Wireless Network Deauthentication of UAV

Aravind.S[1],Bharath kumar.C[2],Dilli Babu.B[3],Gokula Krishnan.M[4]
[1, 2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] Valliammai Engineering College,Potheri,Chennai

Abstract- *In present days, there are lot of trouble caused by these unmanned aerial vehicles. Security problems of these UAV have been described and analysed. UAVs are introduced as a playthings with very low cost. Now-a-days it is used by many organizations which leads to detrimental attack.Some UAVs used for country missions like monitoring,security missions by defence department.Not all professional UAVs are not harmful.This proposal will prove the security defile of a UAV which is used by defence force for many complicated missions.In this proposition,it is demonstrated how one can perform the identified security vulnerabilities,man in middle attack and throw in control commands to communicate with UAV.The drone with video stream as a ability to record the confidential information.This proposal will perform security analysis on unmanned aerial vehicle.This project will focus mainly on security vulnerabilities like unencrypted wireless connections,the user management of the GNU/Linux operating system which runs on the drone.The aim of this project is to show how the UAV can be secured from the unauthorized access and also the vulnerabilities of UAV.The instructions to secure the UAV's wireless connection and its operation with official android application will be provided*

Keywords- UAV,GNU/LINUX,Defile,Man in Middle Attack,unencrypted Wireless Coneection

I. INTRODUCTION

It is true that the recreational Unmanned Aerial Vehicles (UAVs), accessible to the general public, are not secure is not new. There are different paper and journals have been published showing that one can easily hack into these devices. These professional UAVs are applied in the field of surveillance, border control and search & rescue. These professional UAVs can deliver the performance and functionalities that are needed for sensitive and critical operations. The advanced features of these professional UAVs are long endurance and the ability to carry heavy payload. Hence, the more expensive the device the more advanced it is, and professional UAVs can easily cost several thousands of dollars. In that range of applicability, one should expect that security is a top priority for professional UAVs. From this analysis on a professional UAV, it is clearly shown that this is not the case. It undergoes critical operations for which these UAVs are used in danger of failure at the very least.In this demo, it is shown that professional UAVs are not as secure as one might expect [1]. It is demonstrated by learning how the UAV communicates with the control station, one can perform a Man-in-the-Middle (MitM) attack and potentially take control over the UAV, even several kilometers away from the actual UAV's control station.. With this findings the awareness raised within

1. The general public that use and trust such professional UAVs,
2. The scientific community by illustrating that further research is needed in this area, and
3. The manufactures by showing the importance of implementing a higher level of security in their devices.

The paper also describes the security vulnerabilities of the UAV using different attacking scenarios. Also, the ways to take countermeasures from these attacks are also listed.

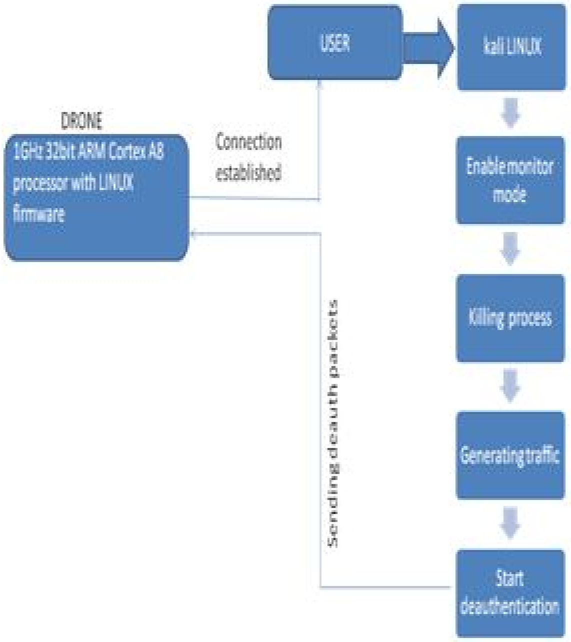
II. EXISTING SYSTEM

In order to control a drone remotely, you must be able to communicate with it wirelessly. Radio waves are an invisible wave form on the electromagnetic spectrum. Like all things on the electromagnetic spectrum, radio is measured in hertz (Hz). Extremely low frequency is anywhere from 3Hz to 30Hz and tremendously high frequency is 300 GHz – 3000GHz.For radio to work, you must have a transmitter to send the messages and a receiver to get the messages. At a rudimentary level, this is how remotely controlling an aircraft is accomplished. More precisely, your transmitter and receiver need to be tuned to the same frequency. To avoid situations such as your drone being controlled by someone else's remote control, devices use a unique identification code to identify a transmission on one particular radio frequency as the transmission it wants to receive. In the existing system the RF drone have been hacked by using the Hack RF Device Since the RF drone are Upgraded to Wi-Fi Drone,which will not be hacked by using Hack RF devices.

II. PROPOSED SYSTEM

we proposed the system that should communicate with UAV by establish wireless connection into drone network.the purpose is to proceed the deauthentication process by sending the abstract commands(AT command) to drone. system should be able to send abstract commands to drone.The system should be able to send and receive data from drone and process data packets.While sending deauth packets the system should able to interact appropriate abstract for UAV to avoid any obstacle along its flight path.

B .Architecture Diagram



`

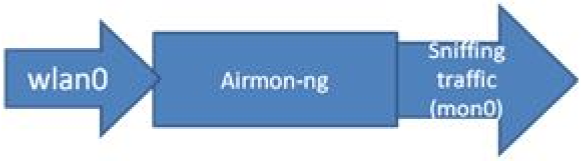
FIG.1 SYSTEM ARCHITECTURE

III. LIST OF MODULES

1.Starting Monitor Mode
2.Killing Unwanted process
3.Scanning UAV networks
4.Identification of UAV’s BSSID ID
5.Deauthenticating UAV network

1. Starting Monitor Mode

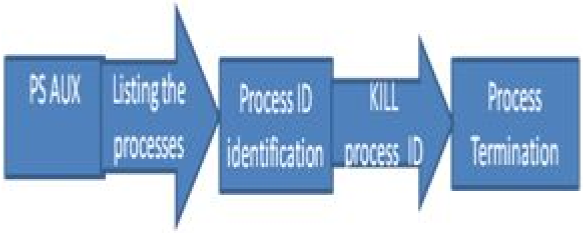
Monitor mode allows a system with wireless controller to monitor all traffic received from the wireless network.This mode is also used for packet sniffing.This mode observes the widespread traffic.This mode is also useful during the design phases of wifi network construction to discover how many wifi devices are already using spectrum in an given area and how busy various wifi channels are in that area.In this mode the wireless network adapter is changed into monitor mode by using the airmon-ng command.



Figure(1):Starting Monitor Mode

2. Killing Unwanted process

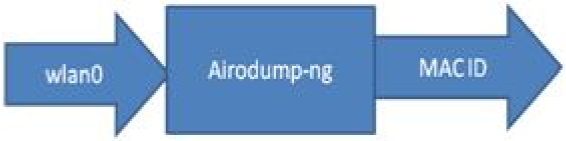
It is a command set in LINUX used to send a signal to terminate the process.The killing process works when the process ID of a particular process is given (KILL process_ID or KILL ALL).This command terminate all the process running in background of the system so that can able to continue the deauthentication process without any time delay.



Figure(2):Kill Process

3. Scanning UAV’s Network

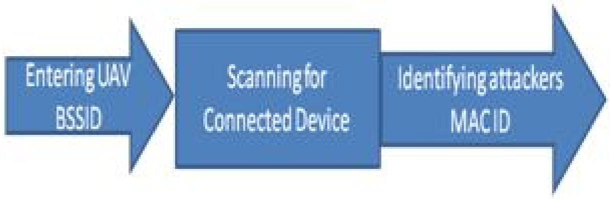
This module scan each and every wifi network within the range(depends on the system wifi range).MAC ID ,channel number and name of all the network will be identified in this process.The following scanning process will able to identify all the available networks where the drone network is being separately identified.Most of the drone networks is identified by their specific name which is different from other networks.



Figure(3) Scanning UAV’s Network

4. Identification of UAV’s BSSID

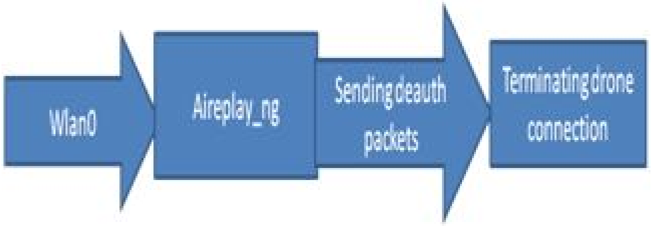
This module identify the MAC ID of the system connected to the Wifi network.Channel number will also be identified.The BSSID of the intial drone controller is necessary to terminate the connection of drone with the owner.



Figure(4):BSSID Identification

5.Deauthentication of UAV's Network

In the final module the drone is identified and the deauthentication procsee is initiated.In the deauthentication process aireplay-ng command is used to send the deauth packets.The deauth packets is continuosly sent to the drone network to terminate the connection between controller and the drone.



Figure(5):Deauthenticating UAV's Network

V. OBJECTIVE OF THE SYSTEM

- To provide security from the unauthorized attackers.
- To analyse the threats of wireless networks.
- To enhance safety of the people.

VI. CONCLUSION

There were lot of difficulties faced during the development of the proposed system. One of the biggest challenges that encountered in this project was the fast draining battery issue. This possesses a very big challenging issue in this project because every system testing session could only last for 10 to 12 minutes only. In fact, a lot of system testing cases needed to be evaluated. Such limitation greatly affects overall system testing progress since longer testing duration is needed to carry out various system testing. Weather events such as high winds and climatic changes also affect the overall performance of the UAV. The UAV might not able to fly properly under such conditions. Further study and proper enhancement can be done on this project. One of the modules that can be enriched on is the obstacle detection system (ODS). Due to time constraint and limited prior knowledge of Java technologies, the ODS is still under development and explores the possibilities of developing a good detection system for the flying drone. Also by using a Virtual Private Network (VPN) service, UAV can be made secured from the hackers. It acts as a gateway between the UAV and the internet. In addition to this implementing MAC filtering in the UAV enables to specify the MAC address for connection. Currently in WPA 256 bit keys are used. For higher standards 512 bit keys can be recommended enabling higher level of security. Above all to make the UAV more secured, enabling firewall in the base station and the UAV can be done. This is basically a hardware firewall being implemented at both the ends. Also, NAT configuration can be made so that the UAV network can be made unidentifiable by the outside network.

REFERENCES

[1] J. Pleban, R. Band, and R. Creutzburg, "Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy", published in IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics on January, 2014. ISSN No. 2231-1009 DOI: 10.1117/12.2044868.

[2] Sait Murat Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing", published in Recent Advances in Space Technologies (RAST), 2013 6th International Conference on 12-14 June 2013, Volume No. 12 pp 795-800, ISBN: 978-1-4673-6395-2 DOI: 10.1109/RAST.2013.6581320.

[3] Aakash Sehrawat; T.Anupriya Choudhury; Gaurav Raj, "Surveillance drone for disaster management and military security'',Published in 2017 International Conference on Computing, Communication and Automation (ICCCA),Electronic ISBN:978-1-5090-6471-7,DOI:10.1109/CCAA.2017.8229846

[4] Fred Samland ; Jana Fruth ; Mario Hildebrandt;Tobias Hoppe and Jana Dittmann,"AR.Drone: security threat analysis and exemplary attack to track persons"In IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, Volume No.8301, public shed on 2012, pp1-8, ISSN No.0973-3426 DOI: 01/2312.902990

[5] http://laurent.fallet.free.fr/docs/concordia/aircrack.pdf

[6] http://eprints.utar.edu.my/1846/1/FYP_2_Full Report.pdf