University Libraries
University of Nevada, Las Vegas

12-1-2016

Improvement of Security in UAS Communication and Navigation using ADS-B

Vedadatta Gouripeddi
University of Nevada, Las Vegas, gouriped@unlv.nevada.edu

IMPROVEMENT OF SECURITY IN UAS COMMUNICATION AND NAVIGATION USING

ADS-B

By

Vedadatta Gouripeddi

Bachelor of Technology, Computer Science
Jawaharlal Nehru Technological University, India
2009

A thesis submitted in partial fulfillment
of the requirements for the

Master of Science in Computer Science

Department of Computer Science
Howard R. Hughes College of Engineering
The Graduate College

University of Nevada, Las Vegas
December 2016

UNLV | GRADUATE COLLEGE

Thesis Approval

The Graduate College
The University of Nevada, Las Vegas

November 17, 2016

This thesis prepared by

Vedadatta Gouripeddi

entitled

Improvement of Security in UAS Communication and Navigation using ADS-B

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science
Department of Computer Science

Yoohwan Kim, Ph.D.
Examination Committee Chair

Ajoy K. Datta, Ph.D.
Examination Committee Member

Wolfgang Bein, Ph.D.
Examination Committee Member

William Culbreth, Ph.D.
Graduate College Faculty Representative

Kathryn Hausbeck Korgan, Ph.D.
Graduate College Interim Dean

ABSTRACT

Improvement of Security in UAS Communication and Navigation using ADS-B

By

Vedadatta Gouripeddi

Dr. Yoohwan Kim, Examination Committee Chair

Associate Professor, Department of Computer Science

University of Nevada, Las Vegas

In this thesis, we congregate the security threats on UAS and suggest solutions using ADS-B device. UAS ground and intercommunication is prone to availability, confidentiality and integrity attacks. UAS communication has three layered wireless Ad-Hock network which comprises of Complex group key exchange. Loss of one layer in the Ad-hock network leads to a complete loss of communication in the network. Current UAS navigation methods include complete reliance on onboard sensors, radars and GPS. This research proposes solutions for UAS communication, navigation and collision avoidance using ADS-B. ADS-B acts as a back-up when there is a loss in any one of the trees layers in an Ad-Hock network. Integration of ADS-B along with onboard sensors gives an accurate and precise location of the UAS. ADS-B also helps in neighbor discovery which prevents collisions in small UAS.

ACKNOWLEDGEMENTS

I would like to sincerely thank Dr. Yoohwan Kim for the opportunity he has given me to work as a research assistant and his constant support, motivation through tough situations. I would also like to thank him for his guidance in successful completion of my thesis. Door to Dr. Yoohwan Kim office was always open whenever I ran into trouble or had a question about my research.

I would like to thank Dr. Ajoy K. Datta, Dr. Wolfgang Bein, and Dr. William Culbreth, the experts in this committee who were involved in validating and reviewing my thesis. I would like to specially thank Dr. Ajoy K. Datta for the help and support he has given me throughout my masters at UNLV. This masters journey would not have been possible without the support and inspiration from Dr. Ajoy K. Datta.

I must express my profound gratitude to my parents G.V.S Murthy and G. Prasuna. I would like to thank my parents for their constant support. My mother is my hero; she has taught me to never to give up and to always face fears with courage. I would like to thank my sisters V. Jyotsna and G. Krishna Priya who stood by me through sorrow and happiness. Finally, I would like to thank my sister G. Krishna Priya and cousin brother G Ram Kiran for their trust in me and keep me motivated through tough times. This accomplishment would not have been possible without all the names I have mentioned on this page. Thank you.

TABLE OF CONTENTS

v

vi

LIST OF TABLES

LIST OF FIGURES

ix

LIST OF ABBREVIATIONS

ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance - Broadcast
ADS-C	Automatic Dependent Surveillance-Contract
ADS-R	Automatic Dependent Surveillance-Rebroadcast
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
BCAS	Beacon Collison Avoidance System
CPDL	Controller-Pilot Data Link
CPR	Compact Positioning Report
CWN	Collaboration Wireless Network
DDA	Date De-Synchronization Attack
DME	Distance Measurement Equipment
DOS	Denial of Service
DSP	Digital Signal Processor
FANET	Flying Ad Hoc Network

FIS-B	First Information Service-Broadcast
GCS	Ground Control Station
HALE	High Altitude Long Range
HAP	High Altitude Platform
ICAO	International Civil Aviation Organization
ICPK	Implicitly Certified Public Keys
IDA	Information Dispersal Algorithm
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
LODMAC	Location Oriented Directional MAC Protocol
LOS	Line of Sight
MALE	Medium Altitude Long Range
MANET	Mobile Ad Hoc Wireless Network
MBN	Mobile Back Bone Nodes
MEA	Middle of the Earth Attack
MEMS	Microelectromechanical systems
MSO	Message Start Opportunity
NAS	National Air Space

OFT	One-way Function Tree
PCAS	Portable Collision Avoidance System
PKI	Public Key Infrastructure
PRV	Remotely Piloted Vehicle
PSR	Primary Surveillance Radar
PVT	Position Velocity Time
SAAS	Sense and Avoid System
SSR	Secondary Surveillance Radar
TCAS	Traffic Collision Avoidance System
TGDH	Tree-based Group Diffie Hellman
TIS-B	Traffic Information Service-Broadcast
UAS	Unmanned Aerial Systems
UAT	Universal Access Transceiver
VWN	Vulnerable Week Number

CHAPTER 1: INTRODUCTION

An Unmanned aerial system (UAS) is an autonomous air vehicle which does not have any crew on board. Unmanned Aerial systems are also called as drones. One of the most common type of UAS is the remotely piloted air vehicle (RPV). UAS was designed to fly in locations where a manned aircraft would be prone to risk of attacks and a pose a threat to human life. UAS were in use as early as the late 1850's. The first air vehicle was built using a large gas balloon for combat purposes. Developments and research to use UAS for military purposes has taken a strong hold during the World War 1 and World War 2.

In the recent years and a lot of research and investment has been put into drone development and its research. Drones have proved that they are very useful not only in the war fields but also in our day to day activities. Per global market estimates top companies manufacturing consumer drones have seen an average increase of 32% growth rate annually. Figure 2 shows the demand for commercial consumer drones. FAA has registered three hundred thousand consumer drones in January 2016 and predicts that approximately 50% of the drones are not yet registered. By 2020 usage of consumer drone predictions are sky rocketing.

■ Types of UAS

Classification of UAS can be done based on size and range. Classifications based on size are very small, small, medium and large UAS. Very small and small UAS systems are the most commonly bought for civil purposes [1]. Medium and large are used for military purposes. Classification based on range are low cost, range and endurance. High endurance UAS are currently being used as orbital UAS. Orbital UAS are proposed to be the next generation satellites. Orbital UAS fly with the help of solar energy for longer endurance or range. Some of the

1

classifications based on altitude parameter and speed are Medium Altitude Long Range (MALE),

and High Altitude Long Range (HALE). Classification of UAS are shown in Figure 1.
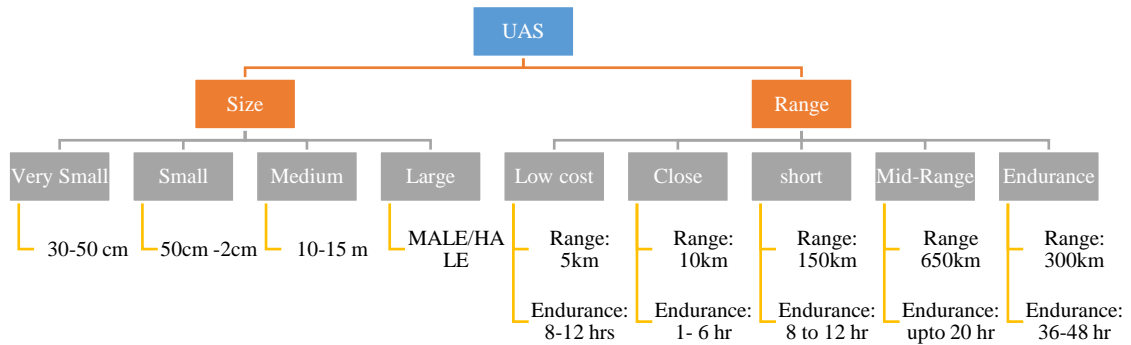
Figure 1: Classification of UAS

CONSUMER DRONE-SALES PREDICTION
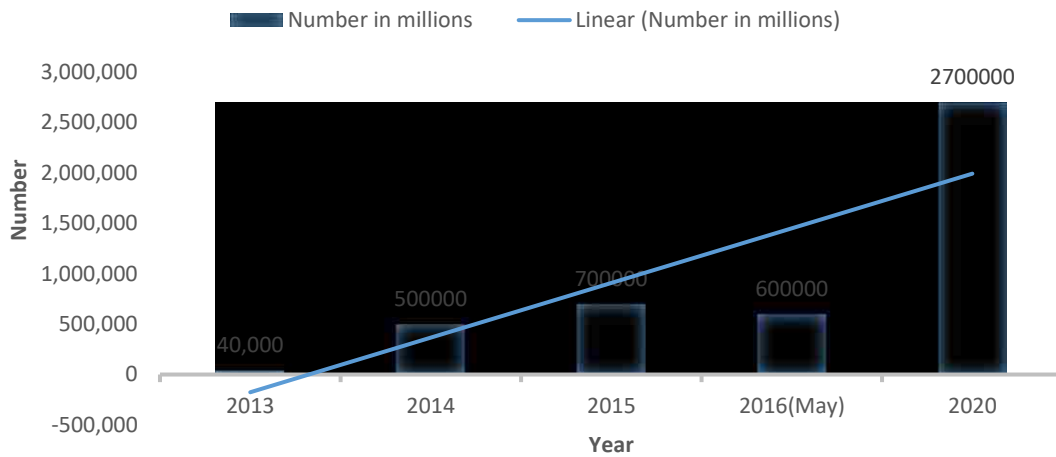
Figure 2: Sales prediction of consumer drones.

UAS Applications

UAS can be used different purposes including civil and military (combat efficient). The most common use of UAS is for surveillance. Surveillance UAS carry advanced equipment such as high resolution video surveillance camera. In addition to capturing surveillance images, UAS cameras help in route planning and terrain detection by leveraging inbuilt vision system both in 2D and 3D. Advancements not only in the technical and software aspects of the UAS but also in the mechanical construction of the UAS has played a major role in broadening their use in recent years. Improvements in mechanical components, electrical motors, artificial intelligence, endurance life, maneuverability, and ease of use have resulted in mass production of UAS for civilian purposes. Solar panels are also being deployed to supplement battery power and improve the endurance of UAS.

Applications UAS is widely used are security, search and rescue, monitoring, disaster management, crop management, communications and survey[2]. Recently introduced into Oceanography, photography and environmental. UAS has proved to be very beneficial in environmental purposes. Some of the environmental purposes are assessing and monitoring pollution, air quality detection, wildlife monitoring and behavioral research, forest monitoring, volcano monitoring, avalanche monitoring etc. Future inventions and research is in the areas of detecting and disabling bombs, identification of hostage situations and distribution of medical supplies in emergency situations[3].

Motivation

UAS is going to play an important role in the future. Applications are going to become more and more dependent on UAS systems. Already some of the sectors like agriculture, wildlife monitoring, weather tracking and security surveillance have started depending on UAS. Ease of

3

operation and low cost maintenance has pushed for a shift from traditional small manned aircrafts to autonomous UAS. Although, there is such a high demand for UAS, full-fledged implementation of the UAS into the National Air Space(NAS) is not possible at least till 2020. Autonomous UAS depend on GPS and other sensors for location identification whereas small UAS use line of sight flight control by using Wi-Fi and low powered networks. Either ways, be it autonomous or line of sight UAS depend on very vulnerable networks which are very easy for attacks. Jamming, spoofing eavesdropping are just some of the many security threats possible on UAS.

To avoid different kinds of security threats that are possible on UAS, fusion and dependency on many sensors is recommended. ADS-B is a surveillance device used to track aircrafts. Implementation of ADS-B into UAS can make a significant difference in improvement of security in UAS. ADS-B also has security issues as perfect security solutions for ADS-B are yet to be proposed. The combination of GPS sensors and ADS-B can provide accurate positional information of the UAS. Integration of ADS-B into UAS can improve clarity in communication and accuracy in navigation.

CHAPTER 2: SECURITY IN UAS COMMUNICATION

The communication in UAS happens typically in three distinct ways – UASs communication with ground control station (GCS), UAS communication with Air traffic control (ATC), and Intercommunication between UAVs. The schematic in Figure 3 shows three types of communications in UAS.
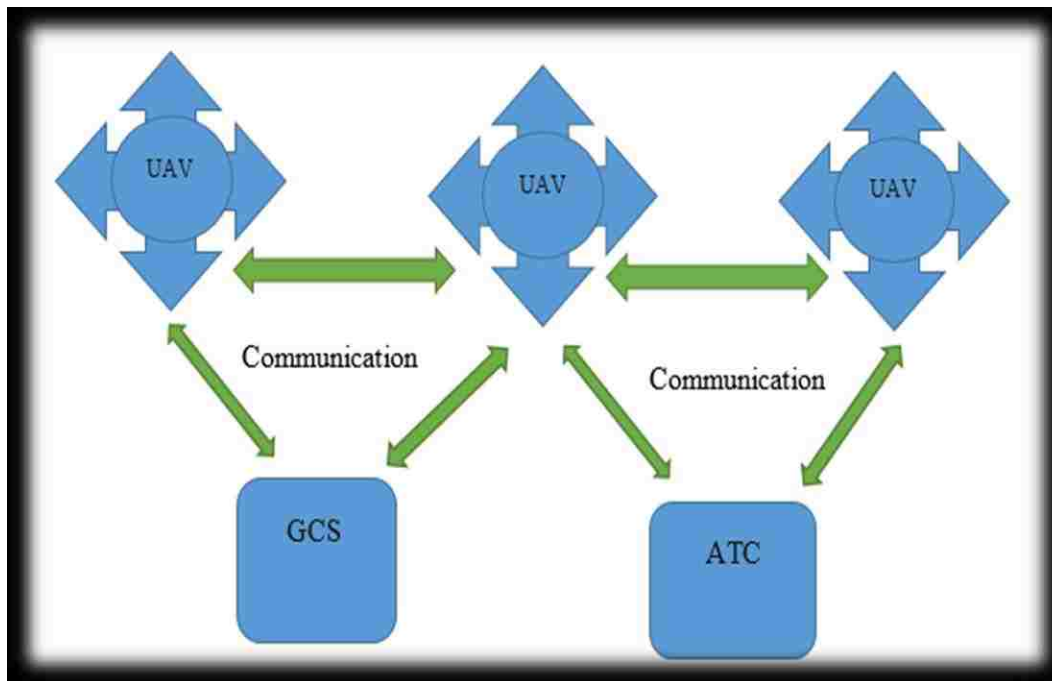
Figure 3: Schematic of UAS Communication

■■■ Communication between UAS and Ground control station (GCS)

Ground control station is a work station from where human can control a UAS. Ground control stations are mostly located on land or sea to control drones within or in the atmosphere. GCS provides necessary capability for operations at different levels. Important motives of GCS are to provide communication, display flight path and mission planning. GCS has a human operating a variety of devices that can establish communication with the UAS. Some of the

5

devices that can be used to establish communication are radio transmitter/receiver, smart phone, a computer and a Control center mostly used for military purposes. Recently developed advancements are small UAS can be controlled by hand held wearable devices. GCS may be divided into two types local and High Quality (HQ). Generally, HQ GCS might be located at some military operated agency, while local is located at any suitable ground location. Local GCS also include portable GCS. Portable GCS are nothing but laptops, tablets and phones. The communication between a GCS and a UAS would be a Line of Sight(LOS) radio based communication or GPRS. Local GCS is more vulnerable to threats than HQ GCS because security measures are already in place for HQ [4]. The basic functions of a GCS are to establish mission planning, flight control or maneuver of a UAS and information transfer.

GCS in the recent years with advancement in technology, a single GCS is being used to control more than one UAS at the same time. GCS set up can be divided into two parts internal and the external as shown in Figure 4 and Figure 5. In the internal part of the GCS has control of the UAS, display, pilot box, UAS flight data, planning and analysis, flight information broadcast and video and audio transmission information. The external part of the GCS consists of wireless communications and wired communications with external interfaces as shown in the table 1.

Figure 4: Inside a Ground Control Station.

6

Table 1: GCS Interfaces.

Position	GCS equipment
Internal	Flight Control and Information
	Display Screen for Control and Vehicle status
	Pilot Box
	UAS Flight Data
	Planning and Analysis
	Audio and Video Transmission Display Panels
External	Equipment for Wireless Communication
	Equipment for Wired Communication
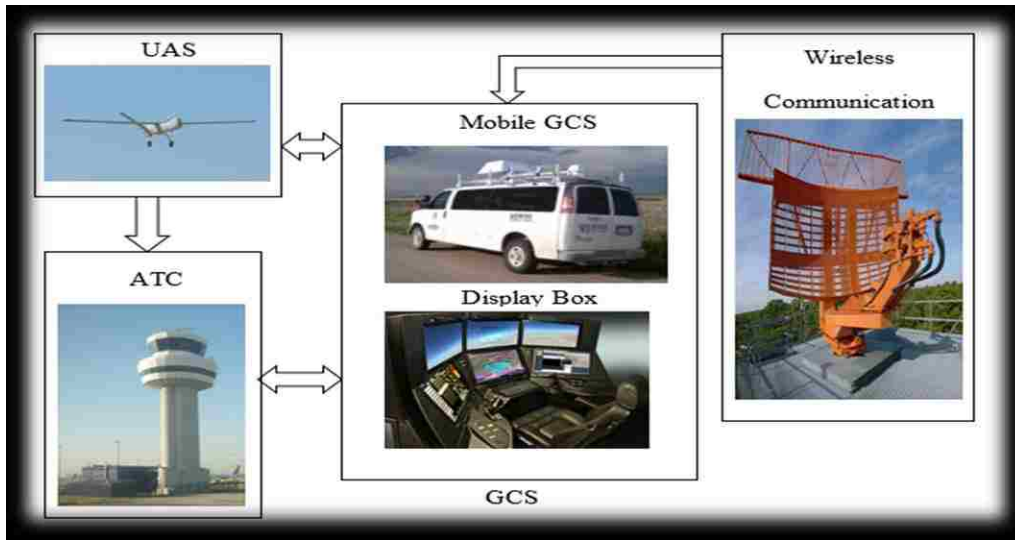
Figure 5: Communication pattern and interface of GCS.

Security in UAS-to-GCS communication is characterized by three different parameters that

are described as follows:

7

2.1.1. Availability

When ground radio transmitter/receiver and air-borne radio transmitter/receiver are in good working condition despite the adverse effects such as rain, foliage, jamming and airframe blockage, then the UAS communication is said to be effectively available. Availability attacks are generally jamming, falsifying signals and denial of service(DOS) [4].

2.1.2. Confidentiality

These attacks generally deal with unauthorized access to information. The easiest way to compromise the information is by intercepting the information. Confidentiality threats to GCS are mostly computer based i.e. malwares, Trojan and key loggers. Basic unintentional human errors also come into account. Confidentiality is inversely proportional to continuity. Continuity is defined as uninterrupted packet delivery during communication between UAS and the GCS [4].

2.1.3. Integrity

Integrity attacks are defined on two basics one, if the existing data is being modified or when data is being fabricated [4].Integrity is a measure of undetected errors in the message over a defined span of time. The greater the number of undetected errors, the lesser the value of integrity.

■ Communication between UAS and air traffic control center (ATC)

ATC is responsible for communicating with the UAS and providing it with the information on landing clearances, route path, meteorological information etc. It also broadcasts positioning, altitude and velocity information among the UASs and other aerial vehicles in vicinity. The ATC's transponder transmits various tele commands to the UAS autopilot and receives telemetry data from the autopilot. Some of the commonly used tele commands are ADS-B, Automatic Dependent

8

Surveillance-Rebroadcast (ADS-R), Automatic Dependent Surveillance – Contract(ADS-C), First Information Service-Broadcast (FIS-B), Traffic Information Service-Broadcast (TIS-B) etc.

◼ UAS Intercommunication

UAS Intercommunication is the communication between different UAS flying in the same vicinity which share each other's flight information. UAS intercommunication is used in both civilian and military purposes. In civilian sector, this is used to provide a simple and low cost communication solution. Intercommunication is key in military applications where UAS form a network for strategical attacks. UAS intercommunication is complex and can prove to be disaster if not handled properly. To ensure that there is a proper synchronization between all the UAS present in the intercommunication network, various protocols are used in UAS intercommunication. A few salient features for intercommunication are discussed in the following sections.

2.3.1. High Altitude Platforms (HAPs)

The demand for high speed wireless communication is increasing day by day. Setting up a broadband connection to deep rural areas has its own complexities. Setting up a mobile high altitude platform for internet access would be the cheaper and better in terms of wider connectivity. High altitude platforms (HAP) are airships or airplanes which are normally setup in the stratosphere. HAP's help in setting up 3G and Wi-Max. HAP's usually use a hydrogen balloon, Helium Air ships or the Drone [5].

HAP's establish a connection with the satellite as well as the ground base stations as a backup. HAP uses resource allocation techniques which helps maximize bandwidth. HAP also has a power advantage over satellite and terrestrial schemes. A tether is used to lift the airship. A PoE cable is used from ground to the HAP which provides power supply and Ethernet. At the HAP a

9

multi directional antenna is mounted which receives and sends data packets. Data packets can be received and sent from the HAP if there exists a line of sight connectivity between the user and the airship. Generally, this kind of setup is used for internet in rural areas where ground connection may not seem to be a possibility.

▬▬▬▬ A terrestrial HAP satellite system.

A terrestrial HAP satellite system includes a satellite link as well as a terrestrial system to improve the quality of the communication. Information is transferred from fiber networks to HAP network. The information from fiber networks is transmitted through a wireless medium to the satellite, which in turn is transmitted to the HAP's [5].

▬▬▬▬ An Integrated terrestrial – HAP system

In this network the HAP's are connected to the terrestrial networks and satellites are not used in this system [5].

▬▬▬▬ A Standalone HAP system

In this standalone HAP system, HAP uses terrestrial as a backup and satellite as an alternative for remote and rural areas. A terrestrial and satellite system are costly. This system can be deployed easily and effectively [5] compared to others.

2.3.2. Flying Ad Hoc Networks(FANET's)

Flying Ad Hock Networks are gaining popularity because of their promising technology. This is useful for both military and civil airspaces. FANET's are nothing but a set of group of small Unmanned Aerial Vehicles which form of a chain of network. This network has many advantages when used in conjuncture with HAP. In FANETS's traditional omnidirectional antennas are used, which are a drawback because of their slow speed of movement. In FANET

10

moving nodes have highly advanced network topologies. To overcome this drawback FANET's currently switched over to directional antennas. Use of directional antennas in FANET systems has a drawback too, that is neighboring nodes or the neighboring UAS cannot be determined through the antenna. The neighbor discovery drawback can be overcome by using the HAP in conjuncture. Layer 1 which is the ground level would consist the GCS or the ground station, Layer 2 would be the small group of UAS circulating and the Level 3 would consist of a HAP. The ground station will be linked with a Master UAS which will be the head of the group of UAS and all the UAS in turn are connected to the HAP [6]. The three-layered conjecture of the FANET is shown in Figure 6.
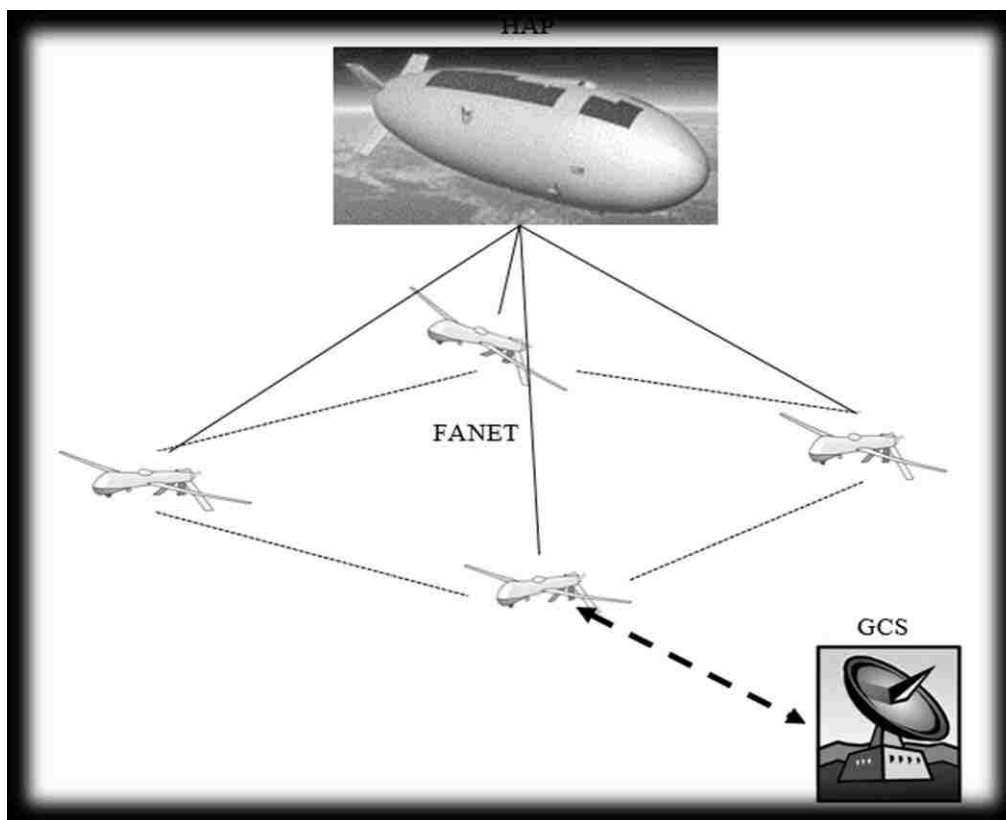
Figure 6: FANET [6]**.**

FANET application works for nodes anywhere between three and twenty. Nodes maintain a distance between them to avoid collision. FANET use a protocol called the Location Oriented Directional MAC Protocol (LODMAC). Nodes in the FANET use this LODMAC to communicate between each other and with the HAP. LODMAC protocol generally consists of three antennas and three receivers on a single node. Three receivers present on the node have three different functions. First receiver is directed towards the HAP and is responsible getting neighboring nodes addresses using the HAP in conjuncture. Second transceiver is used for connections establishment. Third receiver responsible for data transfer. HAP and LODMAC depend on GPS which broadcasts every second. In the first half of the GPS signal, HAP detailing the locations of the all the nodes is broadcasted and in the second half the location of the node is shared with the HAP. Once a node receives the signal, they update their neighbor table with the nearest nodes location vector. Some other important information broadcasted are the specific node id, Antenna orientation and the ID of the node with which it communicates [6]. LODMAC is a very open protocol that address the directional hidden terminal and blocking problems. LODMAC also ensures that it provides all nodes with exact GPS location of its neighbors.

2.3.3. Mobile Ad-hoc Wireless Networks (MANET's)

Wired Communication poses a great access difficulty for installation in a remote area due to factors like inaccessibility, wildlife and a security threat. The best solution to provide simple internet accessibility is by using the Mobile Ad-hoc Wireless Networks which do not require complicated infrastructure. MANET communication has received a great deal of attention in both civilian and military sectors. This technology aims to provide uninterrupted internet access anytime and anywhere. MANET aims to facilitate access to internet and reach the world from any remote location[7].

12

MANET is depending mainly on wireless communication and that is the reason for MANET network to be prone to security attacks. MANET's communication is divided into control group and cell groups [7]. Control groups are the Mobile Backbone Nodes(MBN) and the cell groups are the nodes or the end users situated on the ground in a cluster. Each cell in the cell group is connected and managed by an MBN. Secure group communication is established by this hierarchical architecture. Each time a new node is added or removed from the group, a new key is circulated among all the group members to protect data from potential compromises. The traditional key management approaches do not work so well for the MANET because of the MANET's highly dynamic nature. Attacks from not only outside, attacks from with the group are also expected in MANET's. The traditional group key management schemes do not recommend a strong security plan for threats that are possible from inside the group. As the network size grows in the MANET's the bandwidth availability and speed reduces, for this reason we use an Unmanned Aerial System-Mobile backbone network. The UAV-MBN network have three levels UAS, MBN and ground networks.

▮▮▮▮▮ Group Key Management in UAS-MBN

Group Key Management is layered approach. The lower layer is called cell group which has a ground MANET node and Individual nodes. The upper layer is called the control group which has an MBN node. Cell group has same broadcast range. Control group MBN is responsible for key management and point-to-point wireless communication among themselves in the cell group. Cell group shares a group key which is generated and distributed by the control group manager. Group key management within a cell group is performed by the MBN node. Control group manager nothing but the MBN node [7]. This MBN node's also carry a control group key among themselves. Control group key is managed among themselves in an alternating fashion by all

13

MBN nodes that are in the control group manager family. MBN node is also responsible for relaying data from within the cell group to another cell group.

The cell group uses the One Way Function Tree(OFT) and the control group uses the Tree-based Group Diffie-Hellman(TGDH) [7]. Cell groups are designed in a fashion that they are free to choose which ever key management scheme depending on the communication environment they are in. Dynamics in one cell group do not overlap with that of the other cell group because each cell group is independent of using different key management schemes. A new node can join the cell group by using the public key certificate. To validate the certificate each node needs to maintain a public key infrastructure(PKI). Regular nodes are not that efficient is handling the PKI as they are low on resources. This PKI would be an overload for a node and a time-consuming activity. Use of Implicitly Certified Public Keys(ICPK) works simpler and better for the nodes [7]. ICPK was proposed by Gunther as a variation for ElGamal Signature Scheme. The theatre and ground nodes key exchange scheme is established using the ICPK [7].

▇▇▇▇▇ Group Key Agreement for UAS-MBN

Tree keys are used for the group key agreement. The whole model works on a broadcast model. Group key management works on the hierarchical ternary tree [8]. Maximum degree of a tree is three. The top most node is the root and the bottom most nodes are called the leaves. A node can be a parent for two leaves or an independent node. Each leaf node corresponds to one group member. The depth of a balanced ternary tree depends on the number of group members in the tree. Group key agreement can be divided into member node, key node and a root node. Every cell in the tree becomes a member node including the MBN node. Initially group member is taken in as a leaf node. When the leaf nodes make a two-party or a tripartite key agreement

14

scheme with their neighboring member node a key node is generated. The final node at the top of the tree is represented as the root node [8].

2.3.4. Unmanned Aerial System-Collaboration Wireless Network(UAS-CWN)

Drones can be used in many hostile environments where a ground vehicle or a piloted air craft would not be able to reach. Advancements in technology and motors has resulted in better and faster unmanned aerial vehicles. In the coming years mass production of small sized drones is going to increase beyond measure. The current infrastructure to facilitate all the flying drones in reasonable and healthy communication environment stands as a question. Satellite uplink bandwidth would limit the communication of drones with the base station. Drones are coming up with a method to store data collected during flight and not to transmit it to the base station as and when. Instead they can store the data and upon reaching the ground station all the data can be retrieved. This type of procedure has security threats of its own, like loss of a UAS before reaching its destination. The goal of UAS-CWS is that it uses mesh topology. This topology ensures that there is no loss of data. In UAS-CWN every drone is considered a node [9].

In UAS-CWN every drone acts as a node. When a piece of information is broadcasted, that information is split into pieces using an algorithm called Information Dispersal Algorithm(IDA) [9]. These pieces of information are distributed to their nearest neighbors. Each node in CWN not only gathers information from the nearest node but also breaks down its own data into smaller fragments. The information becomes more complex if it is being split into many smaller fragments. Complexity increases the demand for security is higher. All the information that is being split and transported can be easily reconstructed back at the base station using a data decoder. Working of UAS-CWN is represented diagrammatically in Figure 7.

15
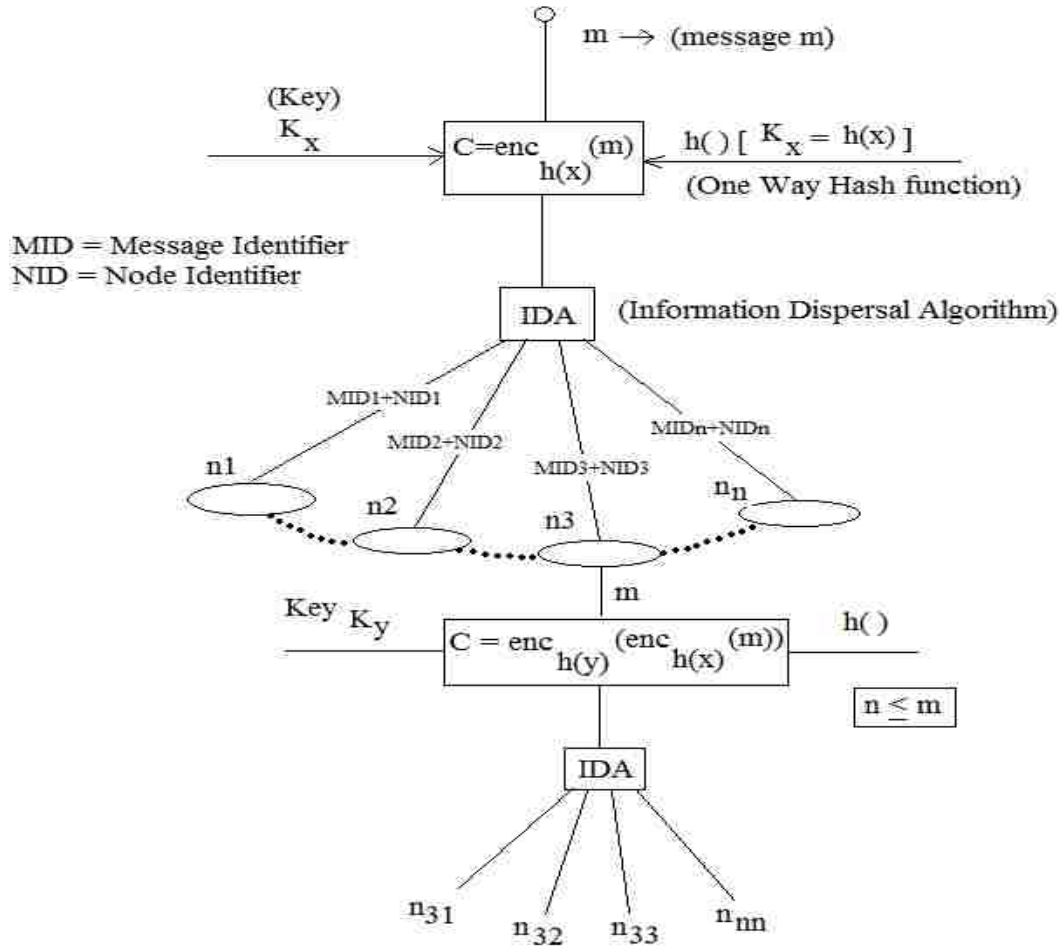
Figure 7: UAS-CWN using Information Dispersal Algorithm [9]

One-way Hash keychain is used when the information is collected by the drone. One-way hash ensures that no two slices of data have the same hash value. A public key and a private key are generated before the mission starts. These public and private keys are dedicated to that UAS alone. The public key for that drone is broadcasted to all the drones in the collaboration network. As soon as the data is received the drone applies the encryption to the data using its symmetric encryption algorithm. IDA is then applied to split the data. Before sending the data to its nearby UAS the data packet is signed to ensure safety [9].

CHAPTER 3: SECURITY IN UAS NAVIGATION

Importance for UAS has grown rapidly in the recent years. The usage of UAS not only for military purposes but also for civilian purposes has increased. Though UAS has made progress in the field of security in military services, civilian UAS have a long way to catch up. Providing security for commercial and civilian UAS is complicated because of the weak cryptography. UAS also depends on human maneuverability through weak communication links. UAS needs directional instructions to maneuver to a desired destination safely and accurately. Secure UAS navigation plays a vital role in achieving this goal. However, major weaknesses of a UAS such as small size, weight, weak computational power and high cost of implementing cryptographic solutions into the UAS result in a weak and insecure UAS navigation. Weak UAS can be attacked with minimal equipment and in a minimum time. The major motivations behind UAS is to hijack a current fully functional UAS rather than building a new working drone which takes time and money.

■ Global Positioning System (GPS).

Present day navigation infrastructure is rapidly becoming dependent on GPS technology. GPS plays a major role in civil purposes. GPS is also used in cell phone towers for precision and power grids to find out power line faults. Among the most critical users of GPS are paramedics and rescue teams. Relying on GPS helps get enhanced position and navigation accuracy [10]. The high dependency on GPS, for critical applications can leave humans vulnerable to security attacks. Drawback of GPS technology is that it derives its positioning solutions from low-power satellite signals, and these signals are most vulnerable to jamming. Military uses security solutions against jamming and have high end encryption standards to protect their GPS devices. Commercial GPS

17

devices do not implement the same security solutions for daily usage as they are too expensive and impractical.

GPS based navigation in military UAS is made safe by network level security measures and strong encryption standards. Civil GPS is considered to be vulnerable because of its weak signal strength [11]. There are solutions for making the GPS signal dependable by integrating the GPS receiver with inertial devices. These solutions help resist simple attacks but not prevent attackers who are meticulous and ambitious to spend enough resources to fulfill their tasks[12].

3.1.1. Security in GPS

One important factor of calculating GPS accuracies is to consider timing and synchronization of the GPS. However, if GPS accuracies are quickly restored, impact can be reduced but in the case of long outages, the risk could be potentially dangerous. One other way to avoid risks is by avoiding over-reliance on GPS devices. It is always important to have a backup system or procedure for many GPS applications. Organizations like JAMFEST offer free assistance in evaluating vulnerabilities of civilian GPS [10].

▰▰▰▰ Jamming

Jamming is achieved by sending signals in the same frequency but with higher power to jam signals. This forces the receiver to lose track of the GPS signals and opportunity to get spoofed is created. Jamming concentrates on blocking the signal. Building jammers are least cost effective and less time consuming.

■■■■■ Meaconing

The most important attack in civil GPS applications is called meaconing. Meaconing captures actual GPS transmissions and retransmits them after a short delay. This is an intermediate level attacks and not expensive to build

Table 2. The types of GPS attacks and its risks [10]

S.No.	Types of Attacks	Attacks
1	Unintentional Interference	Radio frequency interference, ionospheric interference and interference relating to spectrum congestion.
2	Intentional	Jamming, Spoofing and release of counterfeit signals
3	Human Factors	User equipment limitations, lack of training, over dependence on technology.

.

■■■■■ Spoofing

Main motto of Spoofing is to capture Position, velocity and Time (PVT) of the UAS. Spoofing has potentially proven to take over the UAS by aligning original GPS with counterfeit and taking control of the UAS. Unlike Jamming, spoofing not only blocks the GPS signals but also take over. Spoofing concentrates on disrupting the integrity of the navigation solution. Spoofing requires multiple antennas and its costly to set up. Three types of novel attacks are discussed below.

19

█████ GPS data level attacks

To produce good, bad or wrong data at higher levels like navigation message in real time. Spoofers are not capable of carrying out this attack. Vulnerabilities at this level exist due to the processing of navigation messages.

1) Middle of the earth attack(MEA): In this attack, attacker transmits bogus data to the receiver that the satellite's orbit is zero. Most of the receivers rejected the data except some. The receiver tries resolve the error by rebooting but could not and it enters an infinite reboot cycle. The receiver only recovers after manual reset of the full hardware [13].

2) Vulnerable Week Number (VWN): Date calculations in GPS consist of 10-bit week and 9-bit time of the week filed. Data can be altered into one past week and the ephemeris expires. At that time of the week can be manipulated [13].

3) Date De-Synchronization Attack(DDA): As Storage contains only 10 bits' possibility of roll over occurs every 19.7 years. When the internal clock counter reaches the maximum, it starts to decrement. This is due to the roll over event. Increasing the week rollover events increases the severity of the attacks [13].

4) Possible security Solution: During the attack the receiver goes into a reboot loop. If the receiver could be programmed to clear the cache this attack could have been avoided. Alterations to GPS week number are due to usage of cheap internal clocks [13].

3.1.2. GPS Spoofing

GPS plays a major role in our day to day lives. Though GPS plays such an important role in our lives, it has many security risks and threats. Its vulnerability to threats is mainly due to its

free availability. GPS signals are transparent and very predictable. Due to this weak nature of its signals, usage of GPS is very risky in UAS navigation. GPS also plays an important role that establishes real time positional awareness. Replacing GPS would be a very hideous and expensive task.

Spoofing a GPS single can be done using a spoofer. Making a spoofer is not in the range of an average person but depending on the motives, a person can use advancements in technology and signal simulators. A little effort and some financial funding are enough to make a spoofer capable of spoofing a moderate UAS. There are again many types of spoofer than can just jam a signal to inject a malicious signal to the transmission. Depending on the severity of the hack the price for developing a spoofer increases. Using a spoofer, counterfeit GPS signals can be injected which makes the GPS signal look like normal GPS signals. To identify is GPS has been hijacked, there are simple devices that can track detect if the UAS is being GPS spoofed.

Distance Measurement Equipment (DME)

This equipment measures the distance between the transponder and the UAS. This is a radar based technology used to calculate the propagation. When the UAS is travelling to a greater distance than specified in the route plan, DME records the propagation and alerts the controller accordingly. Some of the shortcomings of DME are that it is very costly and fails to detect the UAS if the size of the UAS is small.

Inertial Measurement Unit (IMU)

IMU is an electronic device that measure the velocity, angle, acceleration and attitude of a UAS. IMU's are installed in manned aircrafts and in UAS to detect and identify the situation and position of the aircraft or a UAS. An IMU consists of an accelerometer, gyroscope and a magnetometer. Recent advancements in IMU are its integration along with GPS. GPS inputs are

21

combined with IMU measurements to verify the correctness of the readings. IMU detects a sudden change in UAS maneuvers, velocity and direction. If the direction is unintended, immediately the operator is notified through a safe communication channel about a possible spoof attack. IMU also helps a UAS to maneuver safely in tunnels and buildings where there is a loss of GPS signal. Shortcoming of the IMU is that it will not be able to detect minor changes in angle or velocity. A slight degree of angle shift in flight over a long period can get unnoticed. This degree of small tilt for a long period can completely alter the route of the UAS and lead to a different destination which can lead to the UAS hijack. To avoid this kind of spoofing, IMU measurements are cross verified with GPS readings in a GPS-IMU integrated device.

▬▬▬ Dead reckoning

Dead reckoning is a process of identifying your own position periodically in regular intervals of time. If in case of a spoof attack, by the method of dead reckoning we can identify if the UAS has travelled in a wrong path or if the direction of the UAS has changes abruptly. The shortcoming of dead reckoning is that the time interval needs to be in proportion with the amount of distance travelled. If the time interval is too less, dead reckoning may not identify a change in the UAS route plan.

▬▬▬ Jamming to Noise Sensing Defense

A microcontroller made to sense the power band can installed near the front end of the GPS receiver. This microcontroller compares the total received power on the band of threat possibility. This operation is simple and very cheap compared to other mechanisms. The shortcoming of this set up is that it cannot detect any signals that are coming at a greater power than its counterparts [14].

22

■■■■■ Spread Spectrum Security Codes

High rate security codes used for communication are called spread spectrum security codes. Generally, these codes are spread with a frequency that result in a spread, which in turn increase the bandwidth. This technique is used to increase the security of communication so that communication signals are not prone to jamming and distortion.

3.1.3. GPS and INS sensor fusion

Motion status of a UAS can be obtained using Inertial Navigation System(INS) and Inertial Measurement Units (IMU). The IMU and INS provide acceleration and velocity information of the UAS Microelectromechanical systems (MEMS)helped in designing more compact and low power consuming sensors [15]. These sensors are now being used in IMU's and INS. As it is a known fact that low cost sensors decrease the quality of the IMU's and INS, software updates, data processing and feedback looping were introduced to obtain better accuracies. Acceleration components in an IMU are measured by the accelerometer. The accelerometer is fixed on a rotation table. The calibration device attached to IMU can rotate into 37 different positions starting from 0 degree to 180 degrees.

Performance of a UAS depends on multiple and numerous small on board sensors. Small UAS need a simple and least expensive solution as the inertial sensors are expensive. The GPS/INS sensor fusion overcomes these constraints [16].Inertial sensors suffer from providing a solution to the drift in the UAS navigations. Any air navigation with an air drift of 1°/hr. is very expensive [16]. A typical GPS/INS sensor consists of 1-axis gyroscope, one 3-axis accelerometer, one GPS receiver and a digital signal processor [16].Gyroscope read outs are calculated in complex number systems that are called quaternions. The gyroscope is used to calculate the turns made by a UAS in quaternions. Attitude of the UAS when in inertial frame is

23

calculated by the multiplying the quaternion's and attitude of the UAS in navigation frame is calculated by dividing the quaternions at any given time. The accelerometer output's which are the velocity and the position are calculated based on the gravity acceleration vector. Vehicle's position and velocity vector are calculated by using the Strap-Down Inertial Navigation algorithm [16].These resulting values are considered as the initial values so that the cycle can be repeated till the end of the navigation mode.

The performance of the UAS depends a lot on the on-board sensors and systems. Small UAS need on board sensors with light weight and small size. One of the system designed for small UAS is the Global positioning system/Inertial navigation system (GPS/INS). This system has been developed with the use of multiple GPS receivers and sensors which provides better results than a single GPS receiver. Low cost precise inertial sensors are used in GPS/INS fusion [16]. Low cost GPS/INS sensor is provided with a positon precision of 5m,attitude precision within 10°-15°, weight of the whole system is less than 5 kilos and data rate is always greater than 19600 bits per second [16]. In case of an aggressive maneuver, there is a probability that the GPS sensor might provide wrong location specification. To avoid this error multiple GPS sensors are installed in this system. GPS/INS system consist of a gyroscope, a 3-axis accelerometer, GPS receiver with multiple antennas and a digital signal processor (DSP) with memory as shown in Figure 8. Below diagram shows the GPS/INS unit.

The GPS/INS correction algorithm uses the Kalman filtering technique to determine the estimation error [16]. Kalman Filter is an algorithm that uses a series of measurements that calculated over time containing values and inaccuracies. Kalman filter is a linear quadratic expression and an algorithm used to calculate a series of measurements and inaccuracies to provide an estimate of unknown variables. Kalman filter is used in navigational vehicles such as

24

aircrafts and space shuttles. Kalman filter is good at prediction of navigational behavior of an aircraft only in linear expressions and fails in nonlinear. Extended Kalman Filter provides a solution for the nonlinear variables but not completely.
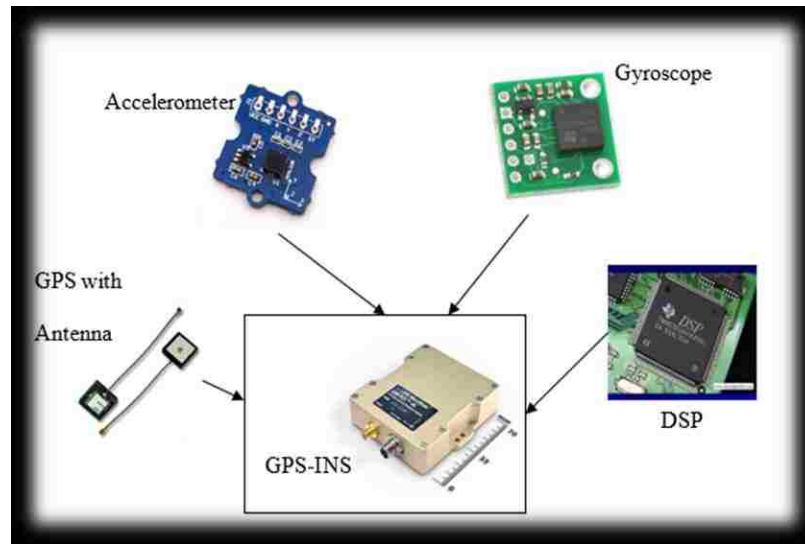
Figure 8: Sensors inside a GPS-INS unit.

. GPS/INS has an extensive use in providing a solution for the complex navigational algorithm. The filtering formulation called state-dependent Riccati equation(SDRE) is combined with the GPS/INS fusion to provide better results compared to Extended Kalman filter [17]. GPS/INS plays a major role in providing a better calculation for complex aerospace problems. GPS/INS along with SDRE gives a precise and closer location accuracy for UAS [17]. GPS/INS fusion is diagrammatically represented in Figure 9.

Traditional Radar system

A Traditional radar is a system used to detect unknown objects at a distance. This system emits radio signals to calculate angle, range and velocity of an object. This system is commonly used in ships, aircrafts, weather services etc. Radar stands for Radio detection and ranging.

Extensive research was made in the field of radar systems during the second world war. During the world war this system was used to detect an un authorized aircraft flying into an unauthorized territory. After the world war, radar system was brought into civil aviation.
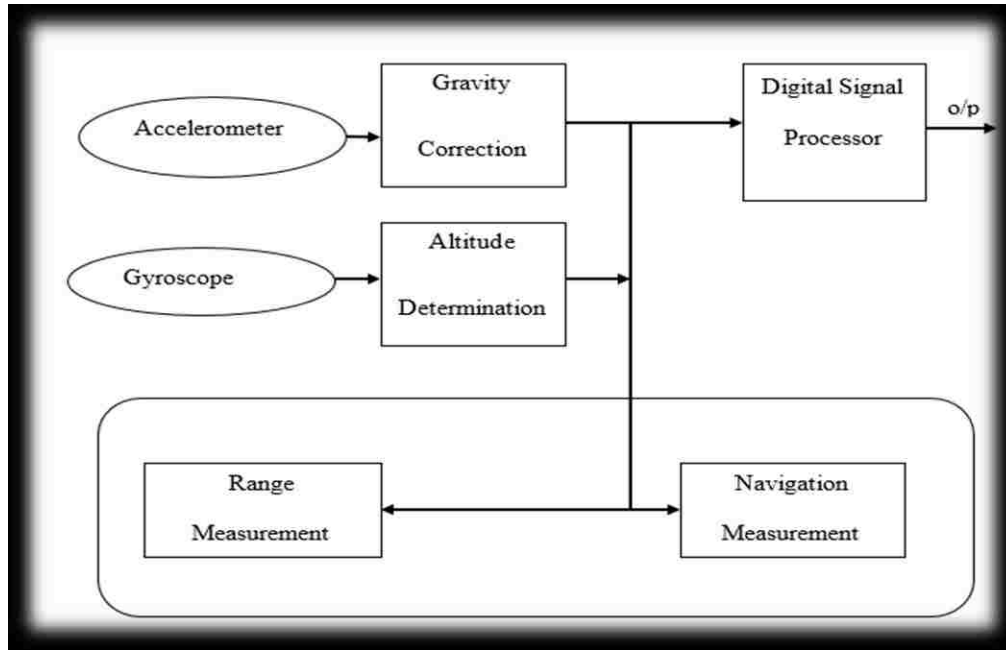
Figure 9: GPS-INS fusion schematic

Over the years, a lot of improvements have been made to the radar system to set a safe and secure standard. In the aviation industry, radar system is used to calculate the aircraft position and speed of an aircraft. Communication between pilot and the control center is established using ground-to-air and air-to-ground radio system. At the ATC, the radar ranges from 40 to 50 miles whereas the radar fixed on the aircraft ranges approximately 20 miles. Though radar plays such an important role in aviation, it has some limitations. Limited range and the increased air traffic has pushed the aviation industry to look for more sophisticated and simpler options. Installing several radar systems to cope with the high air traffic requirement could prove very costly.

26

3.2.1. Security in Radar Systems

Traditional radar systems can not only be used to track and surveil manned aircrafts but also UAS. Traditional radar system is large, costly, outdated and can prove inefficient in many ways unless modified as per the UAS requirement. Radar systems used to detect manned aircrafts cannot detect UAS because of their small size and quick maneuvers. Radars combined with other sensors can help detect UAS.

Radar systems should be compact and very light weight to be installed in a UAS. By reducing power and range, the weight and cost of the radar will be reduced to fit into a UAS. UAS are a minimum of ten times smaller in magnitude compared to the manned aircrafts which makes it very difficult for an active radar system to detect and identify a UAS. Fusion of radar along with camera, infrared sensors, GPS, ADS-B and other surveillance devices makes it easier for a UAS to be detected precisely on a radar. Active radar systems are easily prone to discovery by an adversary compared to camera or infrared sensors [18]. Disadvantage of infrared sensor is that it cannot be detected in severe weather obstructions whereas radar can outperform infrared in those same adverse weather conditions. On board sensors and processors help radar system to identify moving target and establish a surveillance radius of up to 15Km [18]. On board processors help reduce the mega bits of data to convert into kilo bits of data to be transmitted without any burden on the UAS. To overcome the jamming threat, narrow bandwidth is used for communication instead of wide bandwidth. Capacity of the radar for UAS is 1355 Watts, weight 175 pounds and altitude of 3Km [18].

27
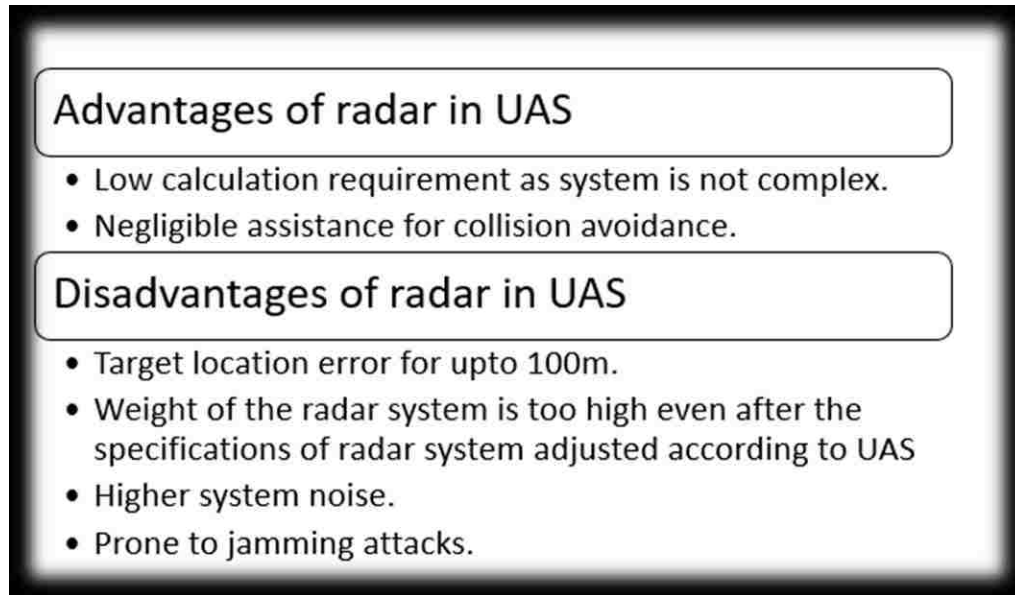
Figure 10: Advantages and disadvantages of radar system in UAS [18][19]**.**

3.2.2. Radar Fusion with ADS-B

The radar system was developed during the period of second world war. Radar system has seen very few technological advancements from then. In the future scenario where accuracy and precision for increasing air traffic, radar system is a step behind. In high air traffic scenarios installing more powerful radars can be very costly. In the future, implementation of self-separation schemes for collision avoidance is tough as radar lacks accurate and precise surveillance location of the object. Therefore, for a better and safe future in aviation, Air Traffic Management (ATM) plays a very important role in Navigation communication and surveillance.

28

ATM is not just trying to provide a solution for the radar systems but a complete solution for the aviation industry by combining different surveillance sensors, radar and GPS.
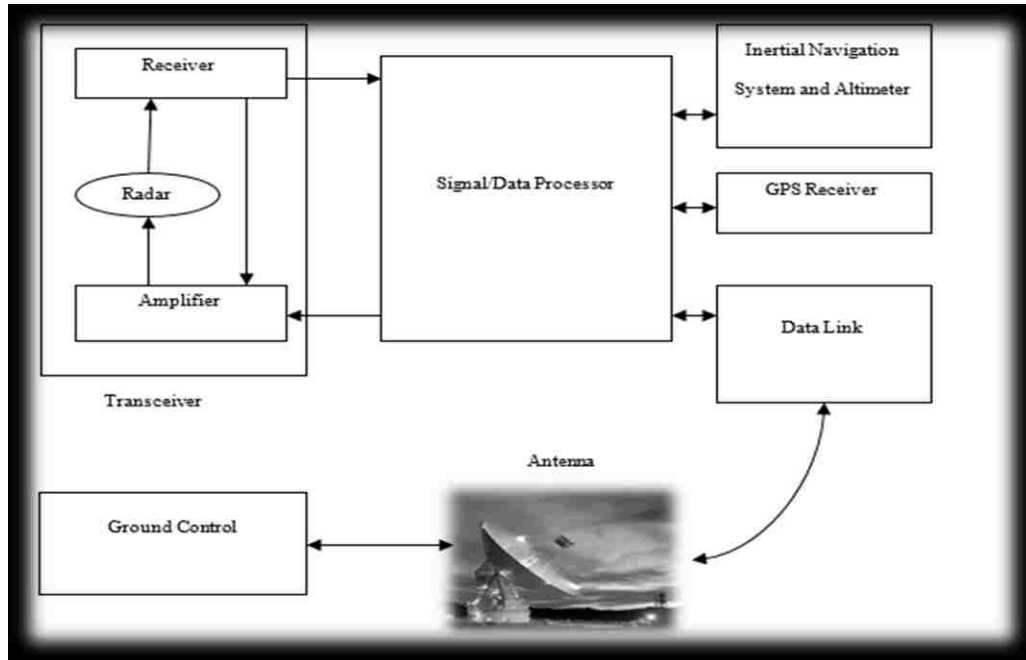
Figure 11: Radar fusion for ADS-B Navigation solution.

Different sensors give their own readings on the location of the aircraft. The output of one sensor alone cannot be fully trusted. There always might be a chance for error. In these cases, ATM relies on different sensors verify each other's outputs to remain on the same technical readings. The sensors and the algorithms work together to determine and eradiate position estimation errors by cross verifying each other's outputs. There are two types of data fusion called the centralized and the decentralized data fusion. In centralized data fusion, a combination of all the sensor measurements are taken into a common calculation than just one sensor measurement. The sensor measurements are sent to a central processor in the centralized architecture. This centralized mechanism calculates estimate of the current state of the aircraft

29

and reevaluates each sensor output through Kalman filter. In decentralized data fusion, sensors operate and perform calculations based on their own algorithms. These reading estimate the measurements of the first state of the aircraft and save the results in the memory. The central data processing unit receives all the individual measurements from each sensor individually. This helps the decentralized mechanism calculate a better accurate state [20].

▰ Collision Avoidance

3.3.1. FLARM

FLARM is a device used in aircrafts for collision avoidance. This device typically consists of a barometer and Internal GPS. After receiving the attitude information from the aircraft its broadcasted information is compared with the forecasted information. If the angle of elevation of the cliff or the terrain is same as the forecasted terrain, then an alert is issued about the possible collision. One drawback of FLARM is the route needs must be pre-planned. If there is a deviation in its route plan, FLARM will not be able to identify a terrain as the details of the terrain or the cliff are not forecasted.

3.3.2. Portable Collision Avoidance System(PCAS) and Traffic Collision Avoidance System (TCAS)

Portable Collision Avoidance System (PCAS) is a passive version of the Traffic Collision Avoidance System (TCAS). TCAS interrogate transponders of nearby aircraft and avoids collisions. PCAS listens to the nearby transponders and informs the pilot about a possible collision. TCAS system sends an interrogation signal which is a broadcast signal. This signal is received by the nearby UAS and replies with its position, coordinates, elevation, speed and other aircraft attitude information. This information is relayed back to the Air traffic control station

30

(ATC). ATC listens to all the communication and transmits the flight information of the nearby aircrafts within 5 miles' radius of UAS.

CHAPTER 4: AUTOMATIC DEPENDENT SURVEILLANCE – BROADCAST (ADS-B)

Automatic Dependent surveillance – Broadcast is an aircraft tracking and broadcast system. ADS-B is one of the most promising surveillance technology of the future. ADS-B is a surveillance system used for air traffic management and control. ADS-B is going to play a major role in the future as approximately two billion passengers would be benefited from 2020. Meaning of ADS-B is described in Figure 12. ADS-B was developed to replace the traditional radar system. Both Air Traffic Control Center(ATC) and pilot use this technology as it is very good at procedures and air to air surveillance. ADS-B broadcasts unencrypted plain text messages over the radio approximately one per second. Though this technology is widely being used and accepted by many countries around the world, some technological improvements are needed. Improvement is required in the fields of data transmission, applications and security. Statistical aircraft manufacture data shows that, in 2013 70 to 80 % of the aircrafts have been already fitted with ADS-B transponders [21].

The main feature of ADS-B is that it will allow the aircraft to broadcast its position, velocity and intent to other nearby receivers[22]. ATC and the aircraft can maintain the same information detail with the help of ADS-B. ADS-B broadcasts flight information to any listening entity. As air traffic is increasing at a demanding rate, the data links that carry the ADS-B broadcast information need to increase their bandwidth to accommodate more flight information in the broadcast message. The data link needs to be developed for the future needs which can focus on developing a secure and dependable data link for transmission. ADS-B also uses GPS as its main source, though GPS itself is considered very vulnerable. ADS-B started using an

extended squitter which would reduce the passive interrogation where messages would exchange too frequently. Squitter can be used for better performance during high data traffic and will ensure efficiency.
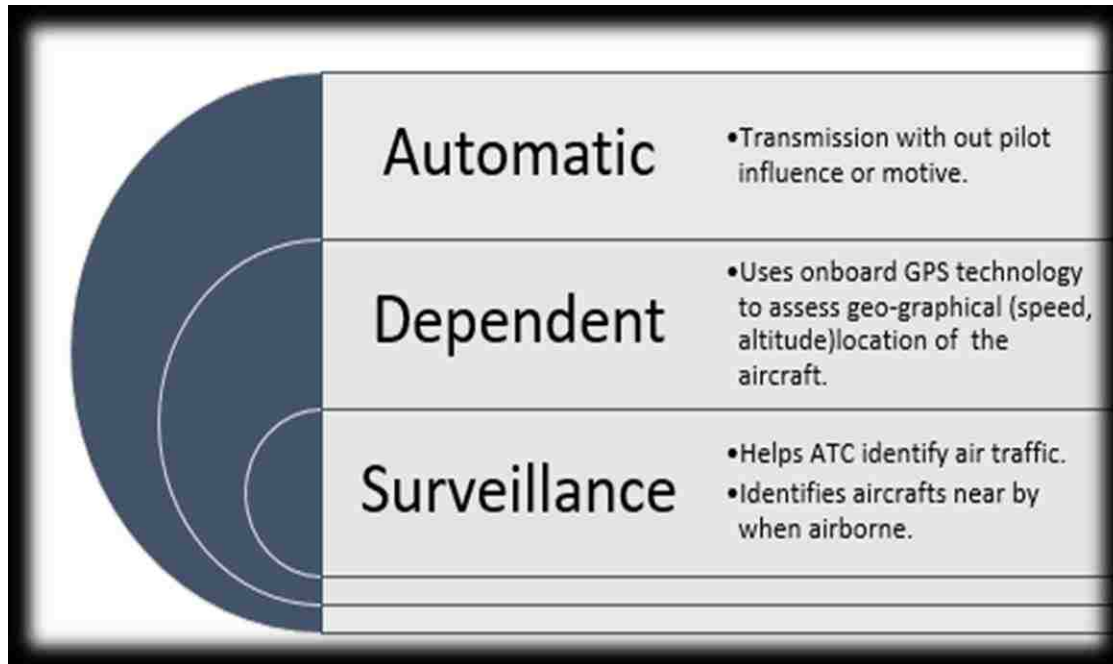
Figure 12: ADS-B meaning and uses.

Birth of ADS-B

Traditional radars were used to identify an aircraft and communication from ATC to the aircraft was made through the Mode -S transponder. Mode S transponder was developed for better accuracy of the aircraft position, identification and location. Initially Mode-S transponder was used to communicate for interrogation and reply. Recent modifications to Mode-S have increased data capacity for extended reply structure for better surveillance. Mode-S not only helps in better communication but also helps with good flight awareness. Mode-S includes both air to ground and air to air communication. Continuous enhancements to Mode-S were made to make it better. Advancements were made to accommodate the geographical location using GPS

satellites. That was when ADS-B was developed to provide enhanced communication using GPS and other combined flight data to predict the flight path and its continues tracking [23].   ADS-B is divided into two sub systems namely ADS-B In and ADS-B out.

4.1.1. ADS-B Out

ADS-B Out is the transmitter that transmits positional and directional data of an aircraft. ADS-B out has the capability of transmitting aircraft identity number called ICAO. This information if sent to the satellites every second which then returns to all the ground stations. ADS-B out ensures that the data is being transmitted systematically and periodically. FAA mandates all aircraft should have an ADS-B out by the year 2020.

4.1.2. ADS-B In

ADS-B In is device which receives and display the nearby flight information that have been transmitted by ADS-B Out. Along with useful flight information ADS-B In provide the pilot with weather and traffic position. ADS-B In graphically displays the nearby aircrafts to the pilot. ADS-B In is currently not being mandated in aircrafts by FAA. In future when ADS-B in is equipped with a long range detection, it allows the aircraft to engage in self-separation techniques which would play an important along with the sense and avoid techniques [24].

4.1.3. Traffic Information Services - Broadcast (TIS-B)

TIS-B is a service that is equipped with both ADS-B In and ADS-B Out for surveillance purpose. TIS-B provides positional information about airplanes that are not equipped with ADS-B. For TIS-B to detect the aircraft that is not equipped with ADS-B, it needs to have a functional transponder that is in the radar coverage.

4.1.4. Flight Information Service – Broadcast (FIS-B)

FIS-B is a service that provides astronomical and complex mathematical data of the flight through radio station. This service is transmitted on the UAT frequency [25].

▄▄ ADS-B Applications

ADS-B is designed in such a manner that it can transmit flight information to the ground station. The details broadcasted by ADS-B are flight identification location which include latitude, longitude and elevation, velocity and most importantly intent of the flight. By Increasing security and increase of data link capacity, responsibilities like collision avoidance, conflict detection and situational awareness can be handed over to ADS-B [22]. By determining the velocity and flight maneuvers, operator in the ATC tower will be able to determine if the flight is in correct route path or has incurred an unexpected change in route. If a flight has a problem with receiving new directions from the ATC through voice, ADS-B can be used to convey the new directions without talking directly to the operator at the ATC.

ADS-B helps determine latitude, longitude and altitude instantaneously to the ATC, which help detect conflict and avoid them before they become unavoidable. With the help of ADS-B 4D trajectory, information can be determined and transferred from and to autopilot. The position of the flight is broadcasted to all nearby hearing devices so that if in case two aircrafts overlap on the same flight path, they can negotiate a new plan securely and safely before complications. Some of the most critical flight operational information's are transmitted manually, by increasing the data link capacity of ADS-B. Additional features like encryption and access protocol can be included if the data link capacity can be increased in the future [22].ADS-B has also made a significant contribution to NAS by carrying information about nearby flights, weather and terrain information.

35

The traditional radar system has low resolution and accuracy. If the airplane is at a longer distance the traditional radar system is not accurate in giving the exact distance from the aircraft to the ATC. The most important disadvantage of traditional radar systems is that they cannot find the height of the aircraft when it is traced at a certain long distance. ADS-B has taken over traditional radar system in the recent times. ADS-B also has a range of about 100-200 miles [26].

ADS-B Data Capacity

ADS-B uses two-state modulated signal for a better performing data rate. The limitation of the message rate is that it can transmit only once per every second. The data rate is divided into three segments; two segments are for the aircraft message and the other is for ground message. The two aircraft messages are called the short message's consisting of 144 bits and the long message consisting of 272 bits. Ground uplink message is used to uplink messages to the aircraft from the ground station. The transmission is divided using time frames. The time frames are 176 milliseconds for ground segment and ADS-B message consisting of 800 milliseconds. These time frames are internally divided into message start opportunities (MSO's). MSO's do not ensure that a message would be delivered without any collision. That is because the time between any two MSO's is shorter than the length of the message [22].

The future enhancements would be to increase the data capacity. By increasing the data capacity instead of a two-state frequency modulation, a four-state frequency modulation would ensure higher bandwidth ranges. Exchange of keys using encryption algorithms, 4D trajectories and larger information about flight data would be possible to transmit with increase in bandwidth. Randomly operated MSO's create a message collision which reduce the message bandwidth or even the participants who want to transmit. When operated in a time slotted

36

manner the messages have lesser chance of collision which increases the bandwidth. When there are not many participants who want to transmit, a single participant can transmit many times to use up the additional bandwidth space created with the help of time slots. To transmit a message in a time slotted manner the participants listen to other participants. ADS-B messages self-assign their time slot. This self-assignment of a time slot helps minimize message collisions. Aviation industry has opted to go with two options relating to ADS-B message transmission. First is the self- assigned time slot system and second is the ground station slot assigned system. The self-assigned time slot system works very good in less air traffic conditions. In lesser air traffic conditions, the messages collisions are very minimal. In cases of large air traffic in places like cities self-assigned time slot will not work properly as many participants will not be able to find an empty time slot. In the second case a ground station would help every participant receives equal opportunity to transmit. The main duty of a ground station is to avoid message collisions and ensure free flow of message traffic [22].

ADS-B has data rate of 1Mbit/sec and is a pulse position modulation (PPM). The ADS-B data blocks are either 56bits or 112 bits[26]. The data links that are suitable for ADS-B are 1090MHz Extended squitter and Universal Access Transceiver(UAT)[26]. 1090Extended Squitter(ES) is a data link which uses 1090MHz frequency. This 1090ES is used communicated with other aircrafts as well as the ATC or GCS. ADS-B signals can be integrated with traditional Mode S transponder. The data blocks are transmitted using the pulse position modulation(PPM) with time slot being one micro second [21]. Mode S transponder has two different types of data lengths one is the 56 bit one and the other being the 112 bit. ADS-B choses the 112 bit.

Figure 13 shows the ADS-B message format. CA bit carries information of the transponder, DF carries the type of message being sent, AA field carries the International Civil

Aviation Organization(ICAO) code and PI carries the CRC error codes. The ICAO is a unique flight identification number. ME 56 carries the actual data that needs to be carried over. It contains the flight information, location intent and other important flight related information's. ME 56 also has a security and encryption for secure transmission [21].

The message format for ADS-B is shown in the below diagram 13. Downlink Format (DF) specifies the type of message. Generally, DF is 17 for Ads-B. There is also a message subdivision(CA) associated with DF. ICAO contains the address of the aircraft or the aircraft identification number. The data frame (DATA) consists the actual ADS-B flight information. Type Code(TC) resides in the beginning of the data frame. TS field specifies that is inside the data. Decoding the flight data from the ADS-B is not simple. The latitude and longitude formats are not directly present in a readable format. The positions of the aircraft are reported in compact position reporting (CPR) formats. CPR helps reduce the message into a fewer bits and maintain the high resolution. Parity check(PC) is same as a checksum. Parity check uses cyclic redundancy to verify the exactness of the received messages.
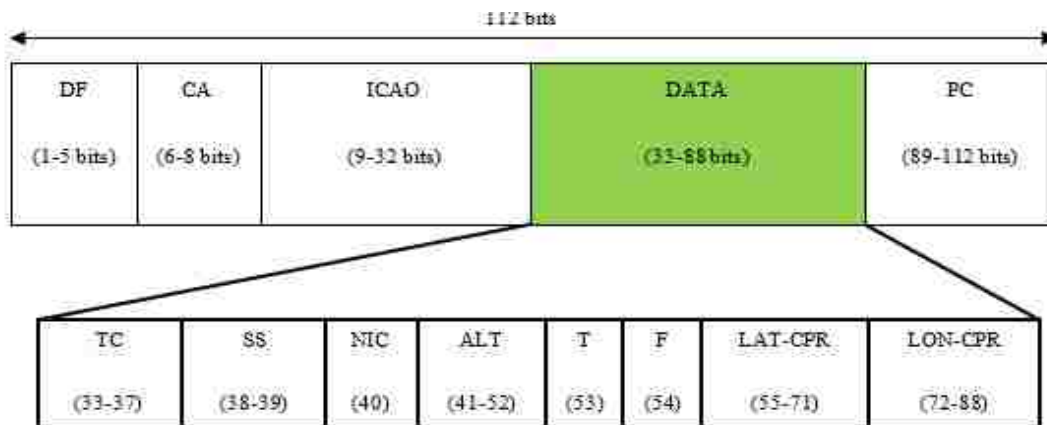

Figure 13: ADS-B data message capacity.

■ Security in ADS-B

ADS-B has turned out to be the most important and reliable option for commercial aviation. Though there is a high demand for ADS-B there hasn't been a worldwide implementation of this technology because of the lack of security measures and due to its vulnerability.

4.4.1. Background

Previously, before ADS-B was introduced Primary surveillance radars (PSR) and Secondary surveillance radar(SSR) were used for flight surveillance. PSR was used earlier where radar signals were transmitted and reflected from the aircraft to find out its distance and positional data. SSR is still in existence where the transponders are fixed to the aircrafts and communicate with ATC. PSR is being replaced with SSR integrated with ADS-B because of its low deployment cost and better accuracy. Communication with ATC takes place via transponders which receive and transmit flight information to ATC. Initially Mode-A and Mode-C were used as interrogation signals but now Mode-S is being used for ADS-B. We can say that ADS-B is an extension of SSR [26].

ADS-B operates at two radio frequencies at the physical level, they are the active interrogation and active response. The active response is also called normal broadcast. Active interrogation operates at 1030 MHz and active response operates at 1090 MHz respectively[26]. Two types of datalinks used for data transmission are 1090 Extended Squitter (ES) and the Universal Access Transceiver(UAT). UAT is used for general aviation whereas 1090ES is used for commercial aviation[21]. The ADS-B has two important architectural components; they are the ADS-B OUT installed in the aircrafts and the ADS-IN installed in the ATC tower.
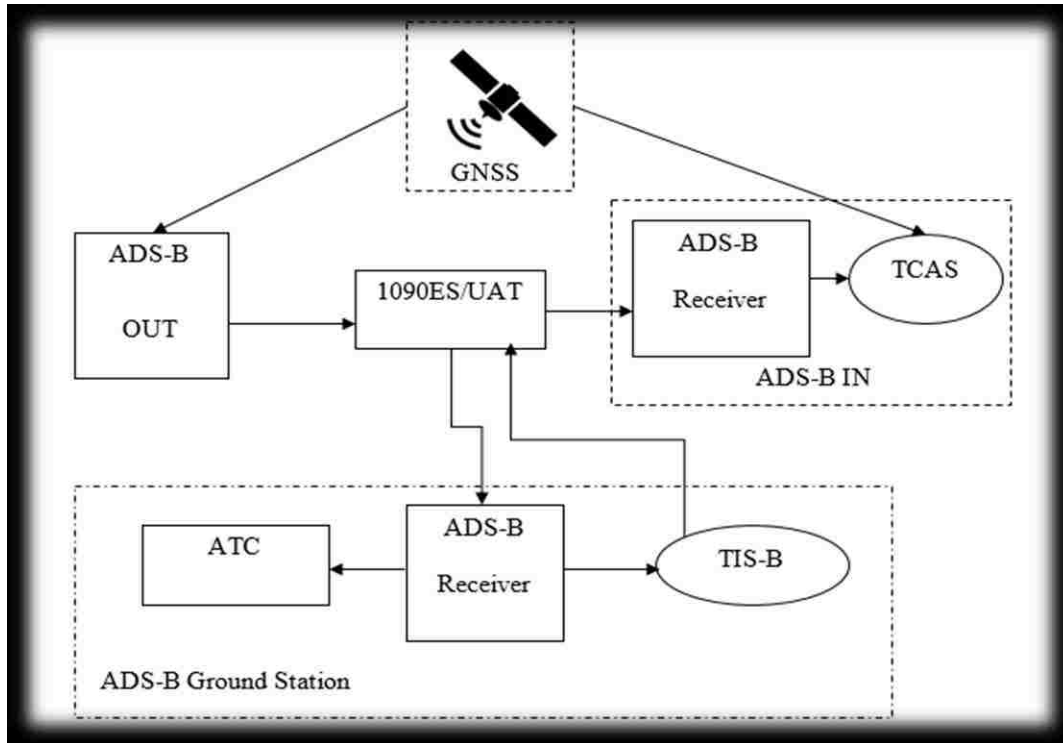
Figure 14: Working of 1090Es/UAT along with ADS-B

Both ADS-B OUT and ADS-B IN are used for aircrafts situational awareness. ADS-B retrieves its own aircraft information from GPS receivers and broadcasts them out through ADS-B OUT. ADS-IN is used as the receiver at the ATC or the ground station to receive information like flight intent, Id position and other important information[21].ADS-B IN is currently not installed in aircrafts as it is in testing phase. If ADS-B IN proves successful, as it would be used for flight spacing and separation operations.

4.4.2. Possible Attacks and Threats on ADS-B

The major concern with ADS-B is that it does not have any security mechanisms in place. Lack of authentications and encryption lead to tampering and unauthorized messages.

Eavesdropping

Unauthorized listening of conversations between two entities or even a group is called eavesdropping.   Lack of encryption and transmission of unsecured broadcast messages leads to eavesdropping in ADS-B. Eavesdropping also acts as a basis for other practical attacks. Eavesdropping is very difficult to detect and also impossible to avoid without encryption [21][26].

Jamming

Any device that blocks or interferes with communication signals is called a jammer. Jammer is the reason for jamming the signals. Lack of Authentication and message signatures makes it easier for ADS-B signals to get jammer [26]. Weather it is a single node or multiple participants in a field, all are prone to jamming. Receiving and sending of messages would get blocked if enemy sends high power signal on the 1090 MHz frequency. Traditional primary radars were easily prone to jamming compared to rotating antennas. Jamming always targets the receivers and not the transmitters. Targeted attack is called reactive jamming and this attack leads to Denial Of Service Attack [21][26].

Spoofing

To replace a reliable communication established between two devices with a false or mock signals. Lack of challenge response and lack of encryption lead to spoofing of ADS-B signals [26].

Replay attack

A message is purposefully replayed with a fraudulent message or in some cases delaying message delivery. Lack of challenge response in ADS-B leads to relay attacks [26].

◼◼◼◼◼ Message Manipulation

Modification of messages at the physical layer is called Message Manipulation. Attackers send high powered signals to change the message data. Bit flipping is a technique of changing 1's to 0' and 0's to 1's. Bit flipping attacks are possible for message manipulation. Lack of message authentication and privacy in ADS-B leads to message manipulation [21][26].

◼◼◼◼◼ Message Injection

Injection of a corrupt message into the air traffic communication system is called Message Injection. Message injection takes place because of lack of authentication at the data link layer [21].

◼◼◼◼◼ Message Deletion

When messages are deleted from a wireless medium they are called Message deletion. There are two types of message deletion techniques, one is the destructive method and the other is the constructive method [21]. Destructive method refers to transmitting inverse interference signal broadcast which erases the messages. In constructive, Large number of bit errors are created which is beyond the CRC correction. In this case message gets dropped as it thinks the message is corrupted [21].

4.4.3. Security Enhancements and recommendations for ADS-B

ADS-B is secure in military application as the whole transmission of ADS-B is used on a single entity. Where as in the case of civilian aircraft, the usage and population density is wider which provides a greater risk compared to military ADS-B. ADS-B device can be configured by the user before using it. At the time of using, through ADS-B device personal messages can be transmitted which are not related to ATC or ADS-B. This random rouge message can lead to

confusion either in the ATC tower or the pilot who is referring to these ADS-B codes. As pilot

main goal is maximum aircraft safety, prank messages could lead to confusion [26].

Figure 15: Security threats based on location, position and goal..

■■■■■■ **Secure Broadcast Authentication**

Secure broadcast authentication works well with ADS-B because ADS-B uses

unidirectional broadcast. Asymmetric property is preferred in ADS-B rather than symmetric

because, symmetric performs better in point-to-point communication because both parties trust

each other. ADS-B is a broadcast and it is very difficult to authenticate. Asymmetric mechanism

helps ADS-B keep its open nature alive. In asymmetric mechanism, receiver can verify messages

but cannot randomly generate messages to broadcast. Secure broadcast authentication ensures

that it is only used when a threat is detected and not each and every time to reduce the stress on

ADS-B [21].

■■■■■ Public Key Infrastructure

Cryptographic methods are a success in the wireless communication networks. Therefore, cryptographic methods are being tested on ADS-B, but had no success as on date. If ADS-B is encrypted, the same keys need to be distributed to all the ADS-B participants. The list of participants can be huge depending on the location at which they are trying to cover. Even if the keys are to be distributed in a small location, keys must be distributed to aircrafts and ground stations which could be time taking. Other most important backdrop is that keys need to be updated frequently which will increase the complexity and reduce the message traffic. Apart from ADS-B there are other data links that help establish communication between pilot and ATC, one of commonly used one is controller-pilot data link(CPDL). Key management can be done using CPDL and support symmetric cipher which work well with non-standard block sizes like ADS-B data link which uses 112 bit messages. The secure communication of CPDL is still a challenge and if in case the CPDL is blocked, there is no alternative for a safe method of sharing keys. Key management can put an additional load on the capacity of the datalink, as there is already heavy traffic through the 1090MHz frequency. Looking at the problems of key management and key sharing, PKI is a better option. One of the other solution is, use of authenticator ground station which has a challenge- response problem. The authenticator GCS needs to maintain a database of all globally used security keys, which is practically a very difficult and risky task. Elliptical curve cipher on ADS-B and UAT could prove beneficial. Key sizes and bandwidth are taken into consider for this proposed solution. Although UAT can transmit loner messages than the 1090ES, its message format needs to be changed for this cipher implementation. If the same implementation is applied on 1090ES, MODE S standard would require 5 more messages to get the signature data and the time stamps accommodated. 1090ES is

44

already crowded and with this solution implemented, there is every chance that the 1090ES could get too crowded. FAA once recommended the use of centralized key distribution, where FAA would manage the role of Certificate Authority(CA). Playing the role of CA is not easy. Even if the FAA would manage to get the CA working, there would be a problem of communication from aircraft to authorities and communication between one another.

Short and long term ADS-B transmission equipped with lightweight PKI, is a quick solution for the above-mentioned problem. Light weight PKI can be adjusted per the bandwidth of the broadcast medium. One trusted ADS-B device should be made a secure device for verifying certificate Authority(CA) chains using PKI. With the help of one trusted ADS-B device random message injections can be avoided. A series of ADS-B messages are transmitted to the nearby ADS-B devices so that they can verify the signature. If in case all the messages were not received the ADS-B, those messages would be saved for later verification of the signature [26]. Looking at all the above security solutions for ADS-B, PKI remains closer to achieving the goal when compared to other cryptographic methods. Though the conclusion of the above made discussion points out that providing a secure 1090ES for ADS-B communication is challenging.

Different cryptographic solutions were tried on ADS-B but none of them was successful. Table 3 shows different cryptographic methods that have been tried on ADS-B and their result. First Step was to distribute same encryption keys, which is a very complicated and a big task. The key management problem can be solved by sharing the keys through a secure communication link. The communication link that can be used is the controller pilot data link communication(CPDCL). For Light weight PKI to get implemented needs to combine many messages together for a complete signature.

45

Table 3: Cryptographic methods tested on ADS-B.

Method	Result
Distribution of same encryption keys.	Insecure to Inside and outside attacks.
Key management Problem	Controller Pilot Data Link Communication (CPDCL).
Challenge-Response	World wise data base of secure keys is not possible.
Light Weight PKI	Combining N messages for signature.
Centralized Key distribution. FAA as a CA.	Many Aviation Authorities Worldwide.
One Time Key Signature	Infeasible

████████ **ADS-C**

A very frequently asked question was, why not replace ADS-B with ADS-C. Although ADS-C has connection oriented security procedures in place, drawbacks of ADS-C are as follows[21].It has a lack of Aeronautical Telecommunication Network(ATN) and Air Navigation System (ANS). ADS-C is cost effective and cannot communicate directly with other aircrafts [21].

CHAPTER 5: ADS-B FOR SMALL UAS

Small UAS are UAS that weight less than 55 pounds. Small UAS are limited in their capabilities. Small UAS always must maintain line of sight and must remain close to the person manipulating the flight controls. Person operating the small UAS must be stationary at the ground always and should not be situated in a moving vehicle[27].

Long range traditional radar systems used to detect regular aircrafts cannot be used in case of small UAS because of the comparatively smaller size and lower power of the UAS. Therefore, alternative surveillance options such as ADS-B has gained prominence in the recent years. A future forecast estimates that ADS-B will play a key role for collision avoidance in UAS by the year 2020. ADS-B uses satellite data to calculate important flight information and send it to the ground stations. Many collision avoidance algorithms use this data to calculate the nearest neighbor flight information which can be used to detect and avoid collision in small UAS. ADS-B also transmits additional information such as systematic tracking and weather data [28].

5.1.1. Sense and avoid systems (SAAS)

As per Federal Aviation Administration (FAA) guidelines, pilot's eye sight is still a key component of SAAS in sensing and avoiding mid-air collisions. Per FAA statistics, one of the major reason for mid-air collisions is pilot's inability to locate the colliding flight. In recent years, SAAS have played a major role in manned aircraft by reducing the burden on pilot to manually look out for nearby collision prone flights. Major collision avoidance schemes were introduced into manned aircrafts in the year 2005. By 2020, FAA's NextGEN-Controlled airspace aims to provide a solution for both manned aircrafts and UAS to share and fly safely in

www.manaraa.com

the National Air Space (NAS). Research to implement SAAS in medium-sized UAS has been progressive. In the case of small UAS, research on implementation of SAAS is very minimum. In 2005, major advancement in the field of SAAS for manned aircrafts were made with the invention of Traffic Collision Avoidance System (TCAS). TCAS has made considerable progress on how it can be adopted to different sizes of UAS systems. According to Haessig et al. [23], the NextGEN-Controlled Airspace is going to implement a more advanced system similar to TCAS known as Airborne Collision Avoidance System (ACAS), which would provide a solution in SAAS for both manned aircraft and UAS.

All manned aircrafts ranging from small two seater planes to jet planes, should registered with the FAA. No plane should fly in the NAS without registration and pilot has meet the FAA regulations to fly a plane. UAS has created a challenging task for FAA, Integrating the UAS and regular manned aircrafts into the NAS pose risks of their own. FAA has therefore classified UAS into five categories based on their weight. At present FAA requires UAS owners to register their drone with them. FAA also does not allow autonomous it allows only remotely piloted drones.

5.1.2. Traffic Collision Avoidance system(TCAS) for UAS.

TCAS is being used in manned aircrafts for about ten years and has provided successful midair collision avoidance solutions. TCAS relies on complex azimuth readings on the aircraft to predict the right trajectory and path for an aircraft. The first collision avoidance system was developed MIT Lincoln laboratories[23] called as the Beacon Collision Avoidance System(BCAS). BCAS system keep a surveil of the aircraft surroundings. BCAS sends an interrogation message to the nearby aircrafts and receives a reply from their transponders. BCAS receives the message from the same transponder used to communicate with ATC. Using these replies, BCAS calculates the range of the nearby aircraft. TCAS was developed based on the

48

BCAS. TCAS also calculates altitude and range. TCAS are more reliable because it uses accurate oscillators to calculate frequency. Measurements in TCAS are made based on the closest point of approach(CPA), which is nothing but the time for the nearest aircraft to reach the same altitude level. TCAS systems are divided into two divisions called the Traffic advisors(TA) and the Resolution advisor(RA). TCAS 1 was implemented only with TA whereas TCAS 2 has both TA and RA[29]. Divisions in TCAS are shown in Figure 16.
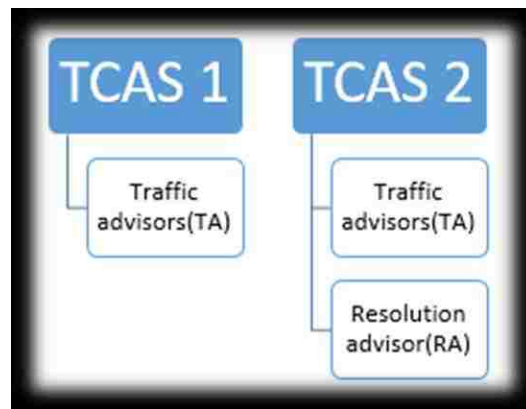

Figure 16: Divisions in TCAS

TCAS has got its own complexities when it comes to implementation in small UAS. Small UAS are very simple and less complex machines. Installation of TCAS in small UAS can lead to unforeseen problems. The complex design structure and difficult operational procedures can limit the performance of the UAS. UAS has limitations on power supply. On board TCAS on small UAS could lead to a faster power outage. TCAS systems are designed for complex operations demanded for the large manned aircrafts. Different alert levels are used in TCAS. Usage of all these alerts on a small UAS may not be necessary. Performance demands for TCAS are at a very high rate. TCAS requires a 2500 ft./min climb rate. Size of TCAS is large and cannot be fitted into majority of the small UAS [29]. Though TCAS come in various weight

49

ranges ranging from 1.8 pounds to 15 pounds, weight could be factor considering a small UAS weighing a maximum 50 pounds. TCAS requires an effective transponder always. Pilot's response is considered crucial in manned aircrafts as RA's depend on them. In case of UAS timely response is automated and message delivery is at risk. Table 4 lists the drawbacks of TCAS in small UAS.

Table 4: TCAS Drawbacks

S.No.	Drawbacks of TCAS in UAS
1	Complex design and operational requirements
2	Undesired communications alerts which choke bandwidth
3	TCAS Functional and performance demands beyond the capability of small UAS.
4	Weight, Power and capacity not supported in many UAS.
5	Dependency of RA's on manual operation response for efficiency. Automatic response would not function in case of a data link failure.
6	Requirement of an active transponder always.

5.1.3. Airborne Collision Avoidance System(ACAS)

The new ACAS system is an advancement of the TCAS. ACASX_u is a model of ACAS for UAS. ACAS system are more flexible compared to the TCAS systems. ACAS X is part of the new NextGEN-Controlled Airspace[23]. A Markov decision process is designed to calculate the rate of collision based on different states of the aircraft. ACAS is programmed using dynamic programming. Dynamic programming help calculate the cost of transition in every state of the aircraft. Based on the complexity or the transition of the state, the cost for each transition is

50

assigned. Cost of transition depends on the criticality level of resolution needed to avoid a collision in that state of the flight. Cost is looked up from the logic table based on combining transitions. These costs are calculated using intelligent structuring and calculations. In some flight scenarios, the data received from the sensors might be inaccurate. Therefore, by combining the probabilistic model and the sensor data the accuracy of the cost assignment can be improved. $ACASX_u$ uses a probabilistic approach for solving the collision avoidance problem in small UAS. TCAS supports active radar systems whereas $ACASX_u$ supports both active radar and additional inputs. Additional inputs include ADS-B, electro optical and infrared sensors. Small UAS perform differently compared to large manned aircrafts. UAS tend to operate at different speeds and change flight course, stop and move dynamically. Therefore, $ACASX_u$ cannot use the same logic table as that of the ACAS for costs. Costs for $ACASX_u$ are assigned keeping the sharp UAS maneuvers in mind [29].

$ACASX_u$ is being designed with the different aircraft airspace classifications in mind. All the manned aircrafts fly in a controlled airspace in constant range and communication with the ATC. The classes that are used by the manned aircrafts are class A through class E. The small UAS target the airspace class G, which does not need to be in touch with the ATC or any other clearance for flying. Class G extends from 1200ft to 12000ft [29]. Therefore, a collision avoidance solution for low altitude airspace depends mainly on secondary sensors like ADS-B. $ACASX_u$ can be increased when data from ADS-B is clubbed with the GPS data for precise location accuracy. ADS-B usage for small UAS has some disadvantages. Table 5 lists the disadvantages of ADS-B when used in $ACASX_u$. $ACASX_u$ needs to overcome the below mentioned errors to enabled $ACASX_u$ for UAS operation in class G.

51

Table 5: Backdrops of ADS-B for use in ACASX_u[29]

S.No.	Backdrops of ADS-B for small UAS.
1	Failure in message data sets.
2	Duplicate messages.
3	Bounce in data.
4	Latency between transmissions.
5	Maximum horizontal position error.
6	Navigational errors.

■■ Implementation and Integration of ADS-B into small UAS

Small UAS(SUAS) are different in operations, magnitude and maneuvers with respect to manned aircrafts. Manned aircrafts have a set of defined rules to obey before flying in the National Air Space(NAS) whereas rules and guidelines are yet to be defined for SUAS. List of some of the basic differences and observations of SUAS with respect to manned aircrafts. SUAS pose a low degree of threat to itself because of its small size. SUAS are considered to pose a moderate and not a serious threat to the manned aircrafts because of the magnitude and the size of the SUAS. The airspeeds at which SUAS operate are very low compared to manned aircrafts. Sudden maneuvers to avoid collision with a large aircraft is not easy because of their low air speeds. Due to the low speeds, SUAS stand more chance of getting hit rather than hitting another flying object. As per the FAA guidelines for hobbyist and commercial SUAS should always fly at the line of sight. Currently SUAS can fly for a short range and lateral distance [24]. Table 6 lists some of the basic physical observational differences.

Table 6: Simple Comparison between SUAS and Manned Aircrafts[30]**.**

S.No.	Comparison metric	SUAS	Manned Aircrafts
1	Air Speed	10 to 35 mph.	540 to 580 mph.
2	Size	350mm to 700mm when measured diagonally excluding propellers.	Size varies largely on the manufacturer and type of aircraft. Average wingspan of 150 to 211 ft., height 63 ft. and length of 150 to 240 ft.
3	Weight	5lbs to 55lbs.	Average takeoff weight of a large aircraft ranges from 12500 to 175000 lbs.
4	Range	0.5 to 2.5 km in SUAS.	Varies from air craft to aircraft but on an average, can fly between 7000 to 15000 km.
5	Elevation	500 ft. and above ground level.	36000 ft. and higher.
6	Day light only operations	Yes.	No
7	Flight time	20 to 25 minutes.	Varies on aircraft model and range from 3 to over 12 hrs.

Collision avoidance with respect to another flying object or stationary object is dependent on the maneuverability of the end user who maintains a line of sight. As of today, eyesight plays a major role in collision avoidance even when operated through a GCS. Situation awareness

should be maintained with the SUAS through visual observation. Though ADS-B is being used in some of the SUAS for navigational and surveillance purposes, it still needs to make progress in the field of collision avoidance. ADS-B Out is mandatory for all aircrafts in the NAS before 2020 but in case of the SUAS it will take a little longer. ADS-B has advantages for SUAS in terms of range, accuracy in situational awareness and frequent message transmission rates when compared to other existing systems[24]. A lot of focus and research is being put in to find a solution for collision avoidance techniques for SUAS, one of the most thought and dependable solution in the coming years is the use of ADS-B. For the Next-gen Airspace ADS-B will play a major role in situational awareness as well as collision avoidance for SUAS.

In areas where is high air traffic density, usage of ADS-B Out alone could not be sufficient. Addition of ADS-B In improves air traffic management. Generally, in areas where there is high air traffic, ground based SAAS is considered as an option. Problem with ground based SAAS is that because of the small size of the UAS, it is very difficult to detect. Due to the high traffic, many SUAS are prone to collisions. In these high air traffic situations, ADS-B is installed at ATC as well as in the SUAS. Though installation of ADS-B at both SUAS and ATC help resolve and detect the collisions more precisely, it too has some backdrops. Due to the increase in air traffic, use of ADS-B bands increases. When the use of bandwidth increases, the overcrowded lines may tend to interrupt important ADS-B messages. To avoid these scenarios, better management of bandwidth needs to be put in place.

ADS-B Out on GCS or the SUAS results in same operation which puts responsibility on the manned aircraft to avoid collision with the SUAS. In Figure 17, five types of ADS-B possible implementations on SUAS and its working are shown.
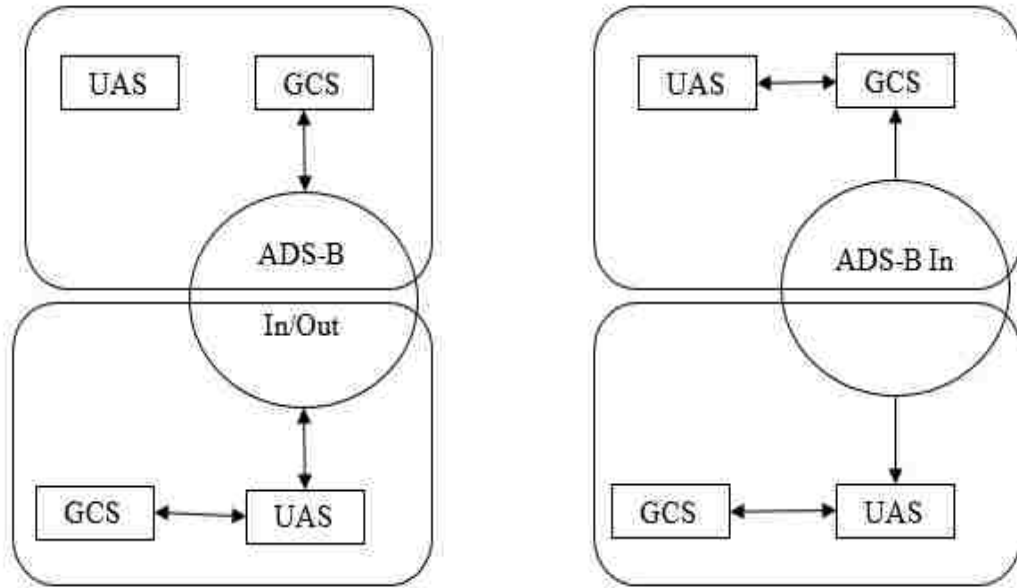
Figure 17: Possible ADS-B implementations for SUAS.

5.2.1. Proposed Configuration 1

In Table 7 diagram of the configuration 1 is shown along with the advantages and disadvantages. Configuration 1 includes an ADS-B In/Out, a GCS and a UAS. The GCS and the UAS are interconnected while the ADS-B In/Out is connected to the UAS[24].

5.2.2. Proposed Configuration 2

In Table 8 the diagram of the configuration 2 is shown along with the advantages and disadvantages. Configuration 2 includes an ADS-B In/Out, a GCS and a UAS. The GCS and UAS are interconnected while the ADS-B In/OUT is connected to the GCS[24].

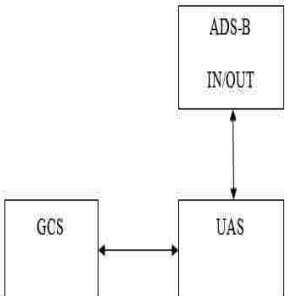**Table 7: Implementation, advantages and disadvantages of configuration 1.**

Configuration 1	Advantages on SUAS	Disadvantages on SUAS
	➢ Normal Working, just like how ADS-B works on the manned aircraft. ➢ Automatic self-separation algorithms will be applied by ADS-B to avoid collisions.	➢ The time delay between transmission and response or latency rate increases. ➢ Additional weight and size problems. ➢ Costly.

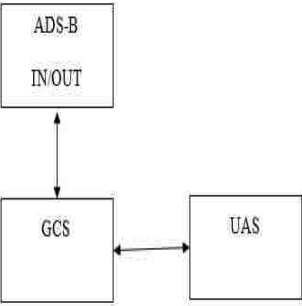**Table 8: Implementation, advantages and disadvantages of configuration 2.**

Configuration 2	Advantages	Disadvantages
	➢ Size and weight related problems have no constraint on the GCS. ➢ ADS-B messages transmission delays from UAS to GCS are very minimum as ADS-B Out communication uses telemetric link.	➢ Against ADS-B implementation standards are ADS-B Out is situated in the GCS. ➢ Ambiguous range of the SUAS may be transmitted.

56

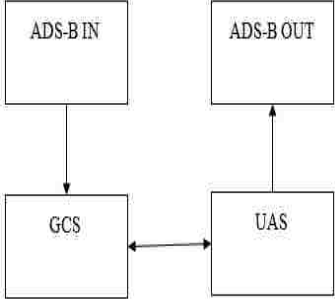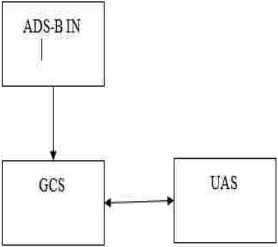**Table 9: Implementation, advantages and disadvantages of configuration 3.**

Configuration 3	Advantages	Disadvantages
	➤ As ADS-B Out is installed on SUAS and ADS-B In is installed on the GCS, position and situational awareness of the SUAS can be instantaneously be seen on the GCS display.	➤ Time delay and loss of transmission from ADS-B out to ADS-B In and again from ADS-B in to GCS can result in a late self-separation and lead to collision.

Table 10: Implementation, advantages and disadvantages of configuration 4.

Configuration 4	Advantages	Disadvantages
	➤ Implementation of ADS-B in on the GCS helps notify the ATC about collision course without time delay so that ATC can communicate with the manned pilot about probable SUAS collision.	➤ Chances of collision are more because big manned aircraft needs to take hard maneuvers to avoid collision with SUAS. Diverting SUAS is easier than diverting a big manned aircraft.

57

5.2.3. Proposed Configuration 3

In Table 9 the diagram of the configuration 3 is shown along with the advantages and disadvantages. Configuration 3 includes an ADS-B In, an ADS-B Out, a GCS and a UAS. The GCS is connected to the ADS-B-In and the UAS is connected to the ADS-B-Out. Both GCS and the UAS are interconnected[24].

5.2.4. Proposed Configuration 4

In Table 10 the diagram of the configuration 4 is shown along with the advantages and disadvantages. Configuration 4 includes an ADS-B In, a GCS and a UAS. The GCS is connected to the ADS-B-In. Both GCS and the UAS are interconnected[24].

58

CHAPTER 6: CONCLUSION

UAS is prone to many security threats. In the field of UAS Navigation and Communication, threats are severe to cause serious damage or even life threatening. UAS navigation in the current scenario relies on GPS or radar system. ADS-B relies on GPS data, an attack on GPS can prove fatal for ADS-B as well. To secure GPS as suggested in table 7, GPS and ADS-B should be integrated with other surveillance sensors for better secure navigation. Security in SUAS is very difficult to establish because of the size and magnitude constraints. Possible security recommendations are given in table 8 for SUAS.

■ UAS security threats and their possible solutions

Table 11 lists the security threats and possible solutions to overcome them.

Table 11: Security threats and its possible solutions.

Security Threat	Solutions
GPS Spoofing	Integrated IMU/DME GPS-INS integration Dead Reckoning
PCAS – XRX Device-False Alarm	FLARM (Currently not yet identified as a solution in UAS)
Terrain Awareness – GPWS	EGPWS with Terrain display and Terrain database look ahead protection

.

59

■ Existing solutions and proposed recommendations

In Table 12 are the solutions and proposed recommendations.

Table 12: Problem, proposed solution and future recommendation.

S.No.	Problem	Solution	Recommendation
1	FANET's have poor neighbor discovery due to use of slow directional antenna.	FANET's three layered approach help identify neighbor. Layer 1 has GCS, Layer 2 has UAS and Layer 3 has HAP which keeps track of all the UAS in layer 2 and transmitting neighbor location using LODMAC protocol.	Loss of HAP would result in loss of complete location details of all the UAS present in layer 2. Use of ADS-B to help neighbor discovery and implementation of SAAS as a backup when there is a loss of HAP.
2	SUAS not identified due to angle of flight angle detections issue when being detect using a radar antenna.	Powerful and large antennas help recognize and identify small UAS. Cost effective.	Integration of radar system with GPS and ADS-B provides accurate surveillance details in locations with high air traffic.
3	UAS collision avoidance using traditional TCAS.	ACAS system to be implemented for NEXT-gen air traffic by 2020.	Use of Light weight ADS-B Out for simple and current solution.

60

BIBLIOGRAPHY

[1] "1.4 Classification of the Unmanned Aerial Systems | GEOG 892: Unmanned Aerial Systems." [Online]. Available: https://www.e-education.psu.edu/geog892/node/5.

[2] "Unmanned Aerial Vehicle Systems Association Commercial Applications." [Online]. Available: https://www.uavs.org/commercial. [Accessed: 01-Nov-2016].

[3] "UAS Applications - CCUVS." [Online]. Available: http://www.ccuvs.com/industry/uas-applications/. [Accessed: 01-Nov-2016].

[4] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, 2012, pp. 585–590.

[5] T. H. Chauhan, S. Agarwal, S. Purohit, and A. Kumar, "Wireless Communications from High Altitude Platforms."

[6] S. Temel and \.Ilker Bekmezci?, "On the performance of Flying Ad Hoc Networks (FANETs) utilizing near space high altitude platforms (HAPs)," in *Recent Advances in Space Technologies (RAST), 2013 6th International Conference on*, 2013, pp. 461–465.

[7] K.-H. Rhee, Y.-H. Park, and G. Tsudik, "A Group Key Management Architecture for Mobile Ad-hoc Wireless Networks.," *J. Inf. Sci. Eng.*, vol. 21, no. 2, pp. 415–428, 2005.

[8] H.-Y. Chien and R.-Y. Lin, "Identity-based key agreement protocol for mobile ad-hoc networks using bilinear pairing," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06)*, 2006, vol. 1, p. 8 pp.-pp.

[9] J. Bian, R. Seker, and M. Xie, "A secure communication framework for large-scale

unmanned aircraft systems," in *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013*, 2013, pp. 1–22.

[10]   D. Hoey and P. Benshoof, "Civil GPS Systems and Potential Vulnerabilities," techreport, 2005.

[11]   S. M. Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," in *Recent Advances in Space Technologies (RAST), 2013 6th International Conference on*, 2013, pp. 795–800.

[12]   T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division*, 2008, vol. 55, p. 56.

[13]   T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 450–461.

[14]   T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *Univ. Texas Austin (July 18, 2012)*, pp. 1–16, 2012.

[15]   K. S. Hatamleh, A. Flores-Abad, P. Xie, G. Martinez, B. Herrera, and O. Ma, "Development of an inertial measurement unit for unmanned aerial vehicles," techreport, 2011.

[16]   C.-S. Yoo and I.-K. Ahn, "Low cost GPS/INS sensor fusion system for UAV navigation," in *Digital Avionics Systems Conference, 2003. DASC '03. The 22nd*, 2003, vol. 2, p.

8.A.1-8.1-9 vol.2.

[17] A. Nemra and N. Aouf, "Robust INS/GPS Sensor Fusion for UAV Localization Using SDRE Nonlinear Filtering," *IEEE Sens. J.*, vol. 10, no. 4, pp. 789–798, Apr. 2010.

[18] C. Schwartz, T. J. Bryant Cosgrove, G. Morse, and andJK Noonan, "A Radar for Unmanned Air Vehicles," *Lincoln Lab. J.*, vol. 3, no. 1, 1990.

[19] A. Moses, M. J. Rutherford, M. Kontitsis, and K. P. Valavanis, "Miniature UAV Radar System."

[20] J. L. R. Da Silva, J. F. B. Brancalion, and D. Fernandes, "Data fusion techniques applied to scenarios including ADS-B and radar sensors for air traffic control," in *Information Fusion, 2009. FUSION'09. 12th International Conference on*, 2009, pp. 1481–1488.

[21] M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[22] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *2006 IEEE Aerospace Conference*, 2006, p. 7 pp.-pp.

[23] D. A. Haessig, R. T. Ogan, and M. Olive, "Sense and Avoid - What's required for aircraft safety?," in *SoutheastCon 2016*, 2016, pp. 1–8.

[24] B. Stark, B. Stevenson, and Y. Chen, "ADS-B for small Unmanned Aerial Systems: Case study and regulatory practices," in *Unmanned Aircraft Systems (ICUAS), 2013 International Conference on*, 2013, pp. 152–159.

[25] "Equip ADS-B – The Ins and Outs of ADS-B." [Online]. Available:

https://www.faa.gov/nextgen/equipadsb/ins_and_outs/. [Accessed: 11-Feb-2016].

[26] 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*, pp. 1–12, 2012.

[27] D. 20591 Federal Aviation Administration, Washington, "Remote Pilot in Command Certification and Responsibilities," 2016. [Online]. Available: https://www.faa.gov/uas/media/Part_107_Summary.pdf. [Accessed: 04-Nov-2016].

[28] P. Pierpaoli, M. Egerstedt, and A. Rahmani, "Altering UAV flight path by threatening collision," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, 2015, p. 4A4-1-4A4-10.

[29] M. Kastelein and M. U. de Haag, "Preliminary analysis of ADS-B performance for use in ACAS systems," in *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)*, 2014, p. 7D3-1-7D3-10.

[30] Federal Aviation Authority, "Overview of Small UAS Notice of Proposed Rulemaking." [Online]. Available: https://www.faa.gov/regulations_policies/rulemaking/media/021515_suas_summary.pdf. [Accessed: 02-Nov-2016].

CURRICULUM VITAE

Graduate College

University of Nevada, Las Vegas

Vedadatta Gouripeddi

Degrees:

Bachelor of Technology in Computer Science, 2009

Jawaharlal Nehru Technological University

Master of Science in Computer Science,2016

University of Nevada, Las Vegas

Thesis Title: Improvement of Security in UAS Communication and Navigation using ADS-B.

Thesis examination committee:

Chair Person, Dr. Yoohwan Kim, Ph.D.

Committee Member, Dr. Ajoy K. Datta, Ph.D.

Committee Member, Dr. Wolfgang Bein, Ph.D.

Graduate College Representative, Dr. William Culbreth, Ph.D.