Spreading Code Identification of Legal Drones in IoT Environment

Khattab M. Ali Alheeti
Department of Computer Networking Systems, College of Computer Science and Information Technology, University Of Anbar - Iraq
co.khattab.alheeti@uoanbar.edu.iq

Muzhir Shaban Al-Ani
University of Human Development, College of Science and Technology, Department of Information Technology, Sulaymaniyah, Iraq
muzhir.al-ani@uhd.edu.iq

Klaus McDonald-Maier
School of Computer Sciences and Electronic Engineering
University of Essex
Colchester, United Kingdom
kdm@essex.ac.uk

***Abstract*— The widespread use of drones has become very common today with large-scale civil and military applications. In the next few coming years, the outlook is expected that the number of drones will reach millions. So, these need to be well organised and managed in order to achieve the benefits of IoT with this accelerated environment. Drones or Unmanned Aerial Vehicles (UAVs) must achieved a level of communications to authenticate a legal working. The proposed approach concentrated on preparing each drone with identification key based on the combination of its international sim number with the date of the first action and the local country code. This approach is called Drone IDentification (DID) that generate a unique code for each drone via spreading technique. In this case any drone not apply this regulation is considered as unauthenticated drone and does not allowed to fly. This approach is very important to establish drone regulation via IoT.**

Keywords*— *Drones, wireless vehicles, UAV, driverless vehicles, IoT Environment.

I. INTRODUCTION

More than a century ago, the world of communications began to play an important role in various areas of life and began to facilitate many things in commerce, business and human life [1,2,3]. Then the world of communications took great strides in moving from the traditional communications to the modern digital communications [4,5,6]. Then wired communications turned into wireless communications [7,8]. Then there were many techniques and technologies for the wireless communications such as Bluetooth, WiFi, WiMax wireless networks, satellite and cellular mobile communications [9,10].

Drones also called Unmanned Aerial Vehicles (UAVs), drones are started with about 100 years ago as remote controlling of moving vehicles [11,12]. Historical records indicated that drones have been used mainly in the military exactly deployed in enemy territory to reduce the accident of pilot losses [13,14]. Recently due to the continuous reduction of costs (hundreds of dollars) and minimum size reduction (few centimeters), the small unmanned aerial vehicles are now more easily accessible to the public and governments [15,16]. So many new applications have appeared in the civil and commercial fields such as detection of fires, traffic control, transport packages, emergency service, aerial photography, prisons detection, criminal tracking, dangerous detection, communications and control … etc [17,18].

Object detection and identification is an important part in the huge worldwide [19,20]. Recently, Internet of Things (IoT) become an important issue and in the near future there will be millions of objects are connected to this environment including drones [21,22].

Recently, drones become an important tool that can cover wide range of civil and military applications. The proposed approach concentrated on introduce an drone identification system of legal drones in IoT Environment. This approach based on using spreading code in order to generate the unique drone identification.

II. DRONES

The drone operates remotely, ranging in size from a small object of centimeter such as an insect (civil purposes) to a plane with its wings of about 100 meters (military purposes) [23,24]. These unmanned aerial vehicles (UAVs) operate on air, in addition to the presence of many drones operating on land and water [25,26]. Drones can fly from several meters to hundreds of kilometers [27,28]. Two types of radio frequencies 2.4 GHz and 5.8 GHz are used for the communications between ground transmitter and the drones [29,30]. Drones including ground-based controller and a communications system between them [31,32]. The main challenges in the communications of drones are concentrated on coverage area, radio interference and mobility optimization [33,34].

In general drones can be classified into two categories; fixed wing and rotary wing as shown in figure 1 [35,36,37].

A. Fixed Wing Characteristics:

- Raising or lifting of the vehicle based on the wings with the fly speed forward.
- Using simpler structure that achieve higher payload and higher speed.
- It needs to keep moving forward and runway for take-off and landing.

B. Rotary Wing Characteristics:

- Raising or lifting of the vehicle based on the blades revolving around a rotary column.
- Its structure leading to lower payload, lower speed, shorter rang.
- Have the ability to move in any direction, in addition it achieve vertical take-off and landing.

978-1-7281-5546-3/19/$31.00 ©2019 IEEE

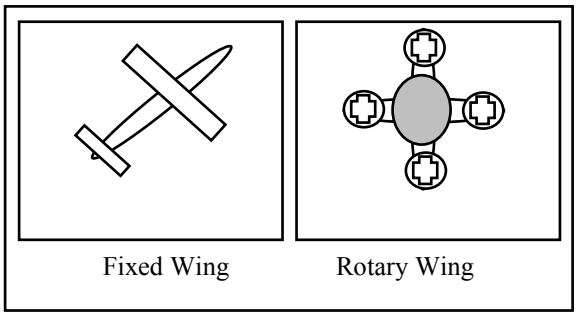

Fig. 1. Types of drones

There are seven types of drones according to their targets:

- Target drones: This type of drones used to give a practice target [38,39].
- Reconnaissance drones: This type of drones used for collection of information including military information [40,41].
- Combat drones: This type of drones can carry out fighting missions [42,43].
- Logistics drones: This type of drones used to carry out the cargos [44,45].
- Research and development drones: This type of drones used to make improvements on the current drones [46,47].
- Civil drones: This type of drones used for civil applications [48].
- Commercial drones: This type of drones used for Commercial applications [49].

III. Related Works

Unmanned aerial vehicles or drones play an important part in the recent applications. This section is concentrated on the recent works related to this field.

Rachel L. Finn et al. (2012) explained how the use of drones for surveillance in civil applications has an impact on privacy and other civil liberties. This work indicated that despite the heterogeneity of these systems, the poor, people of color and anti-government protesters are targeted by drone deployments. This work explained how current privacy legislation in the United States, the United Kingdom and the European Union could apply to drones' systems. They denoted that current regulatory mechanisms do not adequately concerns with privacy and civil liberties because drones are complex multimodal surveillance systems that integrate a range of technologies and capabilities. The work advocated the combination of legislative requirements and impact assessments to adequately address privacy and civil liberties [50].

Dimitrios Zorbas et al. (2013) concentrated on the problem of energy efficiency where flying drones equipped with cameras can detect and track mobile events that occurs in the field. They provided a mathematical model of minimizing the total energy consumption of a drone fleet when coverage of all events is needed. The optimal solution cannot be obtained for the extremely high complexity of the binary optimization problem including in small cases. Instead, they presented a localized solution to the aforementioned problem that takes into account the ability of drones to fly at lower altitudes to conserve energy. They simulated and compared their performance with a centralized algorithm and an approach that uses static drones to cover the entire terrain. The obtained results show that localized solution in a similar way to the centralized algorithm exceeded the static approach by 150% in terms of energy consumed [51].

Uri Volovelsky (2014) proposed the assumption that the entry of drones into the civil market is a certainty, what are the possible implications for the fundamental right to privacy, and the question of civil use permits for drones indicate that the laws of privacy now irrelevant? Five issues are addressed in this article. The first issue is a fundamental right and the right to privacy is unclear. The second issue is to achieve a balance between the benefits of the civilian use of drones and possible infractions of the right to privacy and other fundamental rights. The third issue is the possibility of restricting the use of drones, either for data collection or for use of data. The fourth issue concerned with the choice of law as a basis for examining whether the law can provide appropriate tools to address the risks associated with the use of drones. The fifth issue related to the element of uncertainty [52].

Chase C. Murray (2015) explained that drones are now ready to be widely adopted in the commercial applications. One of these applications is to use these drones for the delivery of the last mile in logistics operations. While significant research efforts are being made to improve the technology required to enable the delivery of drones, less attention has been given to the operational challenges associated with the use of this technology. This article proposed two models to optimize the routing and programming of drones in this new environment of package delivery. In particular, this approach introduced the vehicle routing, motivated by a scenario in which the drone works with a traditional delivery truck to dispatch packages. This approach presented the model of mixed linear programming for two problems of delivery of drones, as well as two simple but effective heuristic approaches to solve problems of practical size. The obtained solutions will facilitate the adoption of drones for the last mile delivery. This allows a faster reception of customer orders at a lower cost to the distributor and with a reduced environmental impact [53].

Dimitrios Zorbas et al. (2016) explained the static targets on the ground using flying drones is a common task for civil and military applications. They presented the location of drones at a minimum cost and their solutions for this task in a two-dimensional field. In this approach two parameters as number of drones and the energy consumption are considered. They assumed that each drone has a minimum and maximum observation altitude. In addition, the energy consumption of the drone is related to this altitude. It is clear that the higher drone altitude, the greater observed area, but the greater of energy consumption. The main goal of this approach is to find drone locations that minimize costs while monitoring all targets. The problem is solved mathematically by defining linear and nonlinear integers for optimized models. This approach introduced centralized and localized heuristics to approximate the solution for static and mobile objectives [54].

Quan Yuan et al. (2017) demonstrated an approach for multi-drone system with a decentralized model predictive control. The drones collect localized information from the neighbors and update their speeds using this approach. In the multi-drone system, the data packets are transmitted by wireless modules in transmission mode, giving such an anonymous and decentralized system where all calculations and controls are carried out in a mini-computer on board each drone. Each drone is a double layer agent system with the coordination layer executing multiple drone float algorithms and the flight control layer navigating in the drone. The final formation of the batch rests both in the range of communication and the distance between the drones desired. This approach performed numerical simulations and field tests with a herd of five drones, which shows that this system works well in the multi-drone system presented with convergence speed and tracking ability of a desired path [55].

Yujie Li et al. (2018) explained that drones technologies have developed rapidly and that are used in many industrial fields such as photography, delivery and agriculture. It is clear that a commercial drone can only fly more than 20 minutes on a single charge and cannot fly in certain areas and cannot fly on bad weather. The most important issues of drone's technologies are reduced energy consumption and travel long distances. This approach proposed a new amphibious air-ground drones that can fly and requires less energy consumption that extends the range of mobility of the drone. The terrestrial mode can be used to cross restricted areas or adverse climatic conditions by sliding. Then they developed an algorithm based on the Convolutional Neural Network (CNN) to detect the route in a captured scene. The proposed approach based on space pyramid pooling blocks to reach accurate segment. The obtained results indicated that the accuracy improvement of the pixel is 85.6% [56].

IV. Statement of the Problem

Next near few yeas showing the huge applications of drones. In the huge environment of IoT existing illegal use of flying drones that cause serious and dangerous problems even though they are using small drones. Millions of devices and sensors are connected to IoT environment for transferring of data including flying drones. The expectation said that there is a big growth of flying drones in the next few years. The proposed solution of the problem is to establish an identification approach depends on the combination both international sim number and the date of establishment with the country code. This approach leading to offer a secure identification drone within IoT environment that avoiding any illegal drone from flying.

V. Methodology

The problem of big drone authentication was solved because most of these drones are concerned to government of licensed companies. So these partners are responsible for the security of their drones. The problem arises and becomes a serious problem with the revolution of using small drones by amateur people for private services.

A. Countries Code

Countries code depends on the list of abbreviations and codes generated by the United Nations (UN). These codes are used as an international standard code to identify nations and these codes are in between 0 to 900 as shown in figure 2. These codes will be used as a primary field of the identification key.

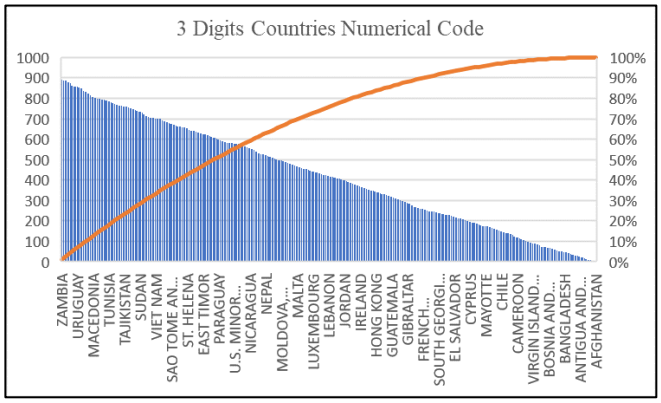

Fig. 2. UN 3 digits countries numerical code.

B. Identification System Design

The authentication system design based on many issues including drone type, country code and drone serial number with the issued date. This approach is called DID. The authentication procedure is stated with the following steps:

- Enter serial number, this includes reading the drone serial number.
- Enter code country, this includes reading the code country by the owner of the drone.
- Generate security code, this includes combining both serial number and biometric data with the issued date.
- Pass the security code, this includes passing the security code from the user device to the drone.
- Validate the security code, this includes reading the generated security code to validate it.
- Check authentication, this includes authenticate the security code for both drone and server provider.
- Check document validation, this includes the validation of document to be transfer.
- Read data, this includes reading the validated document.

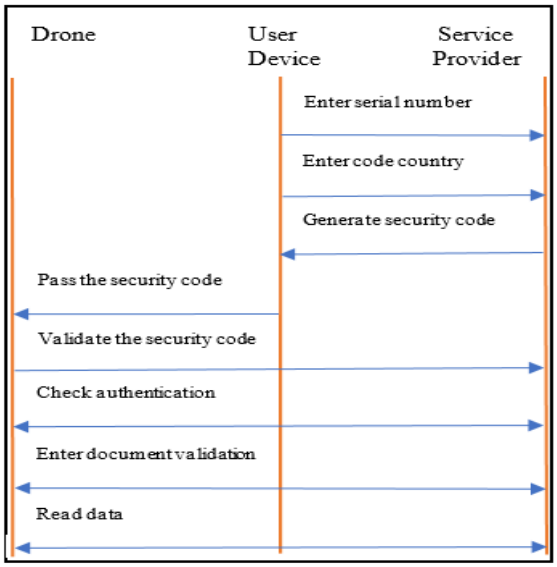

Fig. 3. DID approach.

C. *Generating of Security Code*

Driverless vehicles are started in 2009 as real project and these vehicles may extended to be one of the big issues in the near future. If any accident happen for these vehicles may cause some human and material losses. On the other hand, any accident or illegal uses of drones may cause big losses of human and material. To avoid serious accidents between drones there are simple important regulations must be considered such as (figure 4); check the drone, avoid strong winds, avoid bad weather, avoid crowded areas, avoid flying over people and keep drone in sight.

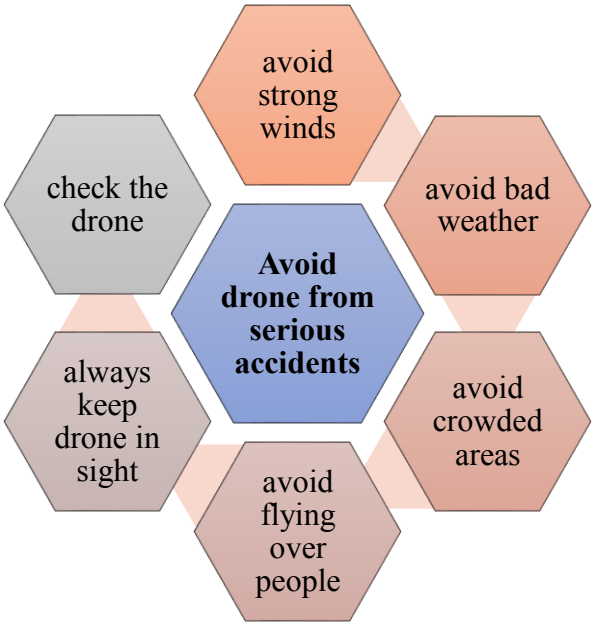

Fig. 4. avoid drones from serious accidents.

For the above reasons, it is important to generate a security code to identify each drone. The security code depends on three main factors: drone serial number, country code and issued date. These three factors are combined in a certain way to generate the authenticated drone code as shown in figure 5.

- **First**: combining drone serial number with the issued date of the drone to generate the spreading code. Drone serial number is represented by 14 bits and the issued date of the drone is also represented by14 bits. The combination of these two codes are done via AND gate, so the output of this process represents the spreading code of 14 codes.
- **Second**: combining the spreading code with the local country code to generate the channel code. The spreading code is represented by 14 bits and the local country code is represented by 8 bits. The combination of these two codes are done via EX-OR gate, so the output of this process represents the channel code of 112 code.
- **Third**: combining all channels together to generate the composite waveform. The composite waveform is transmitted via the carrying media to reach its destination.

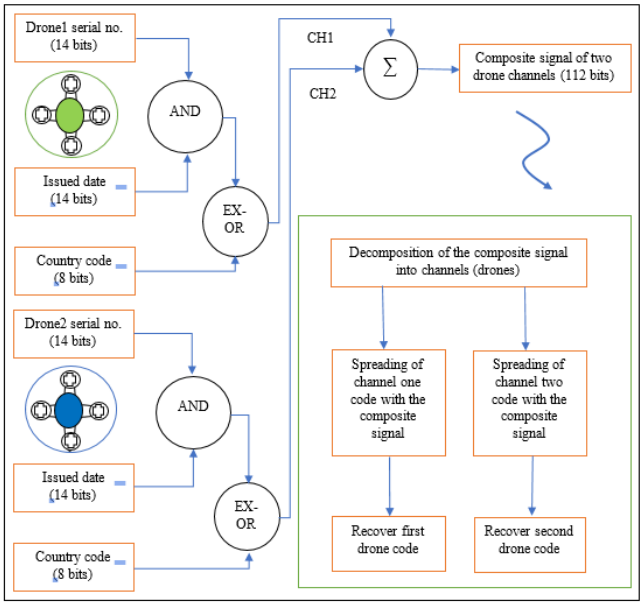

Fig. 5. structure secure code generation.

VI. Results and Discussions

To understand the procedure of this approach, it is better to illustrate a simple direct example that represents the final code generation. Two drones are used to examine this scenario. The first drone is represented by 14 bits (01010101010101), this number is ANDed with the issued date 30/7/18, which is represented by 14 bits (11110 0111 10010). The output of this process is also 14 bits (01010001010000). This output code is used as the spreading code for the next step. This spreading code is distributed over the 8 bits country code. According the alphabetic UN country code, there are 248 countries and territories listed from 1 to 248, so it is better to use 8 bits representation to cover these countries and territories. Iraq is selected as a local country, which have the number 106 that means (01101010). In the next step, EX-OR is applied between the spreading code of 14 bits that become 112 bits after spreading with the country code. As it is clear the output of EX-OR generates '1' for different inputs and generates '0' for similar inputs. The output of the EX-OR represents the unique code of the first drone or first channel (CH1). Then the last step deals with creating the waveforms. This step is started by representing 0 bit by +1 volt and representing 1 bit by -1 volt, so the first drone (CH1) waveform is shown in figure 6 and the overall channel sequence waveform is shown in figure 7.

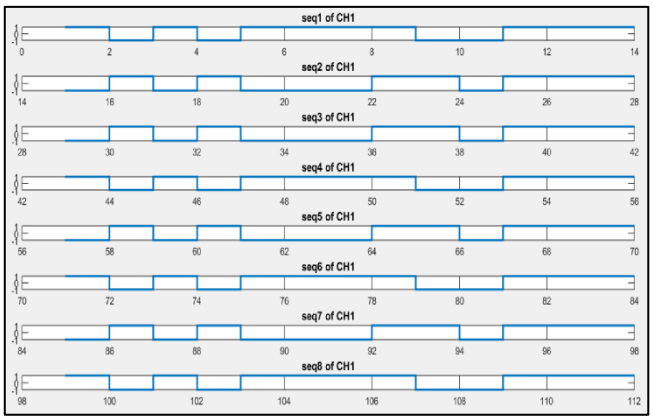

Fig. 6. waves of drone1 (CH1).

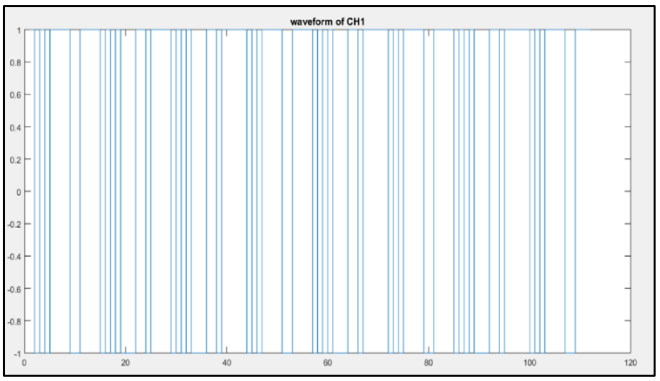

Fig. 7. complete waveform of CH1.

To achieve the sensitivity of this approach, CH2 is represented the information of second drone. In this case all parameters of this channel are the same excluding the drone code number. The second drone is represented by 14 bits (00110011001100), this number is ANDed with the same issued date 30/7/18, which is represented by 14 bits (11110 0111 10010). The output of this process is also 14 bits (00110011000000). This output code is used as the spreading code for the next step. Then Iraq is selected as a local country, which have the number 106 that means (01101010). In the next step, EX-OR is applied between the spreading code of 14 bits that become 112 bits after spreading with the country code. The output of the EX-OR represents the unique code of the second drone or second channel (CH2). Then the last step deals with creating the waveforms in which the second drone (CH2) waveform is shown in figure 8 and the overall channel sequence waveform is shown in figure 9.

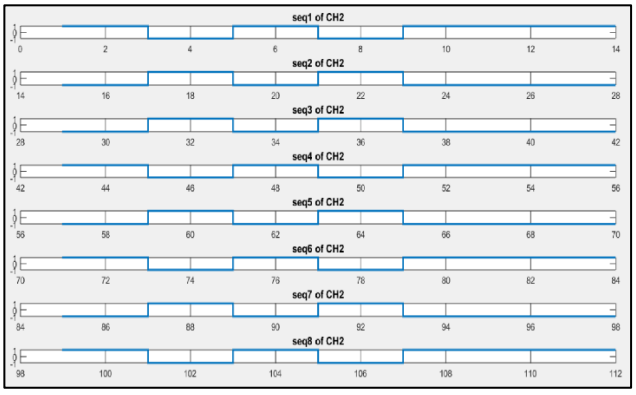

Fig. 8. waves of drone2 (CH2).

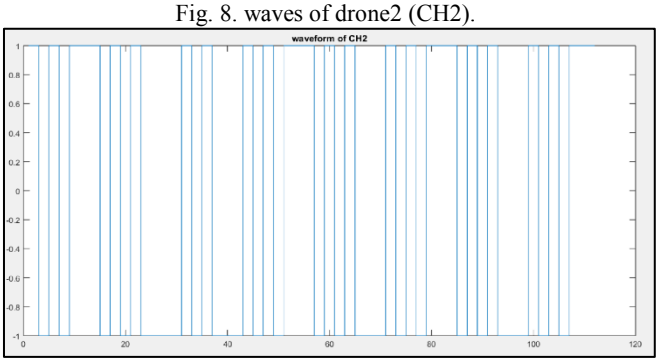

Fig. 9. complete waveform of CH2.

The last step of this procedure is concerned when all of these drones using the same frequency at the same time then the resulting waveform would actually be the adding all waveforms of channels to form the composite waveform in which all users (drones) waveforms are included as shown in figure 10. So, every user is included in this composite waveform. On the other hand, this means every receiver is going a receive this composite waveform. At the receiving end of drone1, the spreading code waveform of drone1 is multiplied by the composite waveform to get new waveform in which it is averaging to get the code value of bit. Finally, we can get the corresponding identification of each drone.

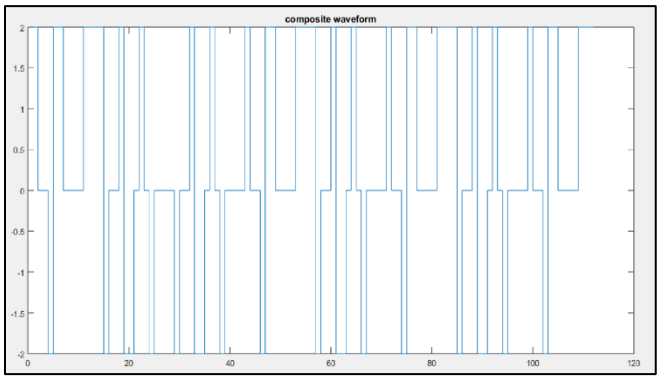

Fig. 10. composite waveform.

VII. Conclusions

Now a day drones play an important part in civil and military applications including in the huge devices and sensors via IoT environment. Next few years will show millions of flying objects (drones) circulating in the free space. A brief study of drone is explained in this work and that realize both identification and communications are very important part in the next huge environment of IoT. The proposed approach based on merging many parameters such as drone serial number, issued date and country cone. This approach adapted the spreading technique to generate an identification code for each drone. This approach is secure, simple, easy to adapt and can be applied for all types of drones. In addition, this approach is very important in the huge number of flying objects in IoT environment.

References

[1] Ali Grami (2016) Chapter 11: Communication Networks, Introduction to Digital Communications, 2016, Pages 457-491.

[2] Liang Liu, Jie Xu, Rui Zhang (2018) Chapter 10: Transmit beamforming for simultaneous wireless information and power transfer, Academic Press Library in Signal Processing, Volume 7, 2018, Pages 479-506.

[3] Jennifer Ann Kurtz (2017) Chapter 1: Wireless Technology Overview, Hacking Wireless Access Points, 2017, Pages 1-19.

[4] Muhammad R. A. Khandaker, Kai-Kit Wong (2018) Chapter 8: Signal processing for massive MIMO communications, Academic Press Library in Signal Processing, Volume 7, 2018, Pages 367-401.

[5] A. Belghith, M. S. Obaidat (2016) Chapter 2: Wireless sensor networks applications to smart homes and cities, Smart Cities and Homes, 2016.

[6] I. A. Glover, R. Atkinson (2017) Chapter 1: Overview of wireless techniques, Wireless MEMS Networks and Applications, 2017, P 1-33.

[7] Tao Jiang, Da Chen, Chunxing Ni, Daiming Qu (2018) Chapter 10: Applications, OQAM/FBMC for Future Wireless Communications.

[8] S. Ahmadi (2016) Chapter 15: Wireless broadband standards and technologies, Academic Press Library in Mobile and Wireless Communications, 2016, Pages 559-619.

[9] Jacob Murray, Paul Wettin, Partha Pratim Pande, Behrooz Shirazi (2016) Chapter 4: Wireless Small-World NoCs, Sustainable Wireless Network-on-Chip Architectures, 2016, Pages 37-45.

[10] Khattab M. Ali Alheeti, Muzhir Shaban Al-Ani, Klaus McDonald-Maier (2018) A hierarchical detection method in external communication for self-driving vehicles based on TDMA, PLoS ONE 13(1): e0188760, January 9, 2018.

[11] Anand Paul, Naveen Chilamkurti, Alfred Daniel, Seungmin Rho (2017) Chapter 1: Introduction: intelligent vehicular communications, Intelligent Vehicular Networks and Communications, 2017, P 1-20.

[12] Anand Paul, Naveen Chilamkurti, Alfred Daniel, Seungmin Rho (2017) Chapter 4: Evaluation of vehicular network models, Intelligent Vehicular Networks and Communications, 2017, Pages 77-112.

[13] Anand Paul, Naveen Chilamkurti, Alfred Daniel, Seungmin Rho (2017) Chapter 3: Vehicular network (VN) model, Intelligent Vehicular Networks and Communications, 2017, Pages 43-75.

[14] Pedro Castillo-García, Laura Elena Muñoz Hernandez, Pedro García Gil (2017) Chapter 5: Data Fusion for UAV Localization, Indoor Navigation Strategies for Aerial Autonomous Systems, 2017.

[15] W. W. Huebsch, S. D. Hamburg, R. W. Guiler (2012) Chapter 3: Aircraft morphing technologies, Innovation in Aeronautics, 2012.

[16] [16] Steve Van Till (2018) Chapter 10: IoT Technology and Standards, The Five Technological Forces Disrupting Security, 2018, P 107-125.

[17] [17] Harsh Kupwade Patil, Thomas M. Chen (2017) Chapter 18: Wireless Sensor Network Security: The Internet of Things, Computer and Information Security Handbook (Third Edition), 2017, P 317-337.

[18] Muzhir Shaban Al-Ani, and Khattab M. Ali Alheeti (2018) Intelligent Internet of Things for Energy Conservation Based on Routing Protocol, 2017 IEEE, 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), – Iraq.

[19] Muzhir Shaban Al-Ani and Qeethara Al-Shayea (2016) Speaker Identification: A Novel Fusion Samples Approach", International Journal of Computer Science and Information Security (IJCSIS), Volume 14, No. 7, July 2016, pp. 423-427, USA.

[20] Feras E. AbuAladas, Akram M. Zeki, Az-Eddine Messikh, Muzhir Shaban Al-Ani (2017) Speaker Identification Based on Curvlet Transform Technique, 2017 International Conference on Computing, Engineering, and Design (ICCED), Kuala Lumpur, Malaysia.

[21] Muzhir Shaban Al-Ani, Zana Azeez Kakarash (2018) Future Aspects of Intelligent Car Parking Based on Internet of Things, UHD journal of science and technology, May 2018 | Vol 2 | Issue 1.

[22] Muzhir Shaban Al-Ani (2017) Flying with Internet of Things via Global Structure", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 12, Issue 3 V IV 2017), P 36-42.

[23] Chu-Chu Li, Jia-Ning Wu, Yun-Qiang Yang, Ren-Gao Zhu, Shao-Ze Yan (2016) Drag reduction effects facilitated by microridges inside the mouthparts of honeybee workers and drones, Journal of Theoretical Biology, Volume 389, 21 January 2016, Pages 1-10.

[24] Austin Choi-Fitzpatrick, Tautvydas Juskauskas (2015) Up in the Air: Applying the Jacobs Crowd Formula to Drone Imagery, Procedia Engineering, Volume 107, 2015, Pages 273-281.

[25] Alessandra Capolupo, Stefania Pindozzi, Collins Okello, Nunzio Fiorentino, Lorenzo Boccia (2015) Photogrammetry for environmental monitoring: The use of drones and hydrological models for detection of soil contaminated by copper, Science of The Total Environment, Volume 514, 1 May 2015, Pages 298-306.

[26] Mitchel Pappot, Robert J. de Boer (2015) The Integration of Drones in Today's Society, Procedia Engineering, Volume 128, 2015, P 54-63.

[27] Roger Clarke (2014) Understanding the drone epidemic, Computer Law & Security Review, Volume 30, Issue 3, June 2014, P 230-246.

[28] Roger Clarke, Lyria Bennett Moses (2014) The regulation of civilian drones' impacts on public safety, Computer Law & Security Review, Volume 30, Issue 3, June 2014, Pages 263-285.

[29] Wayne Chappelle, Tanya Goodman, Laura Reardon, William Thompson (2014) An analysis of post-traumatic stress symptoms in United States Air Force drone operators, Journal of Anxiety Disorders, Volume 28, Issue 5, June 2014, Pages 480-487.

[30] Michael Brooks (2012) Welcome to the personal drone revolution, New Scientist, Volume 216, Issue 2894, 8 December 2012, P 42-45

[31] U. Niethammer, M. R. James, S. Rothmund, J. Travelletti, M. Joswig (2012) UAV-based remote sensing of the Super-Sauze landslide: Evaluation and results, Engineering Geology, Volume 128, 92012.

[32] Pietro Peliti, Lorenzo Rosa, Giuseppe Oriolo, Marilena Vendittelli (2012) Vision-Based Loitering Over a Target for a Fixed-Wing UAV, IFAC Proceedings Volumes, Volume 45, Issue 22, 2012, Pages 51-57.

[33] Jian Zhang, Jianbo Hu, Juyu Lian, Zongji Fan, Wanhui Ye (2016) Seeing the forest from drones: Testing the potential of lightweight drones as a tool for long-term forest monitoring, Biological Conservation, Volume 198, June 2016, Pages 60-69.

[34] Rocci Luppicini, Arthur So (2016) A technoethical review of commercial drone use in the context of governance, ethics, and privacy, Technology in Society, Volume 46, August 2016, Pages 109-119.

[35] Frank Thornton (2008) Chapter 8: Kismet Drones, Kismet Hacking, 2008, Pages 187-222.

[36] E. L. Houghton, P. W. Carpenter, Steven H. Collicott, Daniel T. Valentine (2017) Chapter 7: Wing Theory, Aerodynamics for Engineering Students (Seventh Edition), 2017, Pages 449-523.

[37] Matthew L. Wilbur, Mihir P. Mistry, Peter F. Lorber, Robert Blackwell, Uwe T. P. Arnold (2018) Chapter 24: Rotary Wings Morphing Technologies: State of the Art and Perspectives, Morphing Wing Technologies, 2018, Pages 759-797.

[38] Jean-Aimé Maxa, Mohamed Slim Ben Mahmoud, Nicolas Larrieu (2018) Chapter 3: Application to Communications in a Drone Fleet, Model-driven Development for Embedded Software, 2018, P 43-151.

[39] Zahra kavoosi, Mohammad Hossein Raoufat, Maryam Dehghani, Jafari Abdolabbas, Mohammad Jafar Nazemossadat (2018) Feasibility of satellite and drone images for monitoring soil residue cover, Journal of the Saudi Society of Agricultural Sciences, In press, corrected proof, Available online 28 June 2018.

[40] Cameron H. Malin, Terry Gudaitis, Thomas J. Holt, Max Kilger (2017) Chapter 10: Looking Forward: Deception in the Future, Deception in the Digital Age, 2017, Pages 241-253.

[41] Adrián Arenal Pereira, Jordán Pascual Espada, Rubén González Crespo, Sergio Ríos Aguilar (2018) Platform for controlling and getting data from network connected drones in indoor environments, Future Generation Computer Systems, In press, corrected proof, 2018.

[42] I. Hamerton, L. Mooring (2012) Chapter 7: The use of thermosets in aerospace applications, Thermosets, 2012, Pages 189-227.

[43] Junwon Seo, Luis Duque, Jim Wacker (2018) Drone-enabled bridge inspection methodology and application, Automation in Construction, Volume 94, October 2018, Pages 112-126.

[44] Boualem Rabta, Christian Wankmüller, Gerald Reiner (2018) A drone fleet model for last-mile distribution in disaster relief operations, International Journal of Disaster Risk Reduction, Volume 28, 2018.

[45] Yunus Karaca, Mustafa Cicek, Ozgur Tatli, Aynur Sahin, Suleyman Turedi (2018) The potential use of unmanned aircraft systems (drones) in mountain search and rescue operations, The American Journal of Emergency Medicine, Volume 36, Issue 4, April 2018, Pages 583-588.

[46] Alfredo Roma (2017) Drones and popularisation of space, 2017.

[47] Oliver Kearns (2017) Secrecy and absence in the residue of covert drone strikes, Political Geography, Volume 57, March 2017, P 13-23.

[48] A. Claesson, L. Svensson, P. Nordberg, M. Ringh, J. Hollenberg (2017) Drones may be used to save lives in out of hospital cardiac arrest due to drowning, Resuscitation, Volume 114, May 2017, Pages 152-156.

[49] Janine Teubner, Ingmar Kruse, Hans Scheuerpflug, Claudia Buerhop-Lutz, Christoph J. Brabec (2017) Comparison of Drone-based IR-imaging with Module Resolved Monitoring Power Data, Energy Procedia, Volume 124, September 2017, Pages 560-566.

[50] Rachel L. Finn, David Wright (2012) Unmanned aircraft systems: Surveillance, ethics and privacy in civil application, Computer Law & Security Review, Volume 28, Issue 2, April 2012, Pages 184-194.

[51] Dimitrios Zorbas, Tahiry Razafindralambo, Di Puglia Pugliese Luigi, Francesca Guerriero (2013) Energy Efficient Mobile Target Tracking Using Flying Drones, Procedia Computer Science, Volume 19, 2013.

[52] Uri Volovelsky (2014) Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study, Computer Law & Security Review, Volume 30, Issue 3, June 2014, Pages 306-320.

[53] Chase C. Murray, Amanda G. Chu (2015) The flying sidekick traveling salesman problem: Optimization of drone-assisted parcel delivery, Transportation Research Part C: Emerging Technologies, 2015.

[54] Dimitrios Zorbas, Luigi Di Puglia Pugliese, Tahiry Razafindralambo, Francesca Guerriero (2016) Optimal drone placement and cost-efficient target coverage, Journal of Network and Computer Applications, Volume 75, November 2016, Pages 16-31.

[55] Quan Yuan, Jingyuan Zhan, Xiang Li (2017) Outdoor flocking of quadcopter drones with decentralized model predictive control, ISA Transactions, Volume 71, Part 1, November 2017, Pages 84-92.

[56] Yujie Li, Huimin Lu, Yoshiki Nakayama, Hyoungseop Kim, Seiichi Serikawa (2018) Automatic road detection system for an air–land amphibious car drone, Future Generation Computer Systems, Volume 85, August 2018, Pages 51-59.