng Zhan; Kai Yu; Swindlehurst, A.L., "Wireless Relay Communications with Unmanned Aerial Vehicles: Performance and Optimization," Aerospace and Electronic Systems, IEEE Transactions on, vol.47, no.3, pp.2068-2085, July 2011.