ACCEPTED FROM OPEN CALL

COMMUNICATION SECURITY OF UNMANNED AERIAL VEHICLES

DAOJING HE, SAMMY CHAN, AND MOHSEN GUIZANI

ABSTRACT

Communication security is critically important for the success of Unmanned Aerial Vehicles (UAVs). With the increasing use of UAVs in military and civilian applications, they often carry sensitive information that adversaries might try to get hold of. While UAVs consist of various modules to enable them to function properly, potential security vulnerabilities may also exist in those modules. For example, by launching a GPS spoofing attack or WiFi attack, adversaries can capture the targeted UAV and access the sought after information. In fact, it has become easy to launch such attacks. In this article, we report our low-cost implementation of these attacks and suggest solutions to them.

INTRODUCTION

An unmanned aerial vehicle (UAV) is originally an aircraft that flies without any human pilot on board. Instead, its flight is controlled either remotely by an operator or by on-board computer systems autonomously. Often, UAVs are also referred to as drones. With advances in computing, communication, and device miniaturization, UAVs could also include other flying objects such as quadcopters, balloons, and gliders. Historically, UAVs were used primarily in military operations. They carry out missions that impose high levels of risk to human pilots. In recent years, however, more applications in civilian domains have been found for UAVs. They include search and rescue operations, policing, and inspection. Due to their involved missions, UAVs need to collect, process, and transmit a wide range of sensitive data. They could be related to troop movements, strategic operations, and environmental monitoring. This makes UAVs an interesting target of cyber attacks, manipulation, and theft.

Clearly, UAVs communicate among themselves and with the ground control station via wireless channels, which are vulnerable to various attacks. In fact, it is very easy to launch attacks on UAVs. Here, we consider satellite link security as an example to illustrate the security vulnerability of UAV communications. When the line of sight between a UAV and its ground controller is broken, communications between them can be carried out via the satellite. Unfortunately, some implementations are not equipped with encryption functions. As a result, the control function could possibly be taken over by an adversary. Incidentally, in 2009 a terrorist group was found to have captured an unencrypted UAV video feed using SkyGrabber, a software for capturing free satellite videos. Thus, private and critical UAV information could be accessed by unauthorized users. On the other hand, due to the lack of security mechanisms in implementations of satellite connected UAVs, legitimate access to necessary services could be blocked by Denial-of-Service (DoS) attacks.

In this article, we first give an overview of UAV communications, and present the security requirements for protocols of this kind. Then we describe our experiences in implementing a global positioning system (GPS) spoofing attack and WiFi attack, and provide defense solutions. Finally, we identify new challenges and suggest the directions of future work on securing UAV communications. By this, we illustrate the urgent need of security measures for UAVs.

OVERVIEW AND SECURITY REQUIREMENTS OF UAV COMMUNICATIONS

OVERVIEW OF UAV COMMUNICATIONS

In general, as shown in Fig. 1 [1], a UAV incorporates a set of basic modules that can be grouped into two parts, the UAV part and the ground control station (GCS) part. In the UAV part, the base system module forms the foundation and operating system of the UAV. It links different modules together by supporting inter-module communications. The sensor module consists of various sensors together with the necessary pre-processing functionalities. Commonly equipped sensors are pressure sensors, attitude sensors, and accelerometers, which are essential to safely fly at a steady speed and level. In addition, other sensors such as radar and cameras may also be equipped. GPS can take in waypoints from an aviation system to support autonomous flight, and provide location coordinates and velocity to ground controllers to pinpoint the area of the UAV. The avionic module converts the received control commands into the commands for the engine, rudder, flaps, stabilizers, and spoilers. From time to time, the UAV needs to communicate with the GCS through wireless channels. This includes receiving basic commands from the GCS and sending collected data to the GCS. The GCS not only controls and coordinates

Daojing He is with the East China Normal University. He is the corresponding author.

Sammy Chan is with the City University of Hong Kong.

Mohsen Guizani is with the University of Idaho.

Digital Object Identifier: 10.1109/MWC.2016.1600073WC

the behavior of the UAV, but also processes the data received from the UAV and sends it back. The communication functions using a wireless standard, selected from 3G, 4G, 5G, WiFi, WiFi Direct, Bluetooth, and WiMAX, are provided by the communication module of the UAV. Note that this module also supports communications among UAVs.

As can be seen from Fig. 1, the operation of UAVs depends very much on external inputs. In the literature, some effective schemes for improving the throughput performance and energy efficiency of UAV networks have been proposed [2, 3]. Naturally, the communication channels involved are wireless and thus suffer from security weaknesses. Although UAV networks (UAVNs) bear close resemblance to wireless sensor networks (WSNs) [4] and mobile ad hoc networks (MANETs) in the sense that their nodes all communicate via wireless channels, there are important differences between them. For example, the power requirements, the amount of information transmitted across channels, and the number of nodes in a WSN are much less than that in a UAVN. Also, a UVAN typically has a much larger coverage area than a WSN. Moreover, node mobility in UAVNs is much greater than that of MANETs. Although various security models have been developed for WSNs [4, 5, 6, 7] and MANETs [8, 9], they cannot be applied to UAVs due to the disparity in different properties.

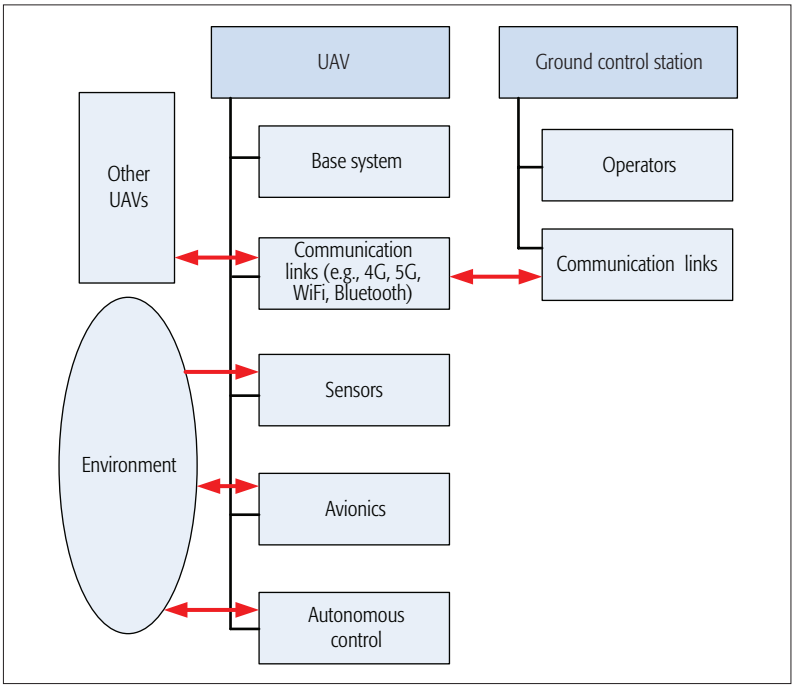


FIGURE 1. The UAV component model with information flow.

SECURITY REQUIREMENTS OF UAV COMMUNICATIONS

The information content of UAV transmission includes remote control commands, telemetry information, and mission sensor information. A remote control command is sent from the GCS to the targeted UAV; the main function is to control the UAV flight attitude and then guide the UAV to the designated position, and control the work of the mission equipment. Telemetry information includes aircraft attitude, flight parameters, equipment status, and other related information that the UAV sends to the GCS. With regard to remote control and telemetry information, their data sizes are very small; often a 12.8 kb/s transmission rate can meet the requirements, but they require real-time, reliable and secure transmission. Mission sensor information refers to the information obtained by the UAV mission equipment, such as cameras, infrared scanners, multi-spectral sensors, synthetic aperture radar, etc. The data volume of each mission sensor node is related to factors such as sensor type, image format size, resolution, and data compression technique.

At present, the security threats to UAV communications include the following.

Eavesdropping: Due to the lack of encryption and other protective mechanisms, the exchanged UAV information in the open environment can be directly accessed by the adversary.

Information Injection: Without appropriate authentication schemes, an adversary can masquerade as a legitimate entity to inject false information or commands.

Denial-of-Service (DoS) and Distributed DoS: Without the appropriate DoS/DDoS-resistant mechanism, a multitude of compromised systems (or a compromised system) attack a single targeted UAV, thereby causing denial of service for legitimate users of the targeted UAV.

Accordingly, as with traditional network security, the security goals of UAV communications include availability, confidentiality, integrity, authentication, and non-repudiation, although they have different meanings. They are illustrated as follows.

Availability: Availability is defined as a key characteristic of network security, which means that a UAV can provide effective service when necessary, even if it is being attacked. Availability relates to multiple layers. In the network layer, an adversary can tamper with the routing protocol in UAV ad hoc networks. An example is when network traffic is maliciously redirected to an invalid address or off the network. In the session layer, an adversary could delete the encrypted session channel. In the application layer, the key management service can also be threatened. A DoS attack can be launched on each protocol layer of UAV communications, such that normal services are not available. For example, in the physical layer, the adversary can interfere with the communication channel through larger power blocking. In the network layer, the adversary destroys the routing information, so that the network cannot be interconnected. At a higher layer, the attacker disables the high-level services by forging a variety of applications. For UAV communications, availability also relates to the power supply problem. When there is no energy for each UAV, the UAV will be completely paralyzed.

Confidentiality: This requirement ensures that communication information among UAVs cannot be leaked to unauthorized users, entities, or processes.

Integrity: This means that the message transmission process is not interrupted, and the received information should be exactly the same as the sent information. If there is no integrity

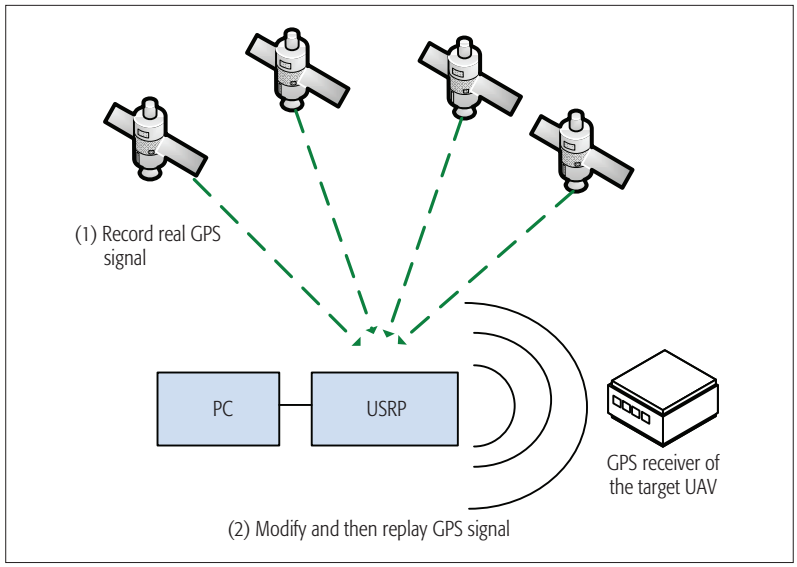


FIGURE 2. A record-modify-and-replay system for GPS spoofing.

protection, malicious attacks in the network or wireless channel interference may cause the information to be destroyed, and thus become invalid.

Authentication: Because of the multi-source and heterogeneous network for UAV communications, each node needs to be able to recognize the identity of the node that it communicates with. At the same time, it is better to ensure user authentication without the global certification agency. Without authentication, an adversary can easily impersonate as a legitimate node and then obtain important resources and information and interfere with the communication of other nodes. Also, authentication is usually not enough, as it is only responsible for ensuring the identity of a person, and therefore it is important to decide whether or not to allow an entity to do certain things by authorization.

Non-Repudiation: Non-repudiation is used to ensure that a node cannot deny that it has issued certain information. This requirement strengthens the management of various actions and thus prevents the denial of the behavior that has occurred. The aim is to provide a basis or means of inquiry on the emergence of security issues.

Two Specific Attacks

In addition to the general security requirements described above, here we describe two specific attacks through example scenarios, along with the defense solutions.

GPS Jamming and Spoofing

The Global Positioning System is a navigation system that provides precise velocity, timing, and position information to receivers based on satellites. Both military (P-Code) and civilian signals are broadcast by GPS satellites. However, only military GPS signals are encrypted to prevent unauthorized use and counterfeiting, while civilian GPS signals are sent as clear signals. The transparency of civilian GPS signals, on one hand, offers free accessibility to anyone and leads to extremely popular civilian GPS systems. On the other hand, it makes civilian GPS systems vulnerable to various attacks such as jamming, meaconing, and spoofing.

Jamming is an attack that prevents a receiver from receiving the authentic GPS signals. This can be achieved by sending interfering signals with higher power in the same frequency band. Meaconing refers to capturing genuine GPS signals and retransmitting to the receiver with added delay. In spoofing, the adversary transmits a malicious signal with power stronger than that of the authentic signal so that the receiver is misled to use the forged signal for subsequent processing. It is a more damaging attack and is one of the major threats in civilian GPS services, as the receiving UAV is taken over by the adversary.

Incidentally, a recent security attack has been launched on UAVs, resulting in the capture of a US RQ 170 Sentinel by Iranian forces [10]. It is postulated in [11] that the UAV was subject to a GPS spoofing attack. Such an attack can be launched by making use of the details of the GPS functionality. The attacker could generate a spoofed GPS signal that has higher power than the GPS satellite signal, and overlay it over the GPS satellite signal. The UAV is then led to wrongly estimate its current position. Presumably, the Iranian side jammed the satellite channel of the UAV and spoofed the GPS signal so that the UAV was landed safely in Iranian territory.

Due to the predictability of civilian GPS signals, successful spoofing attacks are quite achievable. The steps involved in a spoofing attack are:

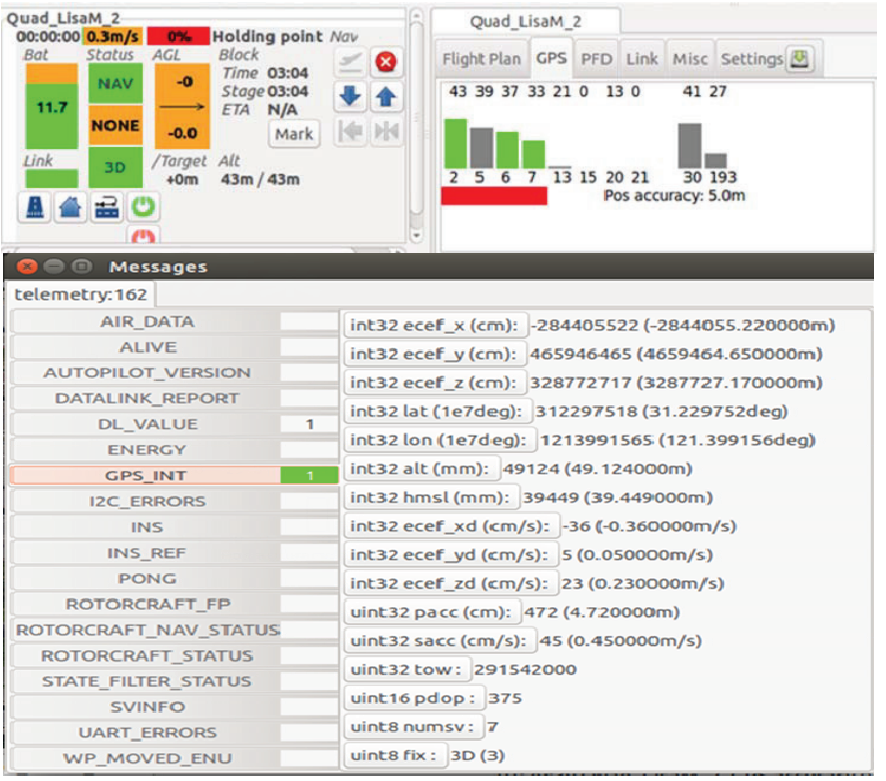
1. Acquire and track the coarse/acquisition signals.
2. Produce and calibrate a fake signal.
3. Align the forged and authentic GPS signals.
4. Raise the power of the forged signal to suppress the authentic signal.

We have designed and developed a low-cost GPS record-modify-and-replay system, with hardware based on the Ettus USRP (Universal Software Radio Peripheral) radio family and software based on GNU Radio. Ettus radio provides a development platform for software defined radios at a low cost. It supports a wideband transceiver front end that can operate at any of the GPS signal frequencies in the entire GPS signal band. Thus, record and playback of civilian GPS signals are supported.

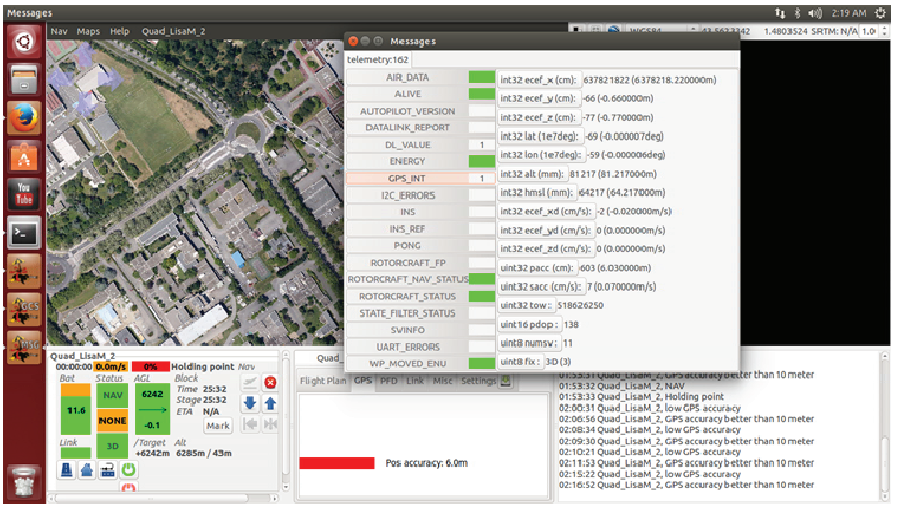
Figure 2 depicts the system and the working process. The GPS signal received from the satellites is recorded. It is then converted into baseband and sampled by the USPR. The sampled data are then stored by the PC. For replaying, the PC sends the modified baseband data to the USRP for A/D conversion and up-converting to RF signals. This reproduced signal can be used for GPS spoofing. Figure 3 shows the results of a GPS spoofing attack. Figure 3a depicts the real GPS data (e.g., the longitude is about 121.39 and the latitude is about 31.23) through the quadcopter's ground control station's GPS API when the UAV is located at the East China Normal University in Shanghai City. In contrast, Fig. 3b shows the spoofing GPS message received by the ground control station (e.g., the longitude and latitude are both zero, respectively) from the quadcopter at the same location when our GPS record-modify-and-replay system is functioning. The figure demonstrates that the record-modify-and-replay system works well in the GPS band.

Countermeasure

It is challenging to design defense solutions for the GPS spoofing problem. Here, we summarize



(a)



(b)

FIGURE 3. Results of GPS spoofing attack (through the quadcopter's ground control station's GPS API); a) The real GPS message (the longitude is about 121.39 and the latitude is about 31.23)(when the quadcopter is located at the East China Normal University in Shanghai city); b) The spoofing GPS message, the longitude and latitude is zero, respectively (when the quadcopter is located at the East China Normal University in Shanghai city).

existing solutions. The first approach is a jamming-to-noise sensing defense [12]. This approach defends against GPS spoofing by monitoring the total received power in the GPS band of interest. As the presence of spoofing signals would increase the total received power, it could be readily detected by a jamming-to-noise (J-N) sensor. Thus, this approach can force the spoofing signal to be below a certain threshold. Also, it is quite a simple approach, and is readily-implementable because it is stand-alone and does not rely on any cryptographic function. However, if the threshold is set to a suitable value to achieve a reasonable rate for false alarm, a J-N sensor may not be able to detect a spoofing attack as the spoofed signal only has slightly higher power than the authentic signal.

The second approach is a multi-antenna defense [13]. This approach makes use of the fact that it is difficult to mimic the relative carrier phase of the GPS signals as seen by multiple spatially-separated antennas. It is an effective solu-

Ettus radio provides a development platform for software defined radios at a low cost. It supports a wideband transceiver front end that can operate at any of the GPS signal frequencies in the whole GPS signal band. Thus, record and playback of civilian GPS signals are supported.

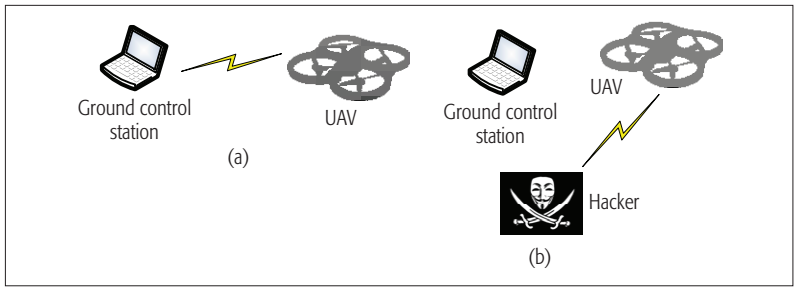


FIGURE 4. De-authentication attack: a) before the attack; b) after the attack.

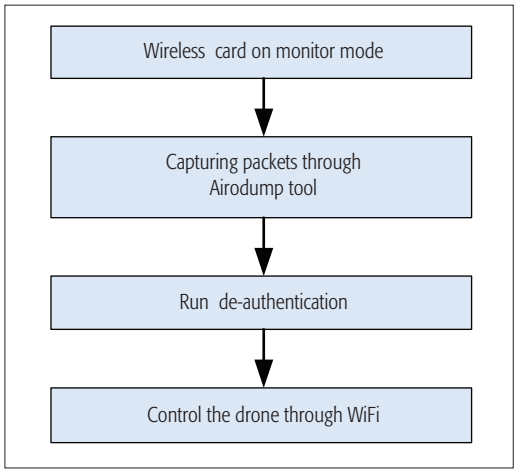


FIGURE 5. A custom step build of hijacking a drone.

tion against spoofing, especially when combined with the physical security function offered by the antenna array. Similar to the previous approach, it is also a stand-alone and non-cryptographic solution. However, the additional RF front-ends and antennas incur more weight and cost to the receiver. Clearly, the most effective approach is to apply cryptographic authentication for C/A signals [14]. Unfortunately, it is not as feasible as the other approaches because it requires significant time and cost for software and hardware modifications.

IEEE 802.11 Wireless Attacks

The IEEE 802.11 standards are widely used for wireless local area networks, and also for ad hoc networking for a range of devices. For example, they can be used as a data link technology between a small civilian UAV, Parrot AR Drone v2, and its ground controller, which could be just a smart phone or tablet PC. For wireless communications, devices must know with whom they communicate before communication sessions commence. Management frames are used to establish this initial association. If management frames are not protected, wireless devices are subject to a number of attacks. One of the major attacks against 802.11 protocols is de-authentication, in which de-authentication management frames are sent to two communicating devices to disconnect them. Then, the attacker can launch further attacks to take control of the UAV, as shown in Fig. 4.

Since a Parrot AR Drone allows users to connect to it and control it via 802.11 protocols, we can gain control of it by packet capturing. Such apps are even available for users to download. Here we use Aircrack-ng [15] to de-authenticate a valid client and gain control over the system.

Figure 5 illustrates the steps of initiating the attack. Aircrack-ng provides a number of tools to hack a device. First, Airmon-ng changes the setting of the wireless card from managed mode to monitor mode. By installing the necessary drivers, the network card can view all the traffic. Second, Airodump-ng can capture packets of a particular client among all the observed clients. De-authentication packets are then sent to disconnect the targeted UAV. Finally, other functions of Aircrack-ng can be used to gain access to the UAV.

Countermeasure

Some commonly deployed security measures can be used to defend against the above attacks. Clearly, encryption can be used to protect the data transferred over the WiFi network. For example, enabling WPA2 (802.11i-2004) encryption is a good way to secure a wireless network. The key length should be appropriately chosen to defeat brute force attacks. Clearly, longer keys are harder to be cracked by brute force ($2^{64} < 2^{128} \ll 2^{256}$ possible keys). It is strongly recommended in the IEEE 802.11i standard that a key should have at least 20 characters. The greater the mix of lower and uppercase letters, numbers, and symbols in the key, the better it is protected against dictionary attacks. Another possible approach is to disable the broadcast of SSID (service set identifier) in order to hide the access point. Alternatively, access to systems can be restricted to a pre-registered MAC address only.

Prospects

Although the research field of communication security of UAVs has received significant attention, there are still many challenging issues that need to be addressed. Here we list several important ones.

Security Access Specifications on Unmanned Aerial Vehicles

Most existing UAV service networks belong to self-organized private networks. The security protection strength of those networks is often weak, and thus there exist security risks such as illegal connections, malicious control, unauthorized access, malicious attacks, and others. Thus, future work should consider how to develop unified security access specifications for UAVs.

Many applications in current mobile systems have already used public key techniques to achieve end-to-end security. Similarly, public key infrastructure is also a viable solution for authentication, integrity, privacy, availability, and scalability of UAVs. Thus, some research should focus on how to develop secure and efficient access solutions on UAVs.

Efficient, Secure Communication Infrastructure for UAVs

It is not efficient to apply the existing secure communication infrastructure to real-time data transmission for UAVs. Let us return to the example of video transmission between UAVs and their ground control station. Even though it is clear that security

measures are needed to protect the signal, only a certain amount of video signal can be encrypted to maintain a real time connection, as video encryption places significant demands on resources. Also, the existing UAVs often use customized protocols and transmission systems, and thus the traditional communication security approaches such as anomaly detection mechanisms cannot be efficiently employed to ensure the security of real-time data transmission for UAVs.

Also, the environment faced by UAV ad hoc networks is very complex, so it is necessary to research and design the distributed security policy and method with good applicability and security strength for UAV ad hoc networks. However, network security is regarded as a way to ensure security of normal operations of a network; it is not allowed to occupy large blocks of resources on the nodes. Thus, the increased security measures should not deteriorate network performance or affect the normal operation of the network. Therefore, in future research work it will be necessary to achieve a good balance between the strength of the security measures and the performance of the network communication.

Conclusions

UAVs have been increasingly used in military and civilian applications in recent years. One of the critical factors that ensures the proper operation of UAVs is communication security. Otherwise, UAVs can be captured by adversaries. In this article, we have demonstrated that some devastating attacks, such as GPS spoofing and WiFi attacks, which seem to be complicated, can be launched easily at a low cost. Thus, communication security for UAVs needs to be tightened.

Acknowledgment

This research is supported by a strategic research grant from the City University of Hong Kong [Project No. 7004429], the Pearl River Nova Program of Guangzhou (No. 2014J2200051), the National Science Foundation of China (Grants: 51477056 and 61321064), the Shanghai Rising-Star Program (No. 15QA1401700), the CCF-Venustech Hongyan Research Initiative, the State Grid Corporation Science and Technology Project "The pilot application on network access security for patrol data captured by unmanned planes and robots and intelligent recognition based on big data platform" (Grant No. SGSDDK000KJJS1600065), and the Specialized Research Fund for the Doctoral Program of Higher Education.

References

[1] K. Hartmann and C. Steup, "The Vulnerability of UAVs to Cyber Attacks — An Approach to the Risk Assessment," *Proc. 5th Int'l. Conf. Cyber Conflict (CyCon)*, June 2013, pp. 1–23.

[2] Z. Fadlullah *et al.*, "A Dynamic Trajectory Control Algorithm for Improving the Communication Throughput and Delay in UAV-Aided Networks," *IEEE Network*, vol. 30, no. 1, Jan. 2016, pp. 100–05.

[3]A. Abdulla *et al.*, "Toward Fair Maximization of Energy Efficiency in Multiple UAS-Aided Networks: A Game-Theoretic Methodology," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, Jan. 2015, pp. 305–16.

[4] J. Granjal, E. Monteiro, and J. Silva, "Security in the Integration of Low-Power Wireless Sensor Networks with the Internet: A Survey," *Ad Hoc Networks*, vol. 24, Jan. 2015, pp. 264–87.

[5] D. He, S. Chan, and M. Guizani, "Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, Jan. 2015, pp. 389–98.

[6] O. Sadio *et al.*, "Improving Security and Mobility for Remote Access: A Wireless Sensor Network Case," *Proc. IEEE Int'l. Conf. Signal Processing, Informatics, Commun. Energy Systems*, Feb. 2015, pp. 1–5.

[7] L. Zhu and Z. Zhan, "A Random Key Management Scheme for Heterogeneous Wireless Sensor Network," *Proc. Int'l. Conf. Cyber Security Smart Cities, Industrial Control System and Communications (SSIC)*, Aug. 2015, pp. 1–5.

[8] W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," *IEEE Trans. Vehic. Tech.*, vol. 63, no. 9, Nov. 2014, pp. 4585–93.

[9] P. Rajakumar, V. Prasanna, and A. Pitchaikkannu, "Security Attacks and Detection Schemes in MANET," *Proc. Int'l. Conf. Electronics Commun. Systems (ICECS)*, Feb. 2014, pp. 1–6.

[10] CNN Wire Staff, "Obama Says U.S. Has Asked Iran to Return Drone Aircraft," 22 Oct. 2013.

[11] A. Kerns *et al.*, "Unmanned Aircraft Capture and Control via GPS Spoofing," *IEEE Trans. Vehic. Tech.*, vol. 31, no. 4, April 2014, pp. 617–36.

[12] D. Borio and C. Gioia, "Real-Time Jamming Detection Using the Sum-of-Squares Paradigm," *Proc. 2015 Int'l. Conf. Localization GNSS (ICL-GNSS)*, June 2015, pp. 1–6.

[13] J. Magiera and R. Katulski, "Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing," *J. Applied Research and Technology*, vol. 13, no. 1, Feb. 2015, pp. 45–57.

[14] A. Kerns, K. Wesson, and T. Humphreys, "A Blueprint for Civil GPS Navigation Message Authentication," *Proc. IEEE/ION Position, Location and Navigation Symposium (PLANS)*, May 2014, pp. 262–69.

[15] http://www.aircrack-ng.org/

Biographies

Daojing He (S'07, M'13) (e-mail: djhe@sei.ecnu.edu.cn) received the B.Eng. (2007) and M. Eng. (2009) degrees from Harbin Institute of Technology (China), and the Ph.D. degree (2012) from Zhejiang University (China), all in computer science. He is currently a professor in the School of Computer Science and Software Engineering, East China Normal University, P.R. China. His research interests include network and systems security. He is an associate editor or on the editorial board of international journals, including *IEEE Communications Magazine* and *IEEE/KICS Journal of Communications and Networks*.

Sammy Chan (S'87, M'89) (e-mail: eeschan@cityu.edu.hk) received B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994 he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994 he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

Mohsen Guizani (S'85, M'89, SM'99, F'09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and Chair of the Electrical and Computer Engineering Department at the University of Idaho, USA. He was a professor and the Associate Vice President for Graduate Studies at Qatar University, Doha, Qatar. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial boards of six technical journals, and he is the founder and EIC of *Wireless Communications and Mobile Computing*, published by John Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is an IEEE Fellow and a Senior Member of ACM.

The increased security measures should not deteriorate network performance or affect the normal operation of the network. Therefore, in future research work it will be necessary to achieve a good balance between the strength of the security measures and the performance of the network communication.