Risk assessment of SDR-based attacks with UAVs

Frédéric Le Roy, Christian Roland, Denis Le Jeune, Jean-Philippe Diguet

Risk assessment of SDR-based attacks with UAVs

Frederic Le Roy[1], Christian Roland[2], Denis Le Jeune[1] and Jean-Philippe Diguet[3]
Lab-STICC, ENSTA Bretagne[1], Université de Bretagne-Sud[2], CNRS[3], Lorient / Brest, France

***Abstract*—The use of Unmanned Aerial Vehicles (UAVs) is rising constantly whether for leisure or professional purposes in civilian or Defense domains. We consider in this study small civilian aerial drones of different types, which are low cost, available off the shelf and so affordable for individuals. Simultaneously, they have also raised security concerns for critical sites such as nuclear stations, strategic locations like official buildings, crowded places as stadiums, etc. The aim of this paper is to provide a survey of the risks assessment with and for UAVs in general. Regarding the security concern we pay a specific attention to attacks that are facilitated and can benefit from an easy access to Software Defined Radio (SDR) boards that can be embedded in the UAV or in the ground segment.**

***Index Terms*—Civilian drones, Software Defined Radio, Security, Attacks**

I. Introduction

Classical threat concerning UAVs is the attack from the drone to a ground target, the counter attack implies a detection up to a neutralization operation from the ground. This schematic view can both be extended to the cases where the attack is from the ground to the drone of from a drone to another drone. We observe that low cost SDR environments and boards can strongly facilitate the implementations of such existing and possible attacks, on the other hand, it also provides opportunities for counter attacks. This survey is mainly devoted to the approaches with acquisition and processing operations by means of low cost SDR COTS (Commercial Off The Shelf) board implementation. So we looked for civilian drone platforms only, of fixed wings or multirotor types, with COTS (modified or not) or DIY (Do It Yourself) UAVs. Different types of communications for the ground control, video transmission and telemetry link can be used like Wi-Fi, LTE (Long Term Evolution), Industrial Scientific and Medical bands (ISM, e.g. 433 or 866 MHz). Such constraints do not prevent to have efficient actions presenting a severe risk.

This paper is organized as follows. In section II, we first present a classification of the risks for this context. Beyond the synthesis of existing demonstrated attacks and countermeasures, the objective is to investigate opportunities which are unexplored or underused so far but that could turn into major risks in the near future. Then, our ambition is not to identify inherent vulnerabilities and countermeasures, which is a future work, but to show how SDR platforms can be used to address them. In section III we briefly present the SDR platforms under consideration with the definitions and the limiting constraints. Sections IV focus to the known literature attacks from drone to ground and from ground to drone respectively. Finally in section V, we summarize current limitations and new concepts not considered so far. We finally conclude by focusing on an analysis of risk for the next future.

II. Classification and related state of the art

In [1] an attack taxonomy to UAV has been proposed, this taxonomy had been firstly introduced by [2] for autonomous vehicle security and adapted by Krishna et al. to UAVs. In this model, two branches separate attack vectors and targets. Attack vector is the way used by an attacker to access to a server or a computer in order to send or execute malicious code on a target device. Two sub-branches are used to define invasive and non-invasve attacks. The first one requires access to the hardware while the other uses side channel such as sound, infra-red or electromagnetic fields. The other branch lists all the targets of potential attack vectors such as sensors, communication links or control units. Another taxonomy proposed in [3] classifies attacks using security parameters CIA (Confidentiaity, Integrity, Availability) this concept is extended to Privacy and Trust when most of the previous attacks can be mapped.

In this study, we chose to present drone attacks with a different point of view, it results in a classification summarised in Table I. The main objective is to identify where the SDR board is or can be used to implement an attack and/or a countermeasure, and so to highlight current and future risks. So the analysis focuses on two facets: the first corresponds to the targets of the attack and the second one corresponds to the direction of the attack. The targets of the attack and so possible countermeasures are multiple, it can be the remote telecontrol, the telemetry, the sensor (mainly GPS), the physical signature (audio, optical, infra-red, radar, electromagnetic, ...), the embedded software or cognitive channel (cognitive scrambling, stealthy communication, ...). The direction of attacks can be from ground to drone or drone to ground, it could also be from drone to drone. We found none or very few attacks on the remote control or data acquisition links from drone to drone or drone to ground direction. Nevertheless, SDR platform is interesting in this context, because it can change or download its configurations to match its strategies to its targets. This is clearly an upcoming risk that must be consider, since it is easy to imagine an attack based on a malicious use of a wireless network that would be implemented with a SDR platform. For instance, the IMSI (International Mobile Subscriber Identity) catcher can be embedded by a UAV, or cognitive embedded SDR radio can reuse spectrum inactivity (or work as a smart jammer) in unauthorised bands. Few works published in the scientific literature exist on data theft (line 2), but press articles relate such facts like the well known case of insurgents in Iraq

that hacked live video feeds from unmanned American MQ-1 Predator which was not encrypted. This type of events brings to the light, the possibility of such attacks that require an urgent answer. For sensors hacking (line 3), the same attacks and countermesures can be imagined for drone to drone and drone to ground direction. Compared to what is observed with ground to drone direction, one can also speculate that better results may be obtained thanks to the mobility of UAV. To the best of our knowledge, radio footprint tampering (line 4) has not yet been (at least published) developed and embedded on a drone. However there is no doubt that this is a rising upcoming risk. Firmware or forentics attacks (line5) are currently rare, however for some drones such as Dji, firmware updates uses Wi-Fi, so such an attack is possible and so may soon be revealed. We will extend this discussion in Section III.

III. SDR PLATFORMS

SDR nodes provide flexibility, upgradability for civilian and military radio equipment. They can be used with success to implement multistandard terminals or when context-aware radio equipment is needed. In their new survey on SDR, the authors of [46] discuss on architecture, design methodologies, development tools and perspectives. They propose a comparison of SDR platforms according to the following criteria : programmability, flexibility, portability, power consumption, energy efficiency and cost. This synthesis is interesting for software developers to choose an SDR platform and tools that best-fit their needs but important features are missing for radio and system architects. For instance, it is difficult to choose the best SDR platform that can be embedded by a drone for one given application (e.g. detection, eavesdropper, spoofer, telecontrol, telemetry). There is little information available related to frequency tuning capability, oscillator precision, radio-frequency bandwidth, transmission power, number of receiver and transceiver channels and weight. In the context of a small UAV, capacity and form factor such as weight and size are critical to allow the system to be embedded. Moreover the precision parameters are important for problems such as localisation, stealth and spoofing.

The purpose of Table II is to provide a current overview of SDR platforms solutions that do not exceed a cost of 15,000 euros. This is an arbitrary choice but we think it can reflect a kind of maximum price (or psychological threshold) SDR amateurs may consider for the purchase a ground station or an embedded platform. Of course, this list is not exhaustive but we have tried to show the most popular actors of the market place as well as popular platforms in the field of radio ham and academic research. In this table, the first three columns concern communication protocols used by attackers or defenders. The next three columns represent the degree of performance for the acquisition front end. The seventh column gives the scaling of computing power of the SDR platform. The last four columns are interesting to evaluate the SDR platform embeddedability on UAVs.

SDR platform benefits differ according to the role (attacker or target) played by the platform and its mobility needs in the context of UAV attacks. Next, we will identify use cases that justify the use of SDR platform according to these requirements.

A. Interest of SDR on the attacker side

To the attacker side, target can be mobile or static.

1) From the ground to UAVs (fixed SDR): when the attacker and the target are static, the SDR platform offers some flexibility thanks to the access to baseband signals. Time and frequency attacks can then be directly implemented in software. However, when the SDR platform uses an operating system, latency should be taken into account. For example, some protocols used by RFID (Radio Frequency Identification) technology, which is strongly constrained in time, can't be directly supported by a software implementation using SDR platforms [47]. For this type of attack, columns 1 to 6 related to radio front end and converters are the most important criteria of Table II.

2) From the UAV to Ground or UAVs (mobile SDR): when the attacker has a mobile SDR platform, the attacker is in the same channel state as the target, so it can track the target and adapt its algorithms to the slight fluctuations of channel to escape many detection algorithms based on Doppler, delay or power analysis [48]. In this use case, columns 8 to 10 related to form factor and power consumption are the most important criteria of Table II because SDR platform is used as the payload of a UAV.

B. Interest of SDR on the target side

1) Ground against UAV (fixed SDR): direct access to radio signal gives to the defender, the ability to extract relevant signal information like Doppler, Delay, or Phase Coherence. It has then many possibilities to adapt the UAV search algorithms to the observed channel characteristics. In this kind of counter-measures, important columns of Table II are also the same as for fixed SDR attackers platforms. When a defender seeks to locate a single UAV or a swarm, high resolution antenna processing algorithm techniques such as MUSIC, Root-MUSIC or ESPRIT can be implemented by the SDR platform. The expansion capabilities of several synchronized antennas, namely external oscillators (see column 5 of Table II) are important to consider.

2) UAV against Ground or UAVs (mobile SDR): in transmitters geolocalization, the mobility of defenders allows receivers to change the positions of fixed points used by a multilateration algorithms. Tracking of a Periodic RF transmitter with a mobile receiver is an old topic well discussed by the scientific community. Many algorithms, based on optimal sensor placement, have been developed to estimate Time Difference of Arrival Localization (TDOA). Then, mobile SDR platform has the ability to locate transmitters with better accuracy. The TDOA time resolution, and consequently the spatial resolution of a sensor network, depends on the accuracy of sample rate and bandwidth. For these reasons, columns 2, 5 and 8 to 10 of Table II related to accuracy of oscillator, board form factor and power consumption are critical. For such an embedded

TABLE I
SDR-BASED ATTACKS

	Attack from Ground station to Drone		Attack from Drone to Drone		Attack from Drone to Ground	
	Attack	Detection & Countermeasures	Attack	Detection & Countermeasures	Attack	Detection & Countermeasures
Remote Control	[4] [5] [6] [7] [8]	[5] [9] [10]	—	—	—	[11] [12] [13] [14] [15]
Remote Data Acquisition	[5]	—	—	—	[16]	—
Sensors	[17] [18] [19] [20] [21] [26] [27] [28]	[22] [23] [24]	—	[25]	—	[25] [24]
Physical Signature	—	[29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40]	—	—	—	—
Firmware / Forensics	[41], [42], [43]	[44]	[45]	—	—	—

TABLE II
SDR PLATFORMS COMPARISON

	Freq. Bands (MHz-GHz)	Bandwidth (MHz)	Tx power (dbm)	Resolution (ADC/DAC)	Oscillator precision (ppm)	Rx × Tx	Computing Unit	Power (W)	FF Size(mm)	FF Weight (g)	Battery
USRP E312	70-6	56	> 10	12/12	± 2	2x2	Zynq 7020	2-6	133 x 68.2 x 31.8	446	yes
USRP X320	DC-6	120	> 10	14/16	± 2	2x2	Kintex 7-410T	45	217 x 218 x 39	1700	no
Matchstiq S11	70-6	50	< 13	12/12	± 1	1x1	Freescale iMX.6 Spartan6 LX45T	?	112 x 42 x 29	142	no
Quadratiq	70 - 6	50	5	12/12	± 1	4x1	Zynq 7030	18	214 x 147 x 41	708	no
PicoZed	70-6	0.2-56	9	12/12	?	2x2	Zynq 7035	?	Dev Zynq	?	no
PlutoSDR	325-3.8	20	7	12/12	?	1x1	Zynq 7010		117x79x24	114	no
PicoSDR	56-6	56	10-18	12/12	?	4x4/8x8	Virtex6 / Quad-Core i7	35-86	48x215x290 / 45x365x378	2400/5600	no
HackRF	1-6	20	15	8/8	± 20	1x1		?	125x80x26	201	no
BladeRF	300-3.8	28	6	12/12	± 1	1x1	Cyclone IV	4	87x131x18	80	no
LimeSDR	100-3.8	61.44	10	12/12	± 4	2x2	Cyclone IV	4	110x60	20	no
XTRX	100-3.8	61.44	10	12/12	$< \pm 1$	2x2	Artix 7 35T	?	30x51	20	no
AirSpy	24-1.7	6		12	± 0.5	1x0		?	77x26x10	21	no
RTL-SDR V3	0.5-1.7	2.7		8	± 1	1x0		< 2	?	?	no
SDRplay	0.1-2	10		12	± 0.5	1x0		< 1	95x80x30	110	no
FunCube	0.15-0.24/ 420-1.9	?		?	?	1x0		< 1	?	260	no
Warp v3	2.4G / 5.4	40	20	12/12	?	2x2	Virtex-6 LX240T	?	?	?	no
Kudar	5.25G-5.85	30	21	14/16	?	1x1	Virtex-2 P30	?	?	?	no

system, the computing unit (Col. 7) is also very critical since it must not introduce any prejudicial latency.

IV. STATE OF THE ART OF SMALL-UAV RELATED ATTACKS

We identify here the different cases encountered in the current literature with the use of a small UAV platform associated with a COTS SDR solution and we map out these cases in Table I. Three types of applications can be considered, depending on which side we position the SDR hardware and where is the target of the attack: from a ground station to a drone platform, conversely from a drone to the ground, or even from a drone to another drone. In each case, we can regard the SDR to operate the attack or the defense. These different families of applications are represented by columns of Table I. We then detail in rows what is the concrete element of the drone implied in the attack. This element can be the control system, the data telemetry wireless link, the sensors of the platform like a global navigation satellite system (GNSS) component or an inertial navigation system (INS), the measure of a physical signature, for example a visual, electromagnetic or acoustic one. We also consider the possibility to realize the attack directly on part of the hardware.

We can see from this Table that the majority of papers, that address drone-involved risks, are in the ground to drone direction. This is due to the facility to operate with a SDR embeddable solution in the ground side. Nevertheless, as seen in Section III, some SDR solutions can be embedded in a mobile platform, making possible the operation in the drone to ground direction. Drone to drone operations are however, so far very rarely investigated.

In the intensity of uses, we can see the high correlation with the technical aspects of Table II. However, we don't see any structured convergence in the time evolution of the intensity in the different cases, beyond the evolution from a ground side of operation to a mobile one due to the technical correlation. This suggests that the domain is not yet really matured, and that it will probably grow in the future. We discuss this point in the next section.

V. Synthesis and Conclusion

Our study shows that some cases are well explored like "Attacks and Counter-measures" from Ground to Drone. But they also benefit from the poorness of current drone attacks that don't use today SDR capacities as we can see in the Columns "Attack from Drone to Ground" in Table I.

The challenge on the UAV side is the use of embedded SDR, which has already been experimented for specific application like wildlife tracking [49]. Once this question is solved and optimized to provide expected performances, it will actually means that SDR can be used to elaborate more sophisticated attacks. These attacks can for instance rely on cognitive radio techniques to develop stealth communications and remain undetected by conventional base stations. The embedded SDR can also be used to provide the UAV with efficient counter-measures against jamming for instance.

These threats will likely appear but on the ground SDR can also be used to improve counter measures against current and upcoming attacks by introducing adaptive techniques also based on cognitive radio concepts. These detection techniques are known but require today high performance computing [50]. Meanwhile existing solutions are sill improving, for instance SDR can be used to develop smarter GPS Spoofing that take into account the UAV position in order to adapt power [51]. Real-time processing is a challenge on both sides. On the ground real-time detection is required to detect unknown waveforms that can be developed with embedded SDR. On the UAV side, the use of field programmable gate array circuit (FPGA) can also be required to implement fast bandwidth scanning with fast Fourier transform (FFT) to quickly switch to available second user (SU) channels or simply unused channels. Such embedded processing imposes to avoid high-latency I/Os and so requires near sensor computing [47].

To conclude SDR is an opportunity for both attacks and counter-measures, it represents a research domain that must be explored to anticipate upcoming threats. Interesting topics such as "how SDR can improve security or insert new vulnerabilities to UAVs" will be studied in future work.

References

[1] C. G. L. Krishna and R. R. Murphy. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *IEEE Int. Symp. on Safety, Security and Rescue Robotics (SSRR)*, October 2017.

[2] V. L. L. Thing and J. Wu. Autonomous vehicle security: A taxonomy of attacks and defences. In *IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData*, Dec. 2016.

[3] G. Choudhary, V. Sharma, and I. Gupta, T.and You. Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives. *arXiv preprint arXiv:1808.00203*, 2018.

[4] J. Andersson. Attacking DSMx Spread Spectrum Frequency Hopping Drone Remote Control with SDR(Software Defined Radio). In *PacSec*, Tokyo, October 2016.

[5] S. Bunse, C.and Plotz. Security Analysis of Drone Communication Protocols. In Mathias Payer, Awais Rashid, and Jose M. Such, editors, *Engineering Secure Software and Systems*, LNCS. SIP, 2018.

[6] K. Domin, E. Marin, and I. Symeonidis. Security Analysis of the Drone Communication Protocol: Fuzzing the MAVLink protocol. page 7.

[7] D. Mototolea and C. Stolk. Software Defined Radio for Analyzing Drone Communication Protocols. In *Int. Conf. on Communications (COMM)*, June 2018.

[8] E. Rivera, R. Baykov, and G. Gu. A study on unmanned vehicles and cyber security. *Texas (Univ.), USA*, 2014.

[9] D. Mototolea and C. Stolk. Detection and Localization of Small Drones Using Commercial Off-the-Shelf FPGA Based Software Defined Radio Systems. In *Int. Conf. on Communications (COMM)*, June 2018.

[10] H. Shin, K. Choi, Y. Park, J. Choi, and Y. Kim. Security Analysis of FHSS-type Drone Controller. In Ho-won Kim and Dooho Choi, editors, *Information Security Applications*, volume 9503. SIP, Cham, 2016.

[11] R. J. Bamberger, Jay G. Moore, Ravi P. Goonasekeram, and David H. Scheidt. Autonomous geo location of RF emitters using small, unmanned platforms. *Johns Hopkins APL technical digest*, 32(3):636–646, 2013.

[12] O. Bar-Shalom and A. J. Weiss. Emitter geolocation using single moving receiver. *Signal Processing*, 105:70–83, December 2014.

[13] A. Jadon, Z.T. Williams, C. Kafka, H. Rotta, S. Roy, and C.W. Lum. A Database System Architecture for Air-to-Ground UAS Link Characterization. In *AIAA Info. Systems-AIAA Infotech@Aerospace*. 2018.

[14] P. Scerri, R. Glinton, S. Owens, D. Scerri, and K. Sycara. Geolocation of RF emitters by many UAVs. In *AIAA Infotech@ Aerospace Conf. and Exhibit*, page 2858, 2007.

[15] Z. Wang, E. Blasch, G. Chen, D. Shen, X. Lin, and K. Pham. A low-cost, near-real-time two-UAS-based UWB emitter monitoring system. *IEEE Aerospace and Electronic Systems Mag.*, 30(11):4–11, Nov. 2015.

[16] W. D. Watson, S. Huntsman, and J. T. Dolan. Software Defined Networks (SDNs) of RF Internet of Things (RIOTs) on Unmanned Aerial Systems (UASs). In *IEEE Military Communications Conf. (MILCOM)*, pages 291–296, October 2017.

[17] T. Ebinuma. gps-sdr-sim. https://github.com/osqzss/gps-sdr-sim.

[18] L. Huang and Q. Yang. GPS SPOOFING - Low-cost GPS simulator. In *DEF CON 23*, Las Vegas, August 2015.

[19] E. Horton and P. Ranganathan. Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. *The Journal of Global Positioning Systems*, 16(1):9, July 2018.

[20] A. Luo. Drones Hijacking - Multi-dimensional attack vectors and countermeasures. In *DEF CON 24*, Las Vegas, August 2016.

[21] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. Unmanned Aircraft Capture and Control Via GPS Spoofing: Unmanned Aircraft Capture and Control. *Journal of Field Robotics*, 31(4):617–636, July 2014.

[22] A. Costin and A. Francillon. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA*, pages 1–12, 2012.

[23] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi. Efficient drone hijacking detection using onboard motion sensors. In *Design, Automation & Test in Europe Conf. (DATE)*. IEEE, 2017.

[24] Y. Liu, S. Li, Q. Fu, and Z. Liu. Impact assessment of GNSS spoofing attacks on ins/GNSS integrated navigation system. *Sensors*, 18(5):1433, 2018.

[25] H. Sedjelmaci, S. M. Senouci, and N. Ansari. A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks. *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, 48(9):1594–1606, September 2018.

[26] T. Rosa. GNSS/GPS Radio Hacking - From Beautiful Equations to Serious Threats. In *QuBit*, Prague, April 2016.

[27] N. Shijith, P. Poornachandran, V. G. Sujadevi, and M. M. Dharmana. Spoofing technique to counterfeit the GPS receiver on a drone. In *Int. Conf. on Technological Advancements in Power and Energy (TAP Energy)*, pages 1–3, December 2017.

[28] M. Strohmeier, V. Lenders, and I. Martinovic. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Com. Surveys & Tutorials*, 17(2):1066–1087, 2015.

[29] V. Brik, S. Banerjee, and S. Gruteser, M.and Oh. Wireless device identification with radiometric signatures. In *14th ACM Int. conf. on Mobile computing and networking*, pages 116–127. ACM, 2008.

[30] S. Camurati, G.and Poeplau, M. Muench, and A. Hayes, T.and Francillon. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In *ACM SIGSAC Conf. on Computer and Communications Security*, pages 163–177. ACM, 2018.

[31] A. Chaman, J. Wang, J. Sun, H. Hassanieh, and R. R. Choudhury. Ghostbuster: Detecting the Presence of Hidden Eavesdroppers. In *24th Int. Conf. on Mobile Computing and Networking (MobiCom)*, 2018.

[32] L. Huang, X. Wu, C. Zhao, and M. Gao. Identification of radio transmitters fingerprint based on curve fitting. In *IEEE Int. Conf. on Signal Processing, Communication and Computing (ICSPCC)*, 2013.

[33] D. Lee, W. Gyu La, and H. Kim. Drone Detection and Identification System using Artificial Intelligence. In *Int. Conf. on Information and Communication Technology Convergence (ICTC)*, October 2018.

[34] H. Li, G. Johnson, M. Jennings, and Y. Dong. Drone profiling through wireless fingerprinting. In *IEEE 7th Int. Conf. on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 858–863, July 2017.

[35] P. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu. Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication. In *15th Int. Conf. on Mobile Systems, Applications, and Services*. ACM, 2017.

[36] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, and T. Vu. Investigating cost-effective rf-based detection of drones. In *2nd Work. on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, pages 17–22. ACM, 2016.

[37] K. B. Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Int. Conf. on Security and Privacy in Communications Networks and the Workshops-SecureComm*. IEEE, 2007.

[38] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir. Fingerprinting Wi-Fi devices using software defined radios. In *9th ACM Conf. on Security & Privacy in Wireless and Mobile Networks*, pages 3–14. ACM, 2016.

[39] K. Wang, S. Chen, and A. Pan. Time and position spoofing with open source projects. *Black Hat Europe*, 148, 2015.

[40] C. Zhao, C. Chen, and Z. He, Z.and Wu. *Applied Sciences*, (12).

[41] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington. Drone Forensics: Challenges and New Insights. In *2018 9th IFIP Int. Conf. on New Technologies, Mobility and Security (NTMS)*, February 2018.

[42] G. Horsman. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, 16:1–11, March 2016.

[43] U. Jain, M. Rogers, and E. T. Matson. Drone forensic framework: Sensor and data identification and verification. In *IEEE Sensors Applications Symposium (SAS)*, pages 1–6, March 2017.

[44] J. Mead, C. Bobda, and T. Whitaker. In *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*.

[45] T. Reed, J. Geis, and S. Dietrich. Skynet: A 3g-enabled mobile attack drone and stealth botmaster. In *USENIX. Work. on Offensive Technologies*, pages 28–36, August 2011.

[46] R. Akeela and B. Dezfouli. Software-defined Radios: Architecture, State-of-the-art, and Challenges. *arXiv:1804.06564 [cs]*, April 2018. arXiv: 1804.06564.

[47] F. Le Roy, T. Quiniou, A. Mansour, R. Lababidi, and D. Le Jeune. RFID Eavesdropping Using SDR Platforms. In Alessandro De Gloria, editor, *Applications in Electronics Pervading Industry, Environment and Society*, LNEE, pages 208–214. SIP, 2018.

[48] A. Broumandan, R. Siddakatte, and G. Lachapelle. An approach to detect GNSS spoofing. *IEEE Aerospace and Electronic Systems Mag.*, 32(8):64–75, August 2017.

[49] A. Torabi, M.W. Shafer, G. S. Vega, and K. M. Rothfus. UAV-RT: an SDR based aerial platform for wildlife tracking. In *88th IEEE Vehicular Technology Conf., VTC , Chicago, 2018*.

[50] A. Moawad, K. Yao, A. Mansour, and R. Gautier. In *15th Int. Sympo. on Wireless Communication Systems, ISWCS, Lisbon, Portugal, 2018.*

[51] J. Gaspar, R. Ferreira, P. Sebastião, and N. Souto. Capture of uavs through gps spoofing. In *Global Wireless Summit (GWS)*, Nov 2018.