12-4-2013

Towards detection and control of civilian unmanned aerial vehicles

Matthew Peacock
Edith Cowan University, mpeacock@our.ecu.edu.au

Michael N. Johnstone
Edith Cowan University, m.johnstone@ecu.edu.au

DOI: 10.4225/75/57a847dfbefb5
14th Australian Information Warfare Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013

TOWARDS DETECTION AND CONTROL OF CIVILIAN UNMANNED AERIAL VEHICLES

Matthew Peacock[1] and Michael N. Johnstone[1,2]
School of Computer and Security Science, Security Research Institute
Edith Cowan University, Perth, Australia
m.peacock@our.ecu.edu.au, m.johnstone@ecu.edu.au

Abstract
Considering the significant number of non-military unmanned aerial vehicles (UAVs) that can be purchased to operate in unregulated air space and the range of such devices, the potential for security and privacy problems to arise is significant. This can lead to consequent harm for critical infrastructure in the event of these UAVs being used for criminal or terrorist purposes. Further, if these devices are not being detected, there is a privacy problem to be addressed as well. In this paper we test a specific UAV, the Parrot AR Drone version 2, and present a forensic analysis of tests used to deactivate or render the device inoperative. It was found that these devices are open to attack, which means they could be controlled by a third party.

Keywords
Unmanned Aerial Vehicles,Security, Detection, Wireless, 802.11, UAV, Privacy.

INTRODUCTION

Unmanned Aerial Vehicles (UAVs) originated in the military domain, undertaking reconnaissance missions in high-risk situations. Their use expanded as weaponised payloads were attached to UAVs such as the Reaper, allowing precision target strikes to be undertaken. Gaub (2011) compares the proliferation of UAVs to the original adoption of manned flight to achieve air superiority during World War I, with global spending on UAV technology reaching over $6 billion USD annually, according to. Sullivan (2013) notes that military UAVs range in price from ~US$30,000 to ~US$223,000,000 depending on the functionality provided, certainly out of range for most businesses and hobbyist users (assuming that they would be allowed to purchase such devices). Gaub provides an interesting comparison between the civilian take-up of aircraft post-World War I and the current growth of UAV use, citing many parallel characteristics. He points out that the speed of technology transfer is likely to accelerate the use of UAVs in civilian applications.

Concomitant with the military uses, UAVs have gained a foothold in commercial markets. UAVs have been used in the following areas: crop dusting, commercial photography, biological studies and weather reporting. With devices such as the Parrot AR Drone available for ~AUD$350, UAVs have proven to be cost effective alternatives to manned aircraft for a variety of applications.

Unfortunately, small UAVs operate in uncontrolled airspace, which may lead to potential security and privacy problems. CASA (1998) defines uncontrolled airspace as below 400ft. This airspace is deemed too dangerous to operate in for commercial and military aircraft, as the rate of collision with objects increases. As such, registered aircraft are prohibited from entering this airspace. Small UAVs are not bound by these same regulations, with the opposite in action, preventing small UAVs from entering registered airspace until integration technology in the form of air-to-air detection can be standardised and retrofitted to manned aircraft - a problem outlined by Kaiser (2011). Further, purchase of small UAVs is unrestricted.

Misuse of UAVs is a threat to critical infrastructure due to the wide range of damaging payloads that could be carried onboard. Worse, the UAV itself could be used to inflict damage. Given that many small UAVs have on-board HD cameras for guidance purposes, misuse of the camera can raise privacy concerns, because UAVs can traverse property boundaries easily and quickly.

The Parrot AR Drone version 2 (hereafter “Parrot”) is a low-cost commercially available quadricopter,

weighing 420g having a flight time of approximately 12 minutes (Figure 1). The Parrot supports control via wireless 802.11b/g/n so the effective range is limited by the wireless protocol and the battery life. It has a 1GHz 32 bit ARM Cortex A8 processor and runs Linux 2.6.32. There is an on-board gyroscope, accelerometer, magnetometer and pressure sensor as well as ultrasound sensors for ground altitude measurement. It also houses a 720p HD camera which can transmit video to a paired tablet (or phone) or to a USB stick on-board.

This paper explores vulnerabilities in a civilian small UAV, with the aim of determining whether third party control is feasible, therefore taking the first steps towards identifying, realising and mitigating the aforementioned threats to security and privacy.

Figure 1: The Parrot AR Drone used in the tests.

DETECTING UAVS

UAVs in operation are conventionally detected in one of three ways, using radar, visual detection or acoustic sensors. The issues that arise from the reduction in size of UAVs limit the use of these methods. Radar relies on detecting the electromagnetic waves (EM) emitted from aircraft. Due to the non-metallic components and size of small UAVs, the EM signature is smaller, and at a higher frequency. Skolnik (2008) points out that the range of radar detection relies on the frequency of the EM being emitted, the lower the frequency (between 3MHz and 2GHz) the further away objects can be detected (2000 nautical miles to 200 nautical miles respectively). In comparison, small UAVs emit EM at or above the 10Ghz range, limiting detection range to hundreds of metres. While this seems like a suitable detection method, radars operating at this frequency are susceptible to interference from weather conditions, and have high associated monetary and power costs. Similarly, again due to the size of the UAV, visual detection techniques that by design filter out smaller flying objects such as birds have high false negative rates when tuned for small UAV detection.

In contrast, Pham and Srour (2004) claim that acoustic detection methods are not dependent on the size or line of sight issues which affect radar and visual detection, the acoustic method uses microphone arrays to capture the sound of the moving parts of UAVs and compares this signature to a database of recognised sounds for identification. This method has been successful in detecting a range of airborne vehicles, and is a cost effective solution as demonstrated by the implementation of Drone Shield, a modified Raspberry-Pi which acts as a standalone UAV acoustic detection device. The limitations of acoustic detection relate to the large number of small UAVs available, and their customisable parts requiring individual signatures stored in the database for meaningful detection; a manual, consuming task in terms of time and processing power to prepare. Additionally, Gaub (2011) notes that some fixed-wing UAVs can enter glide mode, eliminating any engine noise. As such, further research into suitable detection methods using a hybrid approach of the aforementioned techniques is underway in the U.S air force, but this is limited to proof-of-concept at present.

To overcome the limitations of existing detection methods, viz. size, construction materials and

variety of modules, we propose to use 802.11 protocol fingerprints to detect a UAV. This has advantages of not being reliant on UAV size, not requiring line of sight, protocol standardisation and forensic tool support (hardware and software).

EXPERIMENTAL METHOD

The Parrot operates using a standard WiFi (802.11) protocol to pair with a controller device (an iPad) running freely available software. Therefore, it should be possible to perform packet captures of traffic between the paired devices and thus potentially gain control of the UAV. Using a standard Detect-Acquire-Analyse-(Attack) model (Figure 2), we set up a series of experiments to test potential vulnerabilities of the UAV. The research question was: Could a Parrot AR Drone be controlled by a third party when in operating mode? The hypotheses were:

H_1: Can the network signature of a Parrot be determined when the UAV is operating?
H_2: If the Parrot has open ports, is the UAV vulnerable to direct connections?
H_3: Can the connection procedure between a control device and the UAV be determined and if so, is it similar to a standard wireless connection between any other wireless device and an access point?
H_4: How susceptible are UAVs to de-authentication?
H_5: How effective are de-authentication attacks against UAVs?
H_6: What results from de-authentication attacks can be used against small UAVs?

We used open source software (nmap, wireshark and aircrack-ng) to perform the scans, attacks and packet capture. The hardware used was an S10 Lenovo laptop (running Ubuntu 12.04) equipped with an external Linksys 802.11n USB wireless card, as the attacking entity; A standard (uncracked) iPhone 5 (iOS version 6) was used as the ground controller for the Parrot.

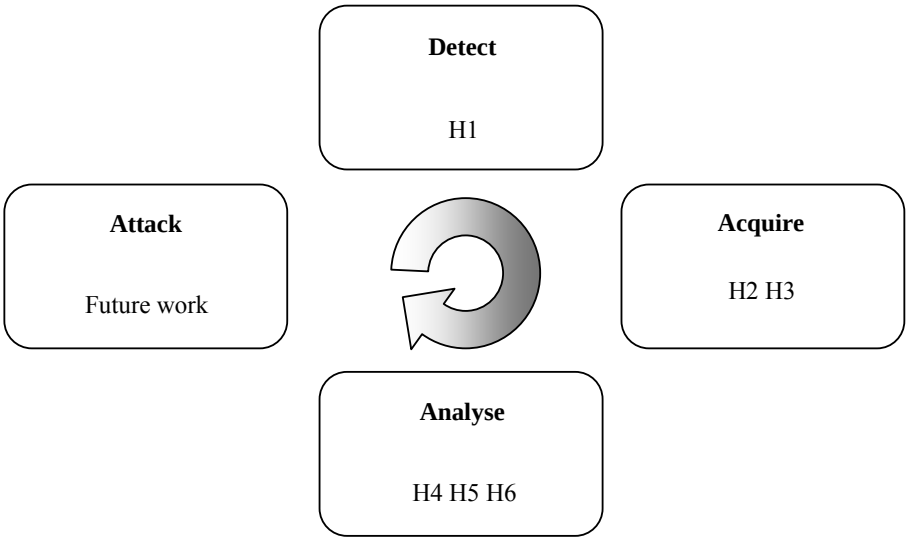

Figure 2: Research Design for Attacks on UAV Wireless Connections.

RESULTS AND DISCUSSION

Signature determination

The vendor MAC address is identifiable (the manufacturer is assigned the allocation 90:03:B7), along with individual fingerprints determined by nmap for ports 21, 23, 5551 and 5555. Given that ftp and telnet are enabled without any security, it is possible to connect to the Parrot and upload files whilst the UAV is operating. Ports 5551 and 5555 may be the video and control ports. By using these fingerprints it is possible to determine what detected APs are Parrot drones. Therefore validating hypothesis H_1 (Can the network signature of a Parrot be determined when the UAV is operating?).

Open Connections

A telnet session initiated to 192.168.1.1 connects directly into the Parrot and receives a shell as root (shown in figure 4), therefore all files/directories are available. Additionally, flight recordings were accessible in the /data/videos directory. This confirms hypothesis H_2 (If the Parrot has open ports, is the UAV vulnerable to direct connections?)

```
BusyBox v1.14.0 () built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ls -l
drwxrwxr-x    4 root     root          5304 Jan  1  1970 bin
drwxr-xr-x    4 root     root           952 Jan  1 00:00 data
drwxrwxrwt    4 root     root          3500 Jan  1 00:00 dev
drwxrwxr-x    3 root     root          1256 Jan  1  1970 etc
drwxr-xr-x    2 root     root          1064 Jan  1 00:01 factory
drwxr-xr-x    3 root     root           368 Jan  1 00:00 firmware
drwxrwxr-x    3 root     root           224 Jan  1  1970 home
drwxr-xr-x    5 root     root          2800 Jan  1  1970 lib
drwxrwxr-x    2 root     root           240 Jan  1  1970 licenses
drwxrwxr-x    2 root     root           160 Jan  1  1970 mnt
dr-xr-xr-x   73 root     root             0 Jan  1  1970 proc
drwxrwxr-x    2 root     root           160 Jan  1  1970 root
drwxrwxr-x    2 root     root          2752 Jan  1  1970 sbin
drwxr-xr-x   12 root     root             0 Jan  1  1970 sys
drwxrwxrwt    3 root     root           160 Jan  1 00:00 tmp
drwxr-xr-x    2 root     root           232 Jan  1 00:00 update
drwxrwxr-x    8 root     root           544 Jan  1  1970 usr
drwxrwxr-x    2 root     root           352 Jan  1  1970 var
#
```

Figure 3: Root shell on Parrot.

No.	Time	Source	Destination	Protocol	Length	Info
6	13.823960	f8:1a:67:09:4f:0d	Parrot_35:24:24	ARP	42	Who has 192.168.1.1? Tell 192.168.1.2
7	13.825718	Parrot_35:24:24	f8:1a:67:09:4f:0d	ARP	42	192.168.1.1 is at 90:03:b7:35:24:24
8	20.847968	192.168.1.2	91.189.94.25	TCP	74	55256 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=161420 TSecr=0 WS=128
9	21.497864	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x92a83e4a
10	21.501009	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x92a83e4b
11	21.502019	Parrot_35:24:24	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.1
12	21.517648	::	ff02::1:ff0f:517d	ICMPv6	78	Neighbor Solicitation for fe80::1aaf:61ff:fe0f:517d
13	21.520355	fe80::1aaf:61ff:fe0f:!	ff02::2	ICMPv6	62	Router Solicitation
14	21.896162	fe80::1aaf:61ff:fe0f:!	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
15	21.897771	fe80::1aaf:61ff:fe0f:!	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
16	22.543722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x92a83e4b
17	22.544851	fe80::1aaf:61ff:fe0f:!	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::1aaf:61ff:fe0f:517d (ovr) is at 18:af:61:0f:51:7d
18	23.498266	192.168.1.1	192.168.1.3	DHCP	590	DHCP Offer - Transaction ID 0x92a83e4a
19	23.500179	192.168.1.1	192.168.1.3	DHCP	590	DHCP Offer - Transaction ID 0x92a83e4b
20	24.556745	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x92a83e4b
21	24.556819	192.168.1.1	192.168.1.3	DHCP	590	DHCP ACK - Transaction ID 0x92a83e4b
22	24.560015	18:af:61:0f:51:7d	Broadcast	ARP	42	Who has 192.168.1.3? Tell 0.0.0.0
23	25.237724	18:af:61:0f:51:7d	Broadcast	ARP	42	Who has 192.168.1.3? Tell 0.0.0.0
24	25.546998	18:af:61:0f:51:7d	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.3 (Request)
25	25.868140	18:af:61:0f:51:7d	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.3 (Request)
26	26.190117	18:af:61:0f:51:7d	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.3 (Request)
27	26.198615	18:af:61:0f:51:7d	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
28	26.198827	Parrot 35:24:24	18:af:61:0f:51:7d	ARP	42	192.168.1.1 is at 90:03:b7:35:24:24

Figure 4: Wireshark capture of Syn/Ack connections.

Connection Procedure

Using the Lenovo S10, external Linksys 802.11n USB wireless card and Wireshark to capture network packets, there is a distinct connection process when the controller connects to the device with a number of ARP packets sent around the network with a DHCP request being given to the device (as shown in figure 4). A repeatable disconnection sequence was not identified after 5 connect/disconnect attempts. Following a number of ARP packets broadcast, DHCP request and ICMPv6 advertisements follow (IPv6 multicast).As part of the pairing protocol, the connecting device (iPhone) is assigned the IP address 192.168.1.3. After several ARP requests to 192.168.1.1 (the Parrot), they are then paired (connected). Connection speed is between 1.5 and 2.5 seconds.

A UDP packet was captured which was recorded from port 5552 to port 5552 from the connecting device to 192.168.1.255 (i.e. a broadcast, see figure 5, sequence #37). This could possibly be used for changing the video feed, if the normal behavior is to broadcast request the video port from the connecting device.

There is evidence of a generic connection pattern for the UAV. The speed of connection suggests that de-authentication and re-authentication could be quick enough to be achieved in mid-air. Further, there is some promising evidence that might enable video capture and substitution. These findings validate hypothesis H_3 (Can the connection procedure between a control device and the UAV be determined and if so, is it similar to a standard wireless connection between any other wireless device and an access point?)

No.	Time	Source	Destination	Protocol	Length	Info
36	36.863998	192.168.1.2	91.189.94.25	TCP	74	55256 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=165424 TSecr=0 WS=128
37	39.066223	192.168.1.3	192.168.1.255	UDP	53	Source port: 5552 Destination port: 5552
38	39.069234	Parrot_35:24:24	18:af:61:0f:51:7d	ARP	42	192.168.1.1 is at 90:03:b7:35:24:24
39	39.073351	192.168.1.1	192.168.1.3	UDP	65	Source port: 5552 Destination port: 5552
40	39.082485	192.168.1.1	192.168.1.3	TCP	92	5551 > 58256 [PSH, ACK] Seq=1 Ack=1 Win=1448 Len=26 TSval=1256 TSecr=662982696
41	39.089731	192.168.1.1	192.168.1.3	TCP	66	5551 > 58256 [ACK] Seq=27 Ack=17 Win=1448 Len=0 TSval=1257 TSecr=662982706
42	39.090229	192.168.1.1	192.168.1.3	TCP	92	5551 > 58256 [PSH, ACK] Seq=27 Ack=17 Win=1448 Len=26 TSval=1257 TSecr=662982706
43	39.092621	192.168.1.1	192.168.1.3	TCP	101	5551 > 58256 [PSH, ACK] Seq=53 Ack=23 Win=1448 Len=35 TSval=1257 TSecr=662982708
44	39.094896	192.168.1.1	192.168.1.3	TCP	92	5551 > 58256 [PSH, ACK] Seq=88 Ack=31 Win=1448 Len=26 TSval=1257 TSecr=662982710
45	39.097006	192.168.1.1	192.168.1.3	TCP	73	5551 > 58256 [PSH, ACK] Seq=114 Ack=49 Win=1448 Len=7 TSval=1258 TSecr=662982712
46	39.099369	192.168.1.1	192.168.1.3	TCP	74	36986 > 58257 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1258 TSecr=662982713 WS=4
47	39.101476	192.168.1.1	192.168.1.3	TCP	123	5551 > 58256 [PSH, ACK] Seq=121 Ack=67 Win=1448 Len=57 TSval=1258 TSecr=662982715
48	39.101512	192.168.1.1	192.168.1.3	TCP	72	36986 > 58257 [PSH, ACK] Seq=1 Ack=0 Win=5792 Len=6 TSval=1258 TSecr=662982715
49	39.101723	192.168.1.1	192.168.1.3	TCP	66	36986 > 58257 [FIN, ACK] Seq=7 Ack=0 Win=5792 Len=0 TSval=1258 TSecr=662982715
50	39.102727	192.168.1.1	192.168.1.3	TCP	92	5551 > 58256 [PSH, ACK] Seq=178 Ack=67 Win=1448 Len=26 TSval=1258 TSecr=662982715
51	39.104224	192.168.1.1	192.168.1.3	TCP	66	36986 > 58257 [ACK] Seq=8 Ack=1 Win=5792 Len=0 TSval=1259 TSecr=662982718
52	39.106864	192.168.1.1	192.168.1.3	TCP	92	5551 > 58256 [PSH, ACK] Seq=204 Ack=74 Win=1448 Len=26 TSval=1259 TSecr=662982720
53	39.107283	192.168.1.1	192.168.1.3	TCP	66	5551 > 58256 [FIN, ACK] Seq=230 Ack=74 Win=1448 Len=0 TSval=1259 TSecr=662982720
54	39.109978	192.168.1.1	192.168.1.3	TCP	74	personal-agent > 58258 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1259 TSecr=662982722 WS=4
55	39.113968	192.168.1.1	192.168.1.3	TCP	74	ftp > 58259 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1260 TSecr=662982725 WS=4
56	39.114592	192.168.1.1	192.168.1.3	TCP	74	5559 > 58260 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1260 TSecr=662982725 WS=4
57	39.124014	192.168.1.1	192.168.1.3	TCP	74	sgi-eventmond > 58261 [SYN, ACK] Seq=0 Ack=0 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1261 TSecr=662982733 WS=4
58	39.125887	192.168.1.1	192.168.1.3	FTP	92	Response: 220 Operation successful
59	39.127903	192.168.1.1	192.168.1.3	TCP	66	ftp > 58259 [ACK] Seq=27 Ack=16 Win=5792 Len=0 TSval=1262 TSecr=662982736
60	39.128224	192.168.1.1	192.168.1.3	FTP	92	Response: 230 Operation successful
61	39.130368	192.168.1.1	192.168.1.3	FTP	92	Response: 250 Operation successful
62	39.133238	192.168.1.1	192.168.1.3	FTP	101	Response: 227 PASV ok (192,168,1,1,213,205)

Figure 5: Wireshark capture of video connection.

De-authentication

De-authentication attacks are a common problem with 802.11 WiFi networks due to that standards reliance on management frames. These frames are exploited commonly over wireless networks to achieve Denial of Service (DoS) attacks. Whilst mitigation techniques are defined in the standard 802.11w protect de-authentication frames, the slow adoption of this standard due to lack of backwards hardware compatibility keeps this type of attack relevant. This led to speculation regarding how UAVs using the 802.11 family of protocols handle de-authentication attacks.

The de-authentication attack was successful. The attack was repeated three times to confirm the result. In addition to de-authenticating the UAV from the control station, this test identified generic states that the Parrot enters when abnormal events occur. In the case of losing data link control, the UAV enters "hover mode", maintaining current altitude until connection is re-established. Once connection is re-established the UAV enters "landing mode", with the UAV landing before control is regained. This validates hypotheses H_4, H_5 and H_6. Further testing in this area could lead to complete third party control of the UAV.

In summary, it was found that the signature of a Parrot can be determined when the UAV is operating. Open ports were found suggesting the Parrot was vulnerable to direct connections. Also, the connection procedure between a control device and the Parrot was scanned and found to be similar to a standard wireless connection. Further, the Parrot was found to be susceptible to a de-authentication attack. Given the short time between de-authentication and re-authentication during the attack (less than three seconds), this suggests that control could be obtained by a non-authorised party, whilst the device is still airborne.

The misuse of small UAVs such as the Parrot by criminal or terrorist elements is a potential threat to critical infrastructure. This is due to their low cost, wide availability, operability in unrestricted airspace and the ability to carry a small but dangerous payload.

CONCLUSIONS AND FURTHER WORK

This study sought to explore whether the standard use and operation of a commercially available civilian UAV could be hampered. The results of a series of experiments that found, tested and evaluated vulnerabilities in the device were articulated and discussed.

Specifically, this study tested a Parrot AR Drone version 2 UAV. It was found that the device had several open ports enabled by default and could be accessed remotely by a third party. Also, the device could be de-authenticated which suggests that control could be shifted from the legitimate paired controller to another (non-authorised) device.

A limitation of this work is that it tested only one UAV, therefore it should be considered proof-of-concept. Further work would involve extending the de-authentication to full real-time control as well as examining the video stream. The Parrot has a high definition camera onboard, therefore misuse of this or any other civilian small UAV will raise privacy and legal concerns because the UAV does not physically enter a property.

REFERENCES

Ahmad, M. S., & Tadakamadla, S. (2011). *Short paper: security evaluation of IEEE 802.11w specification*. Paper presented at the Proceedings of the fourth ACM conference on Wireless network security, Hamburg, Germany.

Bellardo, J., & Savage, S. (2003). *802.11 denial-of-service attacks: real vulnerabilities and practical solutions*. Paper presented at the Proceedings of the 12th conference on USENIX Security

Symposium - Volume 12, Washington, DC.

Bristeau, P.-J., Callou, F., Vissiere, D., & Petit, N. (2011). *The Navigation and Control technology inside the AR.Drone micro UAV*. Paper presented at the International Federation of Automatic control (IFAC) world Congress, Milano(Italy).

Case, E. E., Zelnio, A. M., & Rigling, B. D. (2008). *Low-Cost Acoustic Array for Small UAV Detection and Tracking*. Paper presented at the Aerospace and Electronics Conference, 2008 NAECON 2008, IEEE National, Dayton, OH.

Draganfly. (2013). "Draganflyer-X6 Overview". from http://www.draganfly.com/uav-helicopter/draganflyer-x6a/

DroneShield. (2013). "DroneShield: A simple device that alerts you to nearby drones". from http://www.droneshield.org/Home.html

Gutro, R. (2013). HS3 Mission Identifies Area of Strong Winds, Rain in Hurricane Ingrid: NASA.

Hamran, S-E. (2010). *Radar Performance of Ultra Wideband Waveforms*. Chapter 1 of: Radar Technology, Guy Kouemou (Ed.), ISBN: 978-953-307-029-2, InTech, DOI: 10.5772/7171.

Hindle, P. (2013). UAVs Unleashed. *Microwave Journal*, 8-8,10,12,14,16,18,20,22.

Kaiser, S. A. (2011). UAVs and their integration into non-segregated airspace. *Air and Space Law, 36*(2), 161-172.

Malhotra, B., Nikolaidis, I., & Harms, J. (2008). Distributed classification of acoustic targets in wireless audio-sensor networks. *Computer Networks, 52*(13), 2582-2593. doi: http://dx.doi.org/10.1016/j.comnet.2008.05.008

Moses, A., Rutherford, M. J., & Valavanis, K. P. (2011). *Radar-Based Detection and Identification for Miniature Air Vehicles*. Paper presented at the IEEE International Conference on Control Applications, Denver, CO, USA.

Pham, T., & Srour, N. (2004, September 1). *TTCP AG-6: acoustic detection and tracking of UAVs.* Paper presented at the SPIE. 5417, Unattended/Unmanned Ground, Ocean, and Air Sensor Technologies and Applications VI Orlando, FL.

Skolnik, M. I. (2008). *Radar Handbook, Third Edition* (3rd ed.): McGraw-Hill.

Weiqun Shi, Gus Arbadjis, Brett Bishop, Peter Hill, Rich Plasse, & Yoder, J. (2011). Detecting, Tracking and Identifying Airborne Threats with Netted Sensor Fence. In C. Thomas (Ed.), *Sensor Fusion - Foundation and Applications*: InTech.

Yamaha. (2013). "Yamaha R-50 History". from http://rmax.yamaha-motor.com.au/history