International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Security of Drone Hacking with Raspberry-Pi using Internet-of-Things

Pratheepa Marimuthu, Saran Kumar Sekar

Abstract: ***Internet-of-Things (IoT) implementation in technological application is developing at higher speed because of more demand from the customers and firms which reply with the advantages proposed through the brilliant and elegant hardware unit. Using Drone concept, it is finding more applications in various areas which rises the threat of data hacking and also poses safety risk to common people. We must appreciate due to online data collection from the application of commercial drones which is widespread across varieties of drone use. Implementation of IoT enabled drones in large quantity causes more number of drones which is exposed to the possibility of being attacked or harmed by the fraudster. This research work examine the various issues concerned to drone security, safety, threat, attacks and illustrate a group of wireless fidelity risk possibilities. My research work has observed different types of threat and attacks on commercial drones. The propagation channel risk analyzed are, Access Denial, Authorization techniques, unauthorized third party presence, illegal source access gain and frame misuse of device characteristic features. Our work prohibits illegal connection entry controlled based on Raspberry-pi & wireless fidelity between access point and drone happens using tell-net with the help on IP address and sign up process. The investigation work explains the execution of methodology which includes attack steps and data security enabling using RSA Algorithm. The main work focuses on the data collected on parrot security OS and to secure the communication in Wi-Fi mode using drone and another devices were analyzed.***

Keywords: **Cryptography, Networking, IoT, Cloud**

I. INTRODUCTION

The Internet connection architecture is consist of operating of drone in an aim to provide a specific viewpoint to collect information. In recent days drones are interconnected with number of sensors, automatic and independently linked to through the wireless fidelity to the internetworking, which enables a unique approach for communicating via air. These drones have the ability to collect useful information which is then studied, useful to offer some advantage to the large business organizations [1].

The developments in intelligent devices has introduced various prospects for drone application. There are plenty of drones software apps solely meant for controlling drones that is available from app stores. These apps can be downloaded and installed to our mobile device which enable the drone owner to operate the drones with many features such as switching light to turn high and low, buzzer on and off, motors movements, video and image clicking, steering the drone and many more drone feature that can be controlled using these apps. The drones is enable to be communicated with smart devices using connection of raspberry-pi and Wi-Fi that is controlled via a portable device with sovereignty. Drones are mainly categorizes into entertaining, business purposes and army drones [2]. The main feature provided by the drones is to compute real time data, axial orientation, movement and stabilization in any condition. The drone real time data can also be shared, interfaced and networked with the cloud database. The basic key real time drone risks factors are:

a) To take control of a drone by force
b) Confidentiality
c) Cyber-Security
d) Accidental harm
e) Chains of supply

The projected growth in the demand for drone applications in the various field rises the verities of threats and security risk concern. Drone security area is a unique innovative idea and gradually wide spreading for publics. Drones using IoT system are very much susceptible in many ways. Drones are more vulnerable to internet The main objective of this paper is to observe how the vulnerabilities caused to drone and its communication can be secured using automated Raspberry-pi and Wi-Fi. The scope, application, approach and outcomes are discussed to analyze the significance of cryptography and other important issues on the drones [3]. An example of flying Drone using Raspberry-pi and Wi-Fi is shown in figure 1.

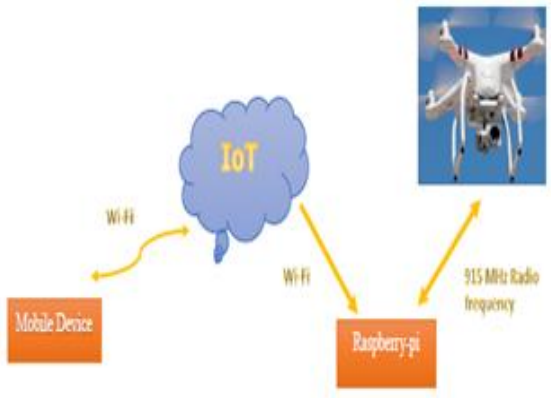

Fig. 1. Flying Drone using Raspberry-Pi and Wi-Fi

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Pratheepa Marimuthu*, M. Tech in CSE from Prist University and MCA from Bharathidasan University, India, PH: +91 8870227422, E-mail: pratheepa.mtech@gmail.com
Saran Kumar Sekar, M.E. in Aeronautical Engineering, Lecturer-Department of Aeronautics, St. Theresa International College, Nakhhonnayok - Thailand, PH: +66928703020, Email: sarankumar@stic.ac.th

II. LITERATURE REVIEWS

The literature review surveys the methods used in unauthorized access to the system recourses.

- **Sign-up Oriented attack Observation [4]:**

This technique notices the wrong sequences of sign up for the purpose of illegal access to system saved in the IoT storage cloud. If there is attack based on same signup, then an alarm event is triggered. This method of attack is useful for soon recognizing the trained attacks and it is complex to detect fresh attacks or the risks for signup will not be available in the database as well new known risk are varying signatures attacks are not noticeable.

- **Attack based on Abnormal Learning [5]:**

It observes attacks which is not known and it depends on device learning techniques to form a prototype of confidential channel activity of traffic and then equates abnormal setup actions compared to this prototype. The device training methods and arithmetical techniques implemented for identical procedures are substantial to be right for implementing on small dimensions nodes. Such process depends over the quantity of frames exchanged among the various nodes, when frame sharing rate is more in contrast to an average activity which action is to activate alarm.

- **Machine Learning Oriented Attacks [6]:**

The usefulness of machine learning methods in scam observation, picture identification and script arrangement which leaves good impression on attack investigators to implements such procedures for abnormal activity to improve the risk factors in IoT setups. Machine Learning procedures are more effective for information handling and administrator using IoT.

- **Deep Learning Oriented Attacks [7]:**

IoT upkeep various set up rules layers which handles different risk factors. Deep learning process is more effective because it supports extremely good features removal proficiency in deep learning to observe some attacks.

III. TECHNOLOGY DETAILS

A. Drone-Q Series

Drone Q Series is small distance Unmanned Aerial Vehicle (UAV) which is ideally suited for calculating 3-D locations of points and the space and point of view among them, recording, safety, scrutiny, Traffic control, public control and tragedy assistance. Drone Q Series UAV is shown in figure 2.

Fig. 2. Drone Q Series UAV

B. Drone-Q Series Technical Specification

Drone Q Series Unmanned Aerial Vehicle technical specifications is listed below:

- Twenty five to forty minutes at MSL of endurance.
- Two to four km line of sight bounds.
- Approximately three and half kg of weight.
- Up-to thirty km per hour of wind resistance
- Three thousand meter AMSL which is the upper limit of altitude launch.
- One meter into one meter drone structure dimension.
- 10x Optical Zoom and 1280 x 720 dots of daylight payload.
- 640 x 480 pixels of thermal payload as shown in figure 3.

Fig. 3. Drone Q Series UAV Payload

C. Wi-Fi Pineapple

Wi-Fi Pineapple as shown in figure 4 is embedded with the following features:

- Two to Five Giga hertz dual band.
- Approximately five hundred Mega Hertz System on Chip.
- 4 tall distance Trans-receiver up to eight hundred micro watts/radio.
- Serial USB, USB Ethernet, Ethernet Ports & Host USB.
- DC power via USB.

Figure 4: Wi-Fi Pineapple Tetra [24]

D. Raspberry-Pi 3 Board

The Raspberry-Pi implemented in board as shown in figure 5.

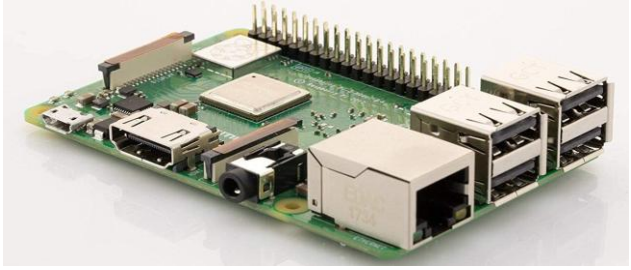

Fig. 5. Raspberry-Pi 3 board [16]

- It contains the following features,
- One point four Giga Hertz sixty four bit quad-core AARM version eight center processing unit and one Giga Byte RAM.
- Wireless LAN 802.11n, Ten to a hundred megabits per second LAN processing rate.
- Four USB Ports, Forty GPIO Pins, Camera Interface, Three Dimension graphics core.

E. Methodology

The following process shown in figure 6 demonstrate the steps starting from methods of hacker initiates and enters gradually into the entire network coverage area to its vulnerable network distance via a Drone, which enables malicious texts and programs over the aimed points and make attempts to seize Wi-Fi, hence penetrate into propagation area to achieve next harmful activity. The hacker uses a Linux oriented Wi-Fi attack tool 'parrot' on the laptop using raspberry-Pi. The attacker can penetrate into the network and it phishing page is shown to all the connections on the network, which intern inhibit the user for re-joining to the main access point.

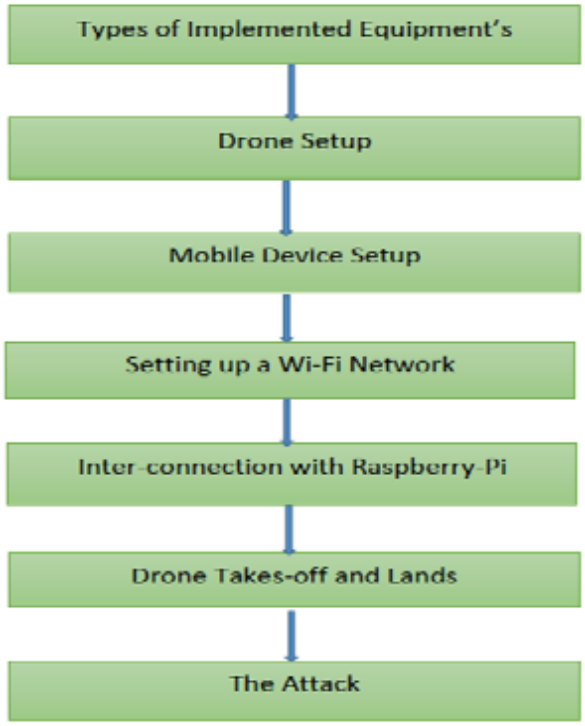

Fig. 6. Research Methodology

IV. TYPES OF RISK AND SECURITY FACTORS

This section discusses about innovative actual research carried out to demonstrates different types of attacks specifically implemented is outlined in Table-I below,

Table-I: Types of Risk Factors

Security Risk	Device Implemented
Man in the Middle	Wireless Fidelity Device
Service Refusal	Smart Mobile Phones
De-Authentication	Use of Laptops and Mobile Phones
Un-authorized source Access	USB, Laptop and Mobile Phone
Frame Modification	Mobile Phones
Deactivation of Drone	Raspberry Pi

V. HACKING OF WI-FI BASED DRONE

The methodology process shown in the section 2.5 consists of various types of risk factors which is shown in table I, which also gives the analysis point of our experimentation outcomes.

The experimentation process is discussed in the following steps.

Step-1: First we organize different hardware devices such as drone, Raspberry-pi, Lap-top and smart mobile handset.

Step-2: Second setting up of drone takes place using raspberry-Pi which operates on Ubuntu OS and is embedded in the drone. The adaptor of network is fixed on the Raspberry-Pi USB port and fixed to the drone device. Five volts and two amperes power is supplied to the Raspberry Pi using a battery source.

Step-3: Third we set up the laptop which uses Ubuntu Parrot operating system which perform the attack process.

Step-4: Fourth, Wi-Fi networking is setup with fast connectivity with higher data rates is also practiced to construct a Wi-Fi network, which also inter-connects Raspberry-Pi & Laptop through Wi-Fi.

Step-5: Fifth step uses a process tool to construct an inter-connection among Drone (i.e. Raspberry-pi) and the Laptop, which enables to utilize remote Raspberry-Pi unit.

Step-6: In sixth step drone fly up and lands.

Step-7: The hijacker operates a Ubuntu based different types of attacks using a "Parrot" tool as listed in table I, using the Raspberry-pi platform by its laptops. The tool used for attack mainly chooses the network adaptor which basically indicates details about the different signals on Wi-Fi. Then attacker attempts to hijack Wi-Fi network and also Ubuntu tool enables to de-authenticate presents running users over the communication network and also seize the Wi-Fi request and reply status signals and also stores it. Ubuntu tool enable hacker to choose a phishing text which is indicated to ever real time users. Next, using this tool obstruct the users to access the main access point reconnections and prepares an equivalent similar access point having the matched title as of the access point of the target.Due to this connected users will find there is no Wi-Fi connectivity on the available access service point. Experiencing the failure, the users will detect secondary Wi-Fi connectivity which contain the matched title as displayed in present Wi-Fi connection.. The uses will in dilemma will make attempts to the equivalent Wi-Fi by inputting the user id key for the Wi-Fi enabling page, expecting to have once again access to the undetectable network connections. Ubuntu tool will then match the user id and password with the help of seized request and reply signal messages to find its original origin. After keys are matched as same, the security is hence compromised and actual Wi-Fi connectivity is now accessed by the hackers.

VI. PARROT SECURITY OS

The tool used for experimentation is a Debian-based Linux distribution based on cloud computation infiltration testing. It offers complete movable secure tab for cloud pen-testing. Computer forensics, hacking, cryptographic and abnormality detection.

- Specifications of the System: built on Debian nine, runs on a custom tough Linux four and half kernel, customs MATE desktop and Lightdm display administrator.
- Digital Forensics: backs "Forensic" boot choice to shun boot automounts plus many more.
- Anonymity: supports Anonsurf including anonymization of complete OS, TOR and I2P anonymous setups and beyond.
- Cryptography: support with custom based Anti-Forensic kits, interfaces for GPG and cryptsetup. Furthermore, it also support encryption kits such as LUKS, Truecrypt and VeraCrypt.
- Program design: braces FALCON (1.0) programming language, multiple compilers and debuggers and beyond.
- Complete support for Qt5 and .net/mono framework.
- It also supports development frameworks for embedded systems and many other amazing features.
- CPU: At least 1GHz Dual Core CPU.
- ARCHITECTURE: 32-bit, 64-bit and ARMHF.
- GPU: No graphic acceleration.
- RAM: 256MB – 512MB.
- HDD Standard: Six GB – Eight GB.
- HDD Full: Eight GB – Sixteen GB.
- BOOT: Legacy BIOS or UEFI (testing).

VII. ENCRYPTION MECHANISM

Encryption techniques used in the work is based on public key network security and text based. RSA Algorithm is chosen in public key cryptography. The encryption and decryption process is as follows:

- Choose randomly 2 prime numbers p and q.
- Compute Q = p x q and the least common multiple D of p – 1 and q - 1.
- Choose the encryption key K, by meeting the following 2 states:

  $1< K < D$, gcd (K, D) = 1 (1)

  Where, gcd represent the greatest common divisor K and
- Compute the decryption key V by meeting the following two states:

  $1 < V < D$, K x V mod D =1 (2)

  Where, mod represents remainder operation.
- The encryption process is represented by,

  $C = p^K$ mod Q (3)
- The decryption process is represented by,

  $P = c^D$ mod Q (4)

  Example in the algorithm used is as followed:

  Select primes: p=17 & q=11.

  Compute: n = p x q = 17 * 11 = 187 and

  Compute :(p-1) (q-1) =16x10=160.

  Select: e: gcd (e, 160) =1, choose e =7.

  Determine V: 23x7 mod 160.

  Encryption C: 88^7 mod 187.

  Decryption P= 11^{23} mod 187 =88.

VIII. EXPERIMENTATION RESULT

The Wi-Fi connection between access point and drone happens using tell-net with the help on IP address and sign up process is listed below:

C:\Users\User>ipconfig
Windows IP Configuration
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix.:
Link-local IPv6 Address . . . . .:
fe80::a9e7:2c78:897f:e49a%15
IPv4 Address . . . . . .: 192.168.42.91
Subnet Mask . . . . . .: 255.255.255.0
Default Gateway . . . . . :192.168.42.1
Ethernet adapter Local Area Connection:
Media State . . . . . .: Media disconnected
Connection-specific DNS Suffix. . :
C: \ User \ User >

The drone forensic is carried out using Parrot Linux OS on the laptop as shown in the list below:

Root 1970-01-02 11:35 tz -> /dev/block/mmcblk0p6
Root 1970-01-02 11:35 tzBackup
->/dev/block/mmcblk0p13
Root 1970-01-02 11:35 userdata ->
/dev/block/mmcblk0p42
Root 1970-01-02 11:35 utags -> /dev/block/mmcblk0p8
Root 1970-01-02 11:35 utagsBackup ->
/dev/block/mmcblk0p15
root@osprey_umts:/dev/block/bootdevice/by-name # □

The Modules to use an USB drive to the Drone details are listed below:

/data/video/usb-drive/load.sh
Setting pin 127
Loading nls_base.ko
Loading nls_utf8.ko
Loading nls_cp437.ko
Loading nls_iso8859-1.ko
Loading sd_mod.ko
Loading nbd.ko
Loading fat.ko
Loading vfat.ko
Loading dwc_otg.ko
Waiting 5 secs…
Displaying last lines of dmesg:
_____
[226.312392] hub 1-0:1.0: power on to power good time: 2ms
[226.312440] hub 1-0:1.0: local power source is good
[226.312465] hub 1-0:1.0: enabling power on all ports
[226.421424] hub 1-0:1.0: state 7 ports ports 1 chg 0000 evt 0000
[226.452524] /home/aferran/.ardrone/linux/ardrone_ARDrone_Version_20110401/Linux/kernel/linux/drivers/usb/inode.c: creating file '001'

[226.4675321 usb usb1: New USB device found, idVendor=1d6b, idProduct=0002
[226.467572] usb usb1: New USB device strings: Mfr=3,Product=2, SerialNumber=1
[226.467600] usb usb1: Product: DWC OTG Controller
[226.467623] usb usb1: Manufacturer: Linux 2.6.27.47-parrot dwc_otg_hcd
fdisk/dev/sda
The number of cylinders for this disk is set to 1109.
There is nothing wrong with that, but this is larger than 1024, and could in certain setups cause problems with:
Software that runs at boot time <e.g., old versions of LILO>
Booting and partitioning software from other OSs
< e.g., DOS FDISK, OS/2 FDISK>
Command <m for help>: p
Disk/dev/sda: 3951 MB, 3951034368 bytes
122 heads, 57 sectors/track, 1109 cylinders
Units = cylinders of 6954 * 512 = 3560448

Device	Boot	Start	End	Blocks	Id	System
/dev/sdal		2	1110	3854336	b	Win95 FAT32

IX. CONCLUSION

The work investigate basically classify and perform verities of security risk factors protection enhancement for the drone with raspberry-pi using IoT. At the beginning literature review on attacks in Wi-Fi based setup was carried out. The classification of attacks was part of the experimentation set up was deals with service refusal, de-authentication, Man-in-the-Middle, unauthorized source intruding and frame modifications.

The test was also carried out on Wi-Fi with raspberry-pi using IoT by executing similar text scripts. The methodology steps is also described the flow how the work involves the process of different attacks execution. Every types of attacks listed in table I is executed and the outcome results were collected to analyze and to secure the Communication in Wi-Fi mode using drone and another devices were analyzed. In a very simple steps, the hacker connect network with a Wi-Fi and pair it with a laptop, then attacker can observe the connected users traffic, which allow capture of information. RSA Algorithm is chosen using public key cryptography to improve the security of communication. From observations it is clear that the drone risk factors are important safety and privacy related issues for the drone users in Wi-Fi environment and the metropolitan area application using IoT.

REFERENCES

1. R. L. Finn, D. Wright, "Privacy data protection and ethics for civil drone practice: A survey of industry regulators and civil society organisations", Computer Law Security Review, vol. 32, no. 4, pp. 577-586, 2016.
2. L. Gupta, R. Jain, G. Vaszkun, "Survey of important issues in uav communication networks", IEEE Communications Surveys Tutorials, vol. 18, no. 2, pp. 1123-1152, 2016.
3. M. Mozaffari, W. Saad, M. Bennis, M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs", IEEE Transactions on Wireless Communications, vol. 15, no. 6, pp. 3949-3963, June 2016.
4. J. Pacheco and S. Hariri, "IoT Security Framework for smart cyber infrastructures," in Foundations and Applications of Self Systems, IEEE International Workshops, pp. 242-247, IEEE, 2016.
5. E. J. Cho, J. H. Kim, and C. S. Hong, "Attack model and detection scheme for botnet on 6lowpan," in Asia-Pacific Network Operations and Management Symposium, pp. 515-518, Springer, 2009.
6. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Communications Surveys & Tutorials, 2019.
7. M. Sakurada and T. Yairi, " Anomaly detection using autoencoders with nonlinear dimensionality reduction," in Proceedings of the MLSDA 2014 2nd workshop on Machine Learning for Sensory Data Analysis, p. 4, ACM, 2014.
8. R. Luppicini, A. So, "A technoethical review of commercial drone use in the context of governance ethics and privacy", Technology in Society, vol. 46, pp. 109-119, 2016.
9. S. M. Shavarani, M. G. Nejad, F. Rismanchian, G. Izbirak, "Application of hierarchical facility location problem for optimization of a drone delivery system: a case study of amazon prime air in the city of san francisco", The International Journal of Advanced Manufacturing Technology, vol. 95, no. 9, pp. 3141-3153, Apr 2018.
10. S. M. Bae, K. H. Han, C. N. Cha, H. Y. Lee, "Development of inventory checking system based on uav and rfid in open storage yard", 2016 International Conference on Information Science and Security (ICISS), pp. 1-2, Dec 2016.
11. M. Mozaffari, W. Saad, M. Bennis, Y. Nam, M. Debbah, "A tutorial on uavs for wireless networks: Applications challenges and open problems", CoRR, 2018.
12. S. Winkler, S. Zeadally, K. Evans, "Privacy and civilian drone use: The need for further regulation", IEEE Security Privacy, vol. 16, no. 5, pp. 72-80, September 2018.
13. J. Engel, J. Sturm, D. Cremers, "Camera-based navigation of a low-cost quadrocopter", 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 2815-2821, Oct 2012.
14. M. Saska, T. Krajnk, J. Faigl, V. Vonsek, L. Peuil, "Low cost mav platform ar-drone in experimental verifications of methods for vision based autonomous navigation", 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 4808-4809, Oct 2012.
15. D. Flores, D. Marcillo, J. Pereira, Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, S. Costanzo, "3d localization system for an unmanned mini quadcopter based on smart indoor wi-fi antennas" in Recent Advances in Information Systems and Technologies, Cham:Springer International Publishing, pp. 543-550, 2017.
16. G. Pasolini, A. Bazzi, F. Zabini, "A raspberry pi-based platform for signal processing education [sp education]", IEEE Signal Processing Magazine, vol. 34, no. 4, pp. 151-158, July 2017.
17. C. Jenks, "Real-time rogue wireless access point detection with the raspberry pi", Linux J., vol. 2014, no. 248, Dec. 2014.
18. F. V. Yarochkin, O. Arkin, M. Kydyraliev, S. Dai, Y. Huang, S. Kuo, "Xprobe2++: Low volume remote network information gathering tool", 2009 IEEE/IFIP International Conference on Dependable Systems Networks, pp. 205-210, June 2009.
19. Y. Kwon, J. Yu, B. Cho, Y. Eun, K. Park, "Empirical analysis of mavlink protocol vulnerability for attacking unmanned aerial vehicles", IEEE Access, vol. 6, pp. 43 203-43 212, 2018.
20. J. Milliken, V. Selis, K. M. Yap, A. Marshall, "Impact of metric selection on wireless deauthentication dos attack performance", IEEE Wireless Communications Letters, vol. 2, no. 5, pp. 571-574, October 2013.
21. M. Agarwal, S. Biswas, S. Nandi, "Advanced stealth man-in-the-middle attack in wpa2 encrypted wi-fi networks", IEEE Communications Letters, vol. 19, no. 4, pp. 581-584, April 2015.
22. Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking ser. MobiCom '00, pp. 275-283, 2000.
23. K. Huang, H. Wang, "Combating the control signal spoofing attack in uav systems", IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7769-7773, Aug 2018.
24. A. Guillen-Perez, R. Sanchez-Iborra, M. Cano, J. C. Sanchez-Aarnoutse, J. Garcia-Haro, "Wifi networks on drones", 2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT), pp. 1-8, Nov 2016.

AUTHORS PROFILE

Pratheepa Marimuthu, did her M. Tech in Computer Science and Engineering from Prist University, MCA from Bharathidasan University. She has done paper Publications and Pursuing Research work to her interested domains specifically in Wireless Communications and Networking, Puducherry, India, PH: +91 8870227422,
E-mail: pratheepa.mtech@gmail.com

Saran Kumar Sekar, did his M. E. in Aeronautical Engineering from Hindustan University, Chennai-India. He has published two papers and actively involved in research work in his area of expertise. Presently he is working as Lecturer in the Department of Aeronautics, St. Theresa International College, Nakhhonnayok- Thailand, PH: +66928703020,
Email: sarankumar@stic.ac.th