A Study of Datalink Security Issues in
Increased-Autonomy Air Traffic Environments

Technical Report

Risk Assessment and Mitigation Strategies for UAV Communication Systems

Karthik Gopalakrishnan and Hamsa Balakrishnan
Massachusetts Institute of Technology

June 2019

Abstract

Unmanned Aerial Vehicles (UAVs) are useful for enabling a variety of applications like remote sensing, logistics and package delivery, remote communication, and potentially even air taxis and other Urban Air Mobility (UAM) solutions. With increasing requirements on the reliability and functionality of these applications of UAVs, there will be significantly more communication between different elements of the system. These communication channels allow for greater real-time coordination between vehicles, pilots and air traffic controllers to ensure a safe integration of UAVs in the manned airspace, adapting mission requirements on-the-go, and efficient use of the airspace. In this report we analyze the communication links present in a Unmanned Aerial System (UAS) for security threats and vulnerabilities against malicious attacks. First, we develop a taxonomy to classify threats to the UAS communication system. Next, we develop a systemic methodology to analyze different types of attacks, and quantify their likelihood, impact, and associated risk. Additionally, mitigation strategies against these attacks are also discussed. Finally, we apply our risk-assessment framework to analyze a hypothetical UAV package delivery system to identify vulnerabilities and present recommendations to reduce the risks.

Chapter 1

Introduction

Unmanned Aerial Vehicles (UAVs), popularly called drones, are aerial vehicles, that are either flown autonomously by on board computers or controlled remotely by pilots. These vehicles come in a wide variety of sizes, from nano drones that fit in ones palm and weigh less that 0.55 lb, to military drones like the MQ-9 Reaper that weigh over 10,000 lbs [2]. Further, the vehicle capabilities also lie on a wide spectrum- hobby drones fly for a few minutes on a single charge, and have a simple features like auto-land and at-times an on board camera to capture images. Commercial drones can fly for up to 20-30 minutes, have GPS navigation capabilities, can follow pre-defined flight paths, and use specialized devices like high-resolution cameras and ultra-sound sensors. On the extreme end of capabilities are the military drones (Unmanned Combat Aerial Vehicles, or UCAVs) which have very precise navigational capabilities, with high fidelity satellite communications, and a high degree of on-board autonomy. Since UAVs do not have a pilot on board, they are typically cheaper to manufacture and operate, can be operated at a large scale, perform missions that are considered too risky for humans, navigate dense urban environments due to their relatively smaller size, and automate repeated tasks performed by conventional manned vehicles. Because of these wide capabilities, these vehicles are used for a variety of applications which we broadly classify into four groups:

- *Surveillance*: Infrastructure health monitoring, traffic flow updates, search and rescue, military reconnaissance, law enforcement
- *Logistics and transportation*: Package delivery, transporting aid to disaster affected areas
- *Communication enabler*: Ad-hoc network router that provide wide area coverage (e.g Google Loon), backup cellular stations in case of emergencies
- *Payload deployment*: Spraying pesticides in farms, releasing fire retardants to control forest fires, deploying missiles

It is easy to argue that the applications of UAS are many, and has far reaching benefits for society. With such a wide range of missions, and vehicle capabilities, a key technology underlying these systems and enabling these versatile applications is the robust communication channels between several elements of the system. We discuss two examples to highlight the need and importance of these communications.

Consider a hobby drone operator that is operating near the vicinity of an airport, who wants to fly high and take photographs of their house. First, they need a constant

communication with their vehicle, which is relatively low on autonomous capabilities to control and fly it. Typically, this is done through a Bluetooth connection between the vehicle and the mobile phone of the user. The pilot may also have to communicate directly with the Air Traffic Controllers (ATC), or some UAS Service Supplier (USS) to ensure that their proposed flight does not conflict with other manned operations from the airport. However, it is expected that this requirement will be dramatically reduced in the future. Once an authorization is provided for a specific period of time, this communication channel need not be active. On the other hand, the Bluetooth link between the pilot and the vehicle needs to remain active, is used for active command and control of the vehicle, can transmit back images that the vehicle captures, and is critical to ensure the safe operations of the vehicle.

As another example, let us consider a UAV performing aerial reconnaissance for the military over a hostile region. This vehicle has a reasonable level of autonomy, has GPS navigation capabilities, has a secure satellite link to transmit videos to the base station as well as receive critical command and control inputs from the remote pilot who may be thousands of kilometers away. Further, this vehicle may also be communicating with several other surveillance UAVs in the airspace to coordinate their efforts using a direct line of sight encrypted wireless link.

These two examples highlight the various communication links that may be present, along with the range of functions that they perform. Some links may require very low latency, like those used to control the vehicle directly, whereas some others like the hobby drone pilot communicating with the USS may not be time sensitive. The communication with a reconnaissance vehicle might have to be secure and encrypted, whereas there are no such requirements for the hobby drone. More generally speaking, links differ on several dimensions such as the nature of information communicated, the latency and bandwidth requirements, the safety criticality of the message transmitted, the medium of transmission and security requirements.

Several of links mentioned previously are integral for the system to complete a mission successfully, and it is important to ensure their robust performance. As the reliance on UAS by society increases, and the economic value of the activities they perform increases, so do the external threats on the system. These UAVs or the associated infrastructure, may become the target of malicious activities. These activities may result in loss of the vehicle, using the vehicle as a projectile, stealing private information collected or transmitted by the vehicle, causing delays in the operations or in general compromising the success of the intended mission. While attacks on the system can happen on several dimensions, ranging from physical attacks, cyber attacks, or even using surface-air or air-air projectiles to attack the vehicle, we focus on a specific class of threats in this work, namely threats to the communication infrastructure.

1.1 Prior Work

There are three areas of prior work that are relevant to this report. They are: risk assessment frameworks for cyber-physical systems, detailed analysis of specific vulnerabilities and security threats, and security measures to improve the communication systems. We present details about the first set of papers, but defer the details of the rest to the appropriate chapters in the report.

Security of cyber physical systems have been widely studied, and specialized for several

domains such as electricity grids [61], SCADA systems [26], and wireless sensor networks [50]. Analyzing security in vehicular ad-hoc networks preceded analysis of UAS. A seminal paper in the field [53], sets up the framework for classifying threats based on scope, extent, intent and activity in vehicle-systems. While the focus of the paper was on road vehicles, the approach could be extended in principle for an UAS. Attacks on UAS have been listed in other works, and some specific cases have been analyzed for the likelihood, impacts and risks [29]. In fact, [47] also presents a useful abstraction of *atomic attacks* that can be composed to generate a wide variety of attacks. However, most prior work has been restricted to a specific architecture, and not generalized to consider several evolving communication technologies like Bluetooth, WiFi etc. While some works have focused on specific architectures for command and control, a complimentary piece of work analyzed specific drones like the Parrot AR, MQ-9-Reaper and RQ Senteniel [22]. Thus there is a research gap in providing architecture and vehicle independent frameworks to analyze the UAV system.

1.2 Outline

The outline of our work is as follows

- First we present a decomposition of the communication system into nodes and links so that each element may be analyzed independently. Then, the requirements of a communication channel is discussed in further detail. Finally, we develop a taxonomy for attacks on the communication system to categorize attacks based on metrics such as its scope, element attacked etc. This work is discussed in Chapter 2.

- We expand on one of the classification techniques, based on the attacker action, to enumerate *atomic attacks* that form the basis of all security threats. These likelihood and impact of these attacks are quantified, and used to evaluate the risk measure for the attack. Such a risk analysis is performed for each sub-component of the system. Chapter 3 presents atomic attacks, and Chapter 4 quantifies the risk levels of each of the system components.

- Next, we discuss mitigation strategies against the atomic attacks. We emphasize the varying effectiveness of these strategies along with the technological and practical challenges in implementing them. We specifically discuss measures that can be incorporated against the high risk attacks (identified previously). This work is presented in Chapter 5.

- Finally, we apply the risk-assessment framework to a hypothetical drone package delivery setting. We consider two different levels of autonomy, which leads to different assumptions on vehicle and system capabilities, and compare the risk profiles under both scenarios. This also provides valuable insights into the effect of technological capabilities in communication system risks, as improved technology also opens up a new set of mission capabilities that come with their new added vulnerabilities. Chapter 6 discusses this case study.

Our contributions are two fold. First, we present a framework to assess security threats specifically in the context of UAS, along with a qualitative guideline on factors that determine the security risk level for various attacks and different elements of the system. This

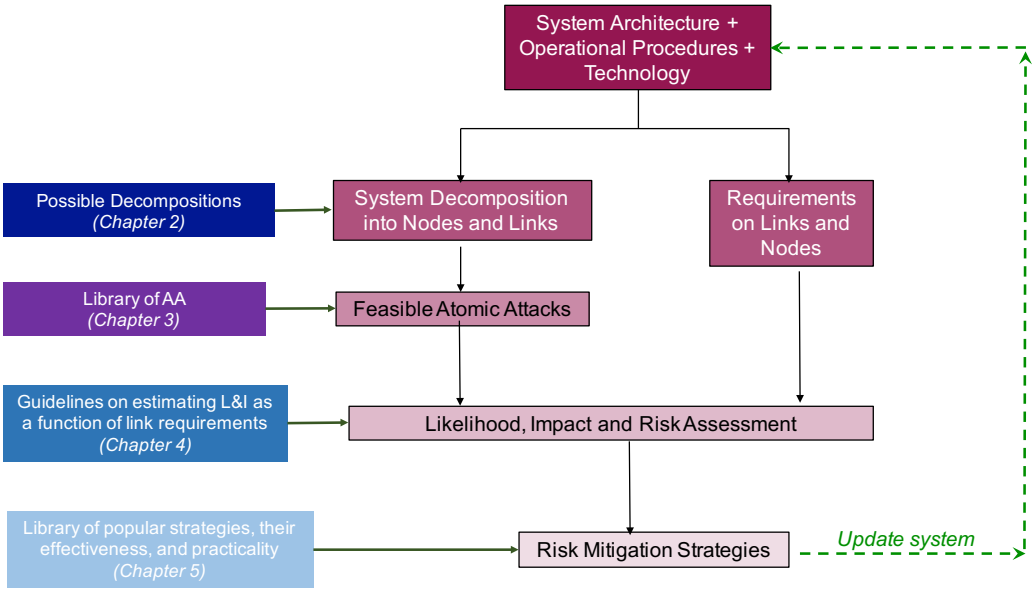

Figure 1.1: Overall framework for assessing vulnerabilities in the UAS communication infrastructure

leads to an effective procedure for choosing mitigation strategies, and implementing them according to a risk-based priority order. Second, we provide a comparison of two potential architectures for UAS package delivery systems based on their communication risk. These can be incorporated into systems engineering toolkits to design safer architectures for operating UAVs, safer integration of these vehicles in the airspace, and improving the resiliency and robustness of UAS technology.

1.3 Risk Assessment Framework

Figure 1.1 summarizes our proposed framework to analyze a given Unmanned Aircraft System. The steps are as follows

1. We start with a detailed description of the system architecture, the operational procedures, and the capabilities of the autonomous technologies. This provides us all the assumptions needed to perform a risk analysis.

2. Based on the system architecture, Chapter 2 provides a guideline on decomposing the system elements into nodes and links, and also specifying the requirements on the links (confidentiality, availability, latency etc).

3. Referring to Chapter 3, we list out all feasible attacks for the particular the node-link decomposition

4. Atomic attacks, along with the technology involved in the UAS determine the likelihood of the attack. The effectiveness of the attack, along with the link requirements determine the impact. Chapter 4 discusses qualitative guidelines on making this assessment. Finally, impact and likelihood are combined to estimate risk of all attacks.

5. The highest risk cases can be considered first, and a variety of mitigation strategies presented in Chapter 5 can be considered to reduce the risk level below a user-defined acceptable threshold.

6. Some of these mitigation strategies may involve adding redundant links, changing the operational practices, or incorporating new technology. This sets up an iterative framework to make changes, keep track of important assumptions, and analyze communication risk in a principled manner.

Chapter 2

Taxonomy of Attacks

In this Chapter, we first describe the communication system elements as nodes and links. This is a generic, architecture independent notion that would help us analyze any given system later. The purpose and function of each of the nodes, and the links will be discussed. Then, we present our taxonomy for classifying threats, and discuss each of the different classification dimensions.

2.1 Classification into Nodes and Links

There are primarily two kinds of works regarding UAV communication: One body of work presents a more systems level view, describing the components, threats, and defenses. The other type of work looks at specific sub-problems that are pertaining to a particular type of channel, say UAV-UAV or UAV-ground.

Mobile Ad-Hoc networks and vehicular networks have been studied over the last decade. [21] is a good survey paper on UAV-UAV communication networks, and explicitly discusses the differences between MANET, VANET and UAVNETs. Protocols for routing of packets in MANETS is described in [13].

2.2 Elements of the communication infrastructure

The ATC, UAV and the pilot (the *nodes* in the communication system) need to maintain effective communication with each other for safe operation in the airspace. Figure 2.1 provides examples of the means to achieve this communication. Each communication link (between two *nodes*) has a different requirement and is enabled by a different technique or strategy. In this section we discuss the elements of the infrastructure, analyzing each individual link and the means of enabling the link.

2.2.1 The Nodes

- **UAV (The Vehicle)**: Each vehicle is considered a node, with separate communication equipment on board it.
- **Air Traffic Controllers (ATC)**: ATC is responsible for the separation of manned aircraft. Each control unit (tower, TRACON or center) is considered a node.

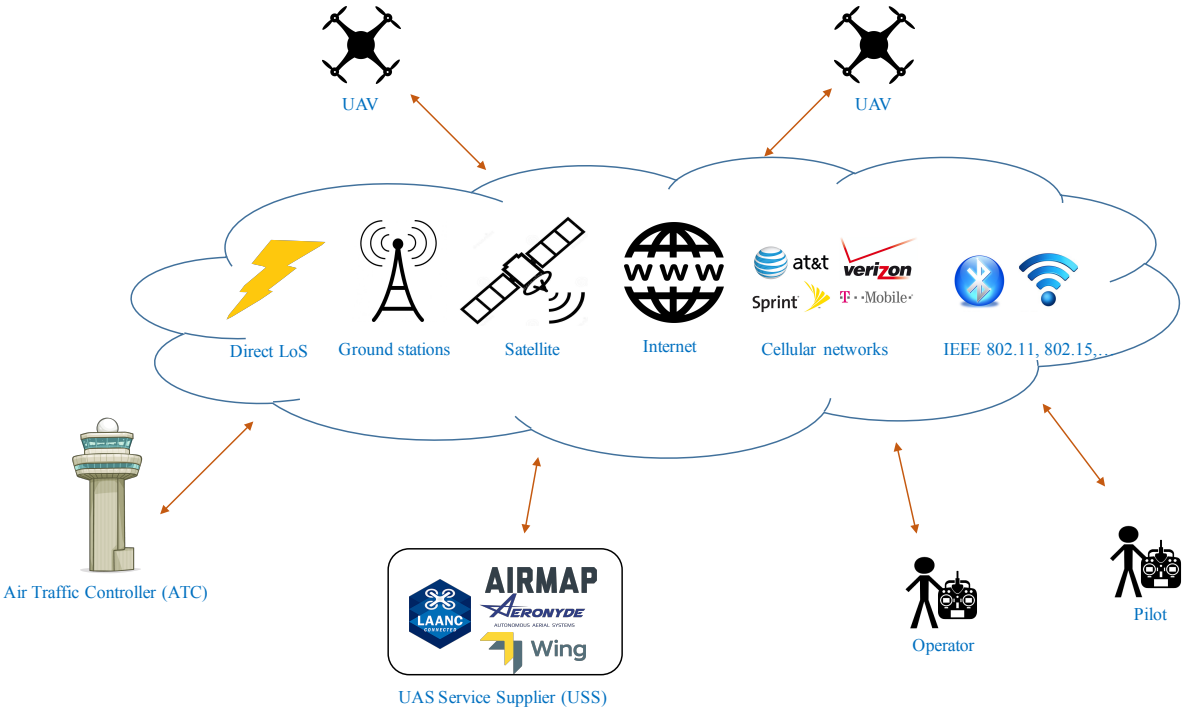

Figure 2.1: Different elements and possible links in the communication infrastructure

- **Operator**: The operator is the person directly responsible for providing control inputs to the vehicle.
- **Remote Pilot**: The pilot is responsible for the safe operation of the vehicle. The pilot may, or may not be the same as the controller. In fact, a single vehicle may have multiple operators, but only one pilot, who is responsible for the overall operations. Throughout this report, we will typically assume that the pilot and the operator are the same person, and will specify explicitly when that is not the case.
- **UAS Service Supplier (USS)**: The USS facilitates UAS Traffic Management (UTM), and coordiantes several activities like providing route clearances as well as coordination with ATC. Several organizations may become a USS node, and can provide these services to UAV operators.

2.2.2 Purpose of the Communication Between Nodes

- **Pilot-Operator**: While the operator is tasked with flying the vehicle, or performing specialized tasks such as photography, analyzing the video feed, scanning for traffic etc., they need to communicate with the remote pilot, who has overall responsibility for the safety of the flight and mission. This means that the pilot would have to communicate with operators to guide them, possibly take over in case of an emergency, or monitor the vehicle and mission progress. If the pilot and operator are co-located, or the same person, then this concept is void, however, if they are located in different facilities, secure, reliable, and low-latency communication links will typically be necessary for the pilot to effectively perform their duties.

Henceforth, for this sub-section, we assume that the pilot and operator are the same person, and use the word Pilot to encompass both.

- **UAV-UAV**: This communication link can be used to share traffic and weather data, act as relays or to coordinate mission. Providing wireless services to a region has been an area of active research. Routing algorithms and security protocols for Mobile Ad Hoc Networks (MANETS) and Vehicular Ad Hoc Networks (VANETS) are being developed [30]. There are however several challenges due to the mobile nature of the vehicles, changing network topology, and power constraints in smaller UAVs. There are several ways in which this communication can be realized. Line of sight communication can be useful for broadcasting traffic or weather information to near by vehicles. If the UAVs are far apart, then dedicated use of ground receivers and transmitters or space based communication is possible. If the vehicles are at a low altitude, then they can use existing telephone carrier channels for communication. When the information exchanged is a control command, weather or traffic alerts, having a low latency, high availability, and high reliability is important. If the UAV network is providing wireless internet service to a region, then latency and bandwidth determine the quality of the service available to the customers.

- **UAV-Pilot**: The information transmitted can be traffic, video or images from a camera, position and intent, or mission dependant data (collecting from sensor networks, internet packets etc). There is a high variability in the latency and bandwidth requirements depending on the autonomy level [43] of the vehicle. If live video feeds are used for control, then a high bandwidth, low latency link would be required. Direct line of sight communication, use of Wifi or Bluetooth protocols (like done in commercial DJI drones) could be better alternatives than satellite links, in terms of latency. The range of the UAVs from the pilot would be extremely limited in that case. If the UAV has a high level of autonomy, and just requires an overall passive mission plan, it can be transferred at a low latency rate. Satellite datalinks, can provide global coverage, but offer low data rates and high latency.

- **Pilot-ATC**: The current procedure in the US is that pilots can fly drones below 400 feet in class G airspace and 5 NM away from any airport without any prior approval or communication with ATC under VMC. If any other operation is desired by a UAS operator, then prior permission needs to be acquired and arrangements would be made to decide if and how communication would occur. However, with increasing traffic, and evolving requirement of the operators, it may be required to maintain and utilize more formal methods of communication. Potential options are: Phone call (land-line, cellular network or SATCOMM), internet or cloud based interface for voice or datalink [46], integration with the NVS [67], and a satellite datalink.

  The information communicated through this channel would be control actions, position and intent, traffic or weather information. Low latency would be the key performance requirement of this channel, and it is unlikely that high bandwidths would be required.

- **UAV-ATC**: Some options to establish this link could be to have a datalink with the ATC, an artificial voice system, or through the UTM (i.e the USS). The datalink

could be through a satellite, cellular network (for low altitude ops in densely populate locations) or line of sight transmission to a network of ATC ground receivers. For manned aircraft, there are two datalink communication options- Aircraft Communication Addressing and Reporting Standards (ACARS) and Controller Pilot Data Link (CPDLC). ACARS is used by pilots to communicate with the airline to obtain information about winds, re-routes, delays, NOTAMS, passenger requirements etc. CPDLC is used by air traffic controllers to send route clearances and over time, is expected to reduce the voice communications in the VHF radio channels. ACARS and CPDLC are usually be transmitted via VHF, HF (for ACARS only) or SATCOMM. These datalinks can be augmented to communicate with the UAS. The challenge would be to identify simple modifications to the existing system, as they were never built for time-sensitive information and assumed redundancy via voice. Concerns of limited spectrum have prompted researchers to consider the higher frequency L band for a UAS datalink [28, 27]. The authors however confess that high speeds and long distances is a major limitation of two popular proposals- L-DACS1 and L-DACS2.

2.2.3 The Links

A short literature review

Physics based channel characterization is important for UAV applications as they often fly at low altitudes, perform dynamic maneuvers and could have stringent requirements on the availability of the channel. Transmission characteristics may result in optimum altitudes for UAVs to maximize link availability and range [7]. Piggybacking on existing LTE cellular connections is also a possible option [5]. The 30-300 GHz frequency (mm wave) has also been considered for UAV applications [34]. The operation of UAVs in dense, cluttered, low altitude environments makes the UAV-ground link to be more dispersive, leading to terrestrial shadowing attenuation and time-varying channel characteristics. Performing experimental investigations aids in building and validating the channel models for this emerging application domain [42, 65]. A survey of different issues in UAV-UAV and UAV-Ground communication is presented is [72].

Voice is the most widely used form of communication in the current ATM system. Several architectures are possible to integrate voice communication from UAS pilots into the system. [67] discusses the pros and cons of the various architectures, giving consideration to the security of the Federal Telecommunications Infrastructure and the number and type of access points the UAS pilots will have to join the network. Detecting anomalous transmissions, voice pattern analysis and aircraft trajectory conformance can be combined to provide a holistic attack detector [62]. Audio watermark, which is a non-perceptible digital signature can also be used to authenticate the identity of the transmitter [25].

GPS signals are one of the common ways in which UAVs navigate, and the UAV obtains the position information through a satellite-UAS link. GPS spoofing and jamming are common attack scenarios and have been studied for a long time, although to a lesser extend in the aviation context which involves mobile receivers [24, 33, 52, 48, 66]. This is also related closely to the problem of GPS integrity for ADS-B application. Jamming attacks are possible not only for GPS signals but also for any EM communication in general. UAS provide a special setting since there are power [68] and mobility constraints [10].

Datalink security is not well studied, even though it is currently being used by commercial manned aircraft. It includes datalink for passengers on aircraft, or the digital communication between ATC or the airline with the pilots. A secure version of ACARS using elliptic key cryptography has been proposed [63]. A more comprehensive overview of datalink security from a computer networks perspective has been provided in [40] and covers several traditional approaches from the networking literature. Cryptographic techniques, although academically popular has not been implemented in any large scale system. Some of the ideas proposed include using an operators EEG signal to generate a key [60], WPA2 encryption for IEEE 8022.11 systems [23], and maintaining trust-based inter UAV communications under power constrains [8].

We describe the links in the communication system:

- **Direct Line of Sight (with Ground Stations)**: VHF radio communication, ADS-B signals. Can be used for voice as well as data communications. ACARS and CPDLC use VHF communication for LoS.For beyond line of sight communications, High Frequency (HF) radio waves are used. These waves get reflected at the ionosphere and provide wider, but less reliable coverage for a greater region of the earth.

- **Satellite links**: Satellite links can be used for any communication between UAV, pilot, and ATC. It can be used to transmit voice, data, or navigation information through GPS. Except for the use of GPS for navigation, the use of satellites is typically associated with high latency. The advantage is that there is no need for any ground infrastructure and its coverage is almost the entire surface of the earth. ACARS is an example of satellite based digital communication that is used today.

- **Cellular networks**: for connecting to drones using cellular LTE infrastructure [37, 71]. There are however a few technical challenges. First- when a UAV is in the air, it can communicate with multiple cell towers creating interference. Second, cell transmitters on the ground are pointed towards the earth, rather that air to maximize coverage for terrestrial users and prevent interference with other cellular towers. The UAVs in the air will be serviced by the side-lobes of the base station. Third, transitions from one cellular base station to another station needs to be handled seamlessly. Reception of cellular signal can also place a restriction on feasible trajectories for the UAVs [73]. There are discussions on incorporating standards for aerial coverage for 5G networks, indicating promise in the idea. 3d beam-forming using directional antennas can alleviate some of these concerns. It is not always necessary that the UAV connects directly to the cellular network. A local portable ground station may be used an an intermediary, that serves as a bridge between the UAV and the cellular network [12]. Cellular networks can be used to maintain traditional voice based communication between the pilot and the ATC too. It is believed that the use of voice for UAS however is not a scalable solution based on the forecasted growth in UAS traffic.

- **Internet or cloud**: The internet can be used by UAVs when they are connected to the cellular network, via a satellite link or wifi/bluetooth. The ATC and and the Pilots can also connect to the internet through conventional means. Internet can be used for uploading flight information by the pilots, ATCs to maintain communication with the pilots to give clearances. The benefit of a UAV connecting to

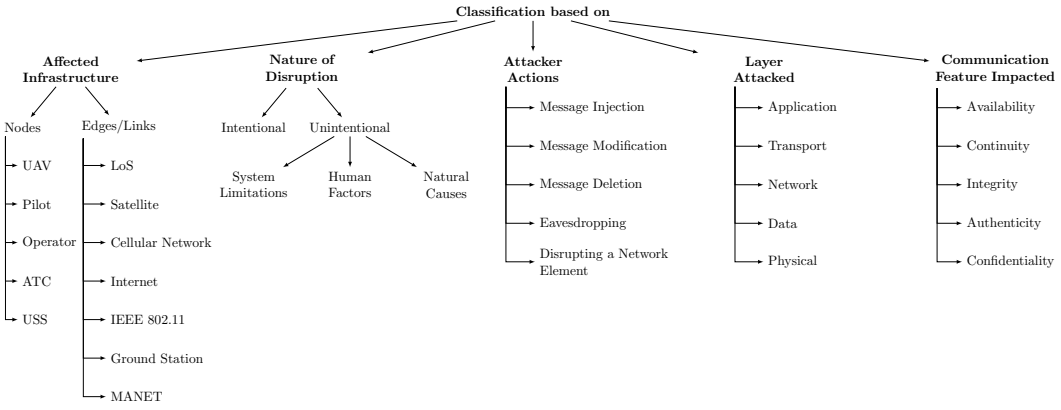

Figure 2.2: Classification of threats to the UAS communication system

the internet, versus other forms of direct communication is not obvious. When a cellular network is used, it may be easier to directly use it to connect to the UAV, or in case of Wifi or Bluetooth, directly communicate the intended data.

- **Wifi, Bluetooth**: They are line of sight protocols (IEEE 802.11 for WLAN/WiFI and IEEE 802.15 for Bluetooth) for communicating in the 2.4 GHz band. Bluetooth is restricted to about 100 meters range. WiFi can be modified to have large range, upto tens of kilometers, but are not commercially used currently. WiMAX is a more recent protocol (IEEE 802.16) used for Wide Area Networks and has been successfully demonstrated to maintain data communications in terminal areas.

2.3 Taxonomy for Malicious Attacks

We develop a taxonomy for classifying the threats to the UAS (Figure 2.2). There are five main dimensions along which we classify attacks: Affected infrastructure, nature of disruption, attacker actions, layer attacked and communication feature impacted. This classification, while useful in itself, extends further in two directions

1. The classification based on the attacker actions is the basis for *Atomic Attacks*, a concept we will describe further in the next chapter. To summarize, these different attacker actions are orthogonal, and are considered to form the basis for describing any complex attack. Thus studying each of these different attacker actions suffices for the security analysis of the system.

2. Classification based on communication feature describes the key features that a communication link is expected to provide. However, for practical purposes, all of those features need not be equally important in a particular context. For instance, the privacy requirement on a link, or the latency depends on the application.

2.3.1 Classification based on Affected Infrastructure

Threats or vulnerabilities can exist for the nodes or the links. There can also be specific threats associated with the medium of usage. In this section, we outline the known threats

to the communication infrastructure and classify them. The purpose of the classification is to enable a systematic approach to providing solutions and security measures.

2.3.2 Classification Based on Nature of Disruption

- Atmospheric conditions
- Satellite not in view
- Ground interference
- transitions/handoffs between stations
- Topology of the environment (buildings, mountains etc)
- Aircraft shadowing
- Human error (incorrect system maintenance, faulty programs, Pilot or ATC error)
- Cellular communication issues- out of range, interference

2.3.3 Classification based on Attacker Actions

Attacker actions can involve deletion, insertion, modification, or eavesdropping on communication. Further it may also involve physically damaging a communication element. These are described in greater detail in the next chapter.

2.3.4 Classification based on Layer Attacked

- Physical layer: Electromagnetic jamming, GPS jamming and spoofing, message modification, message injection, impersonation and man-in-the-middle attacks [24]
- Data layer, Transport layer and Network layer issues are serious for UAV-UAV mobile networks or for any message via the internet or cellular network. Examples of attacks in these layers are- black hole, SYN flooding, Denial of Service (buffer overflow, flooding, spoofing), replay attacks, sybil attck, IEEE 802.11 attacks (capturing and de-authenticating frames) [23] etc.
- Application layer: Malware, spyware, virus
- Social engineer attacks (people giving out codes, passwords etc inadvertently)

2.3.5 Classification based on communication feature Impacted

There are 5 main elements of a communication channel that determine the quality of service.

1. Confidentiality: The message can only be received or decoded by the intended recipient. This ensures privacy of the conversation and prevents eavesdropping. The nature of the communication determines how important confidentiality may be. In some cases, like transmitting locations of the UAS may be intended for all recipients in the neighborhood and confidentiality is a negative feature. However, if the

channel is used for transmitting live video streams for the military, confidentiality is a major concern.

2. Availability: The communication channel can be used for a great fraction of time. Ideally we would require a 100% availability. A system may inherently not be capable of achieving 100% availability, for example HF communication, which depends on ionospheric reflections may not be always available depending on solar activity. On the other hand, wired communications through fiber optic cables are likely to have a high availability and are immune to natural phenomenon.

3. Continuity: The fraction of time a channel is available may be a contiguous block or may be inter-spaced with short moments of unavailability. When there are too many interruptions, it may not be possible to send a complete message in one contiguous available slot. High continuity implies high availability, but the converse is not true. A definition proposed in RTCA Special Committee 203 (also refer to [27, 28])is

$$\text{Continuity} = \frac{\sum_i (\text{Uptime}_i | \text{Uptime}_i > \text{T}_c)}{\text{TotalTime}}$$

4. Integrity: The information that is transmitted is the information is same at what is received at the other end. The message should not be modified because of natural, or intentional factors. Ideal systems would also have self-checking mechanisms that would raise a flag when the message integrity is lost. Integrity is especially important when the transmitted message is a control action for a UAV, where errors could lead to a substantial loss.

5. Authenticity: The identity of the sender is what is claimed in the message.

Another desirable feature is non-repudiation, meaning that the recipient of a message cannot later deny that the message was never reached. In this report however, we do not consider this and leave it for future work.

Chapter 3

Basic Security Threats: Atomic Attacks

- Overview: How to superpose several of them - List of attacks and their description - Specificity of the location of impact of an atomic attack, i.e. tie it to system implementation

The basic building blocks of an attack are referred to as *Atomic attacks*, a concept we borrow from [47]. These atomic attacks can be combined in several ways, or be used in isolation to disrupt the functioning of a node (vehicle, ground station, remote pilot etc) or a link (cellular, Line of Sight, WiFi etc). In this chapter we describe atomic attacks in detail. The next chapter discusses the system level implementation of these atomic attacks, their ability to affect different parts of the system and their impact.

3.1 Atomic Attacks

An attack on a communication system would attempt to affect one the following: availability, continuity, integrity, authenticity, or confidentiality. We place the atomic attacks into three broad categories depending on the vulnerability they exploit: the physical system itself, the software aspects, or the social/human factors. We list out atomic attacks in each of the sub-categories.

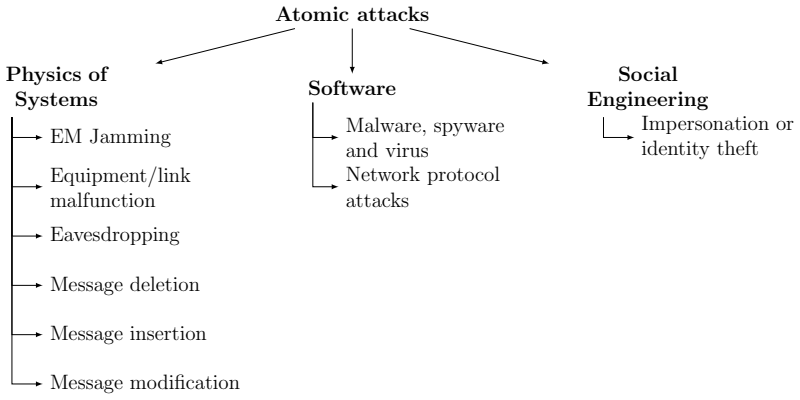

Figure 3.1: List of atomic attacks

3.1.1 Physics of systems

EM Jamming

Electromagnetic signals are the basic manner in which all wireless communication occurs. A transmitter generates and broadcasts the information, whereas a receiver has an appropriate circuit that can decode the signals and extract the information. Jamming an EM signal would make it hard or impossible for the receiver to decode the waves to obtain the transmitted information. They can be jammed by several ways. Typically, an attacker would broadcast noise at high power level on the same frequency, which would decrease the Signal-to-Noise ratio below the receiver device threshold.. A high power attacker transmitter is required near the original transmitter or receiver to achieve the effect. Jamming incapacitates nodes of the communication infrastructure- UAV's, ground stations, or a remote pilots radio station. Physical proximity is the key limitation for such an attack. An attack that directly targets just a UAV is challenging because the jammer needs to be in close proximity to the moving target (probably another UAV). Jamming a wider region of airspace requires high power and is technically more challenging.

Equipment/link damage/malfunction

An attacker may simply vandalize, damage or break a communication element. This could involve tampering with the antaneas in case of wireless links, cutting fiber optic cables, attacking the remote pilot, or breaking parts of the vehicle. Such activity is typically criminal, and have happened in the past in related contexts, for eg the arson attempt at Chicago air traffic control tower in 2014. Among these several possibilities in destroying the communication equipment, some are easier than others, and some are more impact than others.

Eavesdropping

Eavesdropping is a passive attack, where the sole aim of the attacker is to hear the communications. By itself, it does not affect the system, but leads to loss in confidentiality and may form the basis for other more sophisticated attacks.

Message deletion

One way to delete messages is to do EM jamming. That however need not be the only strategy. Message deletion can be done selectively too, especially if the communication is not encrypted. The attacker can then listen to the communications and either not relay it in case of wired transmissions, or send appropriate signals for destructive interference in case of EM waves.

Message injection

Message injection means that an attacker can insert and transmit false messages int he system, and make it seem like it was from a particular sender. These can be potentially dangerous. The injected messages may range from control commands to aerial vehicles, to spurious GPS signals, to fake payload data (e.g if drones are used for providing internet connectivity to a region).

Message modification

Modification of messages is typically more difficult than insertion or deletion of messages. In general, when a message is encrypted and authenticated, there is very little scope for modification. Encryption means that a message cannot be deciphered by anyone who happens to over-hear the conversation. This means that there is either a public key or a private key mechanism that ensures that only intended recipients can decode a message if intercepted. A message is said to be authenticated if the identity of the sender can be ensured using some form of a digital signature. When there is neither encryption, nor authentication, some effort is still needed to modify messages. In case of wireless transmissions, it may require a module that eavesdrops and selectively deletes messages, and another that transmits the modified message. In case of wired networks, this may require the physical presence of an attack module to do these modifications.

3.1.2 Software

In our taxonomy, we distinguish between the software level attacks that occur at the end points of the communication link (i.e the transmitter or receiver / nodes) and software attacks that affect the routing protocols (across all the layers- physical, data, transport, session, network, application etc) in a link. The former is categorized as a Malware, spyware and virus attack, and the latter as a network routing protocol attack.

Malware, Spyware and Virus

These are software that can make any piece of hardware they operate on perform unintended tasks or not perform their required tasks at all. It could affect a ground station, a remote pilots controller, or a UAV itself. The exact impact of these malicious software is varied.

Some example of such malicious software

- Keylogger codes [39]
- Malware to obtain control of a UAVs hardware [69]
- Software that can run in the background and drain the battery

A targeted attack on one element is very likely as it only requires one weak entry point into the system, for instance, software upgrade to a UAV. Targeted attacks obtained by coordinating several elements of the system requires massive security breaches and is less likely.

Network routing protocols

Communication in MANETs [13] and their relation to VANETS and UAVNETS [21] discuss the issues that are of convcern primarily in UAV-UAV networks. Other works provide a more systems overview of the factors that need to be considered that enable secure UAV operations [15].

- SYN flooding is a type of Denial of Service. TCP connections are established with a first Synchronization message, also called as a SYN message. If too many SYN message are received by the server, then the system becomes unresponsive

to legitimate traffic. Back hole attack, or a packet-drop attack is another form of denial-of-service attack.

- In a black-hole attack, a router or network element routinely drops packets that it is supposed to forward. If all the packets are dropped in one instant, it could be easy to trace the rogue router, and typically only a fraction of packets are dropped randomly. In wireless ad-hoc networks, a black hole attack is even more dangerous, because a router can broadcast information that it has the shortest path to a destination. This could make it selectively obtain packets for a particular destination, and drop them.

- Replay attacks occur when legitimate transmissions are repeatedly sent again either by the malicious transmitter itself or an intermediary

- In a Sybil attack, one node in the network can create multiple (fake) identities and obtain greater control of the network operations. For instance, a UAV in an ad-hoc network could pose as several nodes, and have almost all data traffic routed through it. This could give it ability to selectively modify or delete messages.

3.1.3 Social Engineering

Impersonation and identity theft

This is the most common format in which an attacker gains access to the system. It can manifest itself in several ways:

- Phishing attacks

- Eliciting information through social media

- Password thefts

- Left system unattended

Chapter 4

Evaluation of the Impacts and Risks of Atomic Attacks on the System

4.1 Outline

In this chapter, we focus on the means and motivation for attacks on different elements of the communication system. Specific attacks, and the communication infrastructure they affect, are discussed to provide a comprehensive overview of vulnerabilities. There is a wide variety in the type of attacks on these systems.

The aim of this report is

- Elaborate on feasibility of atomic attacks on the nodes and links in the system.
- Define the terms: likelihhod, impact and risk
- Clarify the assumptions that are going to determine the likelihood and impact of the attack.
- Assess the likelihood, impact and risk associated with these attacks on each sub-component

4.2 Feasibility of Atomic Attacks on Systems

Atomic attacks can be carried out individually or in combination on the system. Figure 4.2 enumerates the different elements of the system which would be subject to the atomic attacks. One of the main distinguishing features between these elements are that some are nodes (end points of the communication system) and others are links.

Table 4.1 has a list of the feasible attacks. Each column corresponds to a particular atomic attack, and the primary elements of the communication system that it targets is marked. It is very important to clarify our methodology here. Only the primary targets, or elements of the communication system that are affected during the atomic attack are marked. The secondary effects are not marked explicitly, but we will comment on them. For example, when a node in attacked, it is possible that some of the incident communication links are also affected. The vice-versa case is also possible.

- EM jamming is an attack where a node is typically targetted and is unable to relieve or transmit wireless messages. It may or may not be independent of the

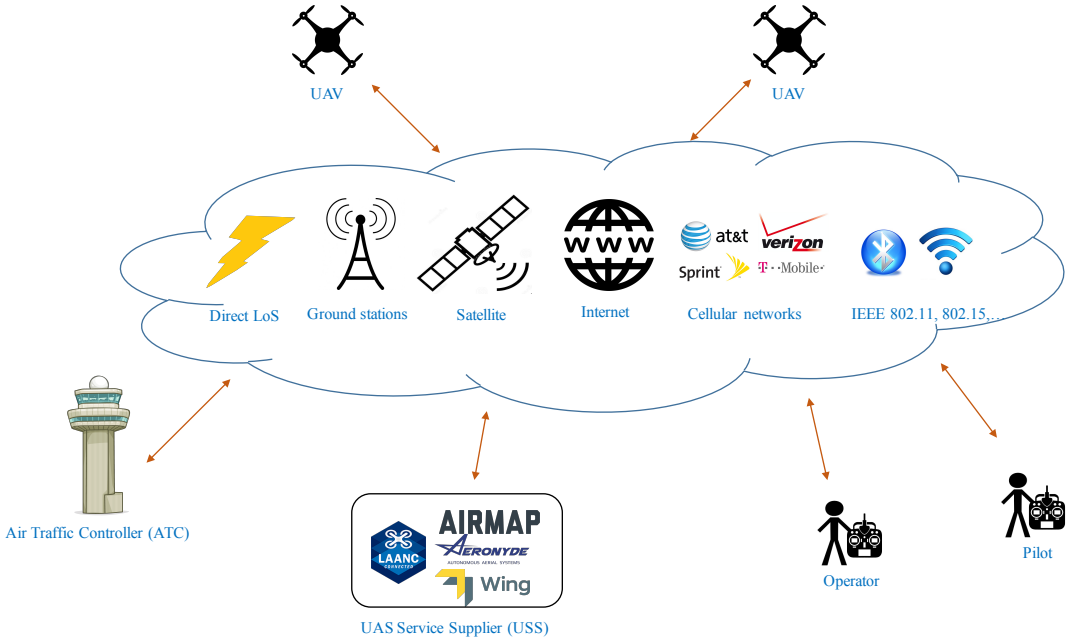

Figure 4.1: Elements of UAS communication

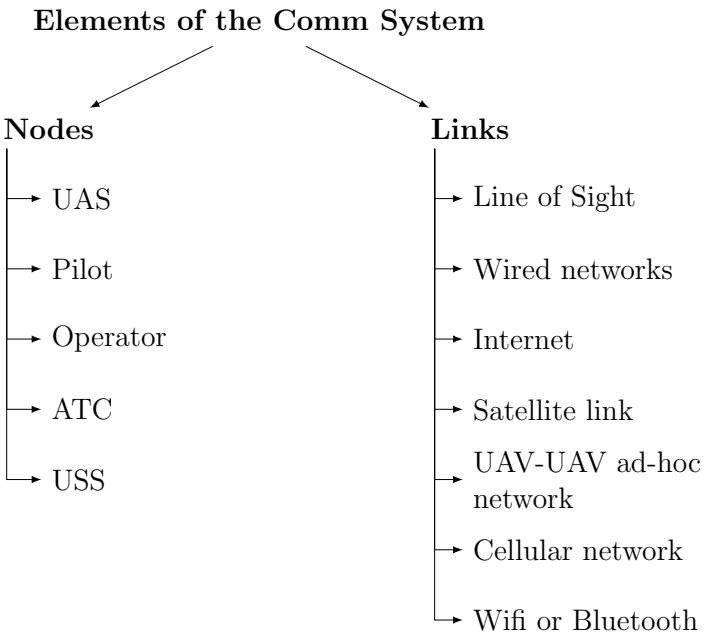

Figure 4.2: Elements of the communication infrastructure

wireless link that is used (radio waves or wifi, say). We categorize EM jamming as a primary attack on the nodes and not on the links itself. This is because of the rational that the jamming is physically performed near a node, even though it may be specific to certain links (depending on the frequencies that get jammed). For instance, a remote pilot may be using a local bluetooth network to control a vehicle, but using a satcomm to remain in contact with the ATC. It is possible for an attacker to jam the bluetooth link and not the satcomm. Other examples of links that are incident on a node, and can be selectively jammed are the Line of Sight communications, cellular networks and any other ad-hoc network. EM jamming prevents any form of communication from happening on links incident on the attacked node. In our classification, this would be different from the message deletion atomic attack because the latter is performed physically at the link level, and is completely independent of the nodes that are involved.

- Equipment malfunction can be performed at nodes, because they are critical for the communication task, or on certain links that are relatively centralized and have known, and easily accessible physical infrastructure that can be damaged. The ATC facilities, remote pilot, or the the vehicle itself are clear targets for equipment damage. Line of Sight communication requires specific ground infrastructure and antenna, which are vulnerable targets. Wired communication also can simply be tampered or cut. Equipment malfunction is not a primary concern on highly distributed systems like Cellular, Ad-Hoc networks, Satcomm, or the Internet. Compromising one equipment is not sufficient to completely disrupt the communication link. However, it may be possible that they can be affected if the node (vehicle, ATC or pilot) are attacked directly.

- Eavesdropping is a link level attack, and can be performed physically by listening in to LoS radio communications (as it is not encrypted currently), tapping onto wired communication, unencrypted satellite based communication or listening to ad-hoc networks that are not encrypted. The internet has a host of security features that encrypt the data. Bluetooth and wifi have encryption inherent in their protocol. Since the ends of the communication link are always nodes, indirectly, this atomic attack also affects the nodes (all three of them).

- Deleting a message requires sending interference signals for wireless links. However to delete a message, one must be able to understand and parse it, which is the same requirement for eavesdropping. Hence, it is only possible to do it for LoS voice communications, wired non-encrypted communications, the GPS part of a satellite link and non-encrypted ad-hoc networks.

- Message modification ans insertion have similar requirements as message deletion and is possible only on the same set of links.

- Malicious software can affect all parts of the system. We consider the attack to be primarily on the nodes. The malicious software can induce several forms of manipulation, ranging from modifying, deleting, or inserting messages. In fact, software level attacks can also easily compromise the confidentiality of the transmission. By far, these also have the greatest potential to spread from one system element to another, and compromise the entire network. Only direct Line of Sight Radio links, and wired networks, that have very limited software components, are immune from

	EM Jamming	Equipment Malfunction	Eavesdropping	Message Deletion	Message Modification	Message insertion	Malware /Spyware	Network Protocol	Social Engineering
ATC/USS	✓	✓					✓		✓
Pilot	✓	✓					✓		✓
Vehicle	✓	✓					✓		
LoS: Voice		✓	✓	✓	✓	✓			
Wired		✓	✓	✓	✓	✓			
Internet								✓	
Satcomm: Datalink + GPS			✓	✓	✓	✓			
Ad-hoc			✓	✓	✓	✓		✓	
Cellular								✓	
WiFi + Bluetooth								✓	

Table 4.1: Atomic attacks and their applicability to systems

these attacks. The attacks on internet, cellular, wifi/bluetooth, and ah-hoc links are typically performed at the protocol level, and get categorized as a network protocol attack.

- Network protocol attacks are performed on links where such protocols play a significant role. These include the internet (which runs on a stack of protocols at several layers, ranging from the physical to application), ad hoc networks, cellular and wifi /bluetooth.

- Social engineering, by its very definition involves attacks that exploit human tendencies and weaknesses. The ideal target for these attacks are the Pilot or the ATC nodes, where there is significant human involvement.

Before we end the section, it is important to emphasize that while there is a primary element of the comm system (either a node or a link) that atomic attacks may target, there could be several secondary effects too. Our aim was to identify and emphasize the primary point of entry from the view of security (which we will discuss later). Hence, attacks on certain nodes can compromise corresponding links (like jamming done at a node, but for a specific frequency) or attacks on links can compromise the node. An example of the latter is a a remote pilot who communicates with a done via bluetooth. If the bluetooth link is attacked, then effectively, the pilot node is also attacked, since there is no alternate means of communication for the pilot. Even an attack on one node can affect the other, for instance if the same drone was subject to EM jamming for the bluetooth frequency (which is primarily an attack on the Vehicle node), the pilot too becomes effectively incapacitated. Thus, a more comprehensive framework to do this analysis would be to take a specific communication architecture and construct a graph with a node each for the vehicle, ATC or pilot, and appropriate edges as per the architecture. Then the following situations can happen

1. All links incident on a node are compromised leading to node being compromised

2. A node being attacked leading to all incident links being compromised

3. Partial attack of a node, leading to some links being compromised

4. A fraction, or specific links being attacked, leading to partial compromise on a node

4.3 Likelihood, Impact and Risk

We have presented several atomic attacks that can be deployed on elements of the UAS communication infrastructure shown in Figure 4.1. Specifically, these elements are the nodes (UAV, ATC, pilot) or links (Line of Sight, Ground stations, cellular infrastructure, satellites, internet, IEEE protocols, ad-hoc networks, fiber optic cables). The detailed analysis of these atomic attacks on these elements of the comm system is the focus of this section. In the analysis, each element is considered and the motivation, means and risk assessment for the feasible atomic attacks (from Table 4.1) is conducted.

The motiation and means of an attacker is important to determine the threat level, and plan appropriate defense strategies. We present the classification methodology from [53] and use the same for our analysis. There are four dimensions of interest:

1. *Membership: Inside versus Outside* An inside attacker is an authenticated and trusted part of the communication setup.

2. *Motivation: Strategic versus Opportunistic* An opportunistic attacker has no intent except general, un-targeted disruption of the communication infrastructure. A strategic attacker has a clear objective, and is typically going to benefit from the attack and is more predictable.

3. *Method: Active versus Passive* Active attackers generate signals or packets, and modifies the existing system. A passive attacker is just an eavesdropper, not directly inducing any harm.

4. *Scope: Local versus Extended* A local attacker only controls or attacks one element of the communication system (either a node or a link), whereas an extended attacker controls several entities spread over a network

These four dimensions give 16 permutations of attacker type. Practically, only some of them are possible. For these, we assign a likelihood of occurrence of the attack. There are three levels of likelihood that we assign:

- *Low:* There is technological limitations and practical constraints that make it very hard to conduct such a type of attack.

- *Medium:* While some effort is required, these are possible, and can be carried out with sufficient planning.

- *High:* There are no technological limitations, and it is very easy to practically carry out the attack by even amateurs.

In addition to likelihood, every attack has an associated Impact, in the event that it materializes. We categorize the impact into three levels:

- *Low:* Impact is local in scope, not leading to loss of an infrastructure element, vehicle or the payload. The effects are reversible, and cause inconvenience to the users, involving time scales of seconds.

- *Medium:* The impact is wider and possibly multiple elements of the system are affected. Disruptions to the service may occur for time scales of minutes.

Likelihood	Impact	Risk
Low	Low	Low
Low	Medium	Low
Medium	Low	Low
Low	High	Medium
Medium	Medium	Medium
High	Low	Medium
Medium	High	High
High	Medium	High
High	High	High

Table 4.2: Risk evaluation based on Likelihood and Impact

- *High:* This involves significant impact on the system, potential loss of vehicles or payloads, and disruptions that may last for several hours.

The combination of impact and likelihood determines is a measure of the risk [29]. High risk events are either more likely, or have very high impact, or both. Low risk events on the other hand are either very unlikely to occur and/or have low impact on occurrence. We use Table 4.2 to assign a risk level based on impact and likelihood.

We begin with an analysis of the three nodes, and then move to the links. The format of analysis is the same. A table presents the feasible atomic attacks, the means and motivation, followed by the likelihood impact and risk analysis. We also discuss the reasoning for each permutation of possible attacks (represented in each row of the table), and the associated references.

4.4 Assumptions

Estimate of the likelihood and impact of an attack are extremely sensitive to the assumptions that are made. Hence, we specify these assumptions now, and further highlight which ones are active when analyzing specific nodes and links.

4.4.1 Assumptions on the attacking agent

A1 (a) The attacking agent is internal to the system and an authorized member

(b) The attacking agent is external to the system

A2 The resources of the attacker is limited to commercially available, off-the-shelf components and open source software

A3 (a) There is one attacker who can physically be present in only one location at a time

(b) There are multiple attackers who can operate from several locations simultaneously

A4 Natural disasters or unintended disruptions are not considered as attacks. In fact, even a failure induced due to poor planning or system design is ignored in our threat model

A5 Opportunistic attacks do not involve a significant or high level of effort. We assume that when a lot of effort is needed to carry out an attack, it has strategic motivations.

4.4.2 Assumptions on the nature of communication

C1 (a) Communication is time-sensitive

(b) Communication is not time-sensitive

C2 (a) Communicated information can result in a control action (change in heading, altitude, airspeed etc)

(b) Communicated information is a payload (eg. images, Internet data etc)

C3 (a) The privacy requirement for the transmitted information is low

(b) The privacy requirement for the transmitted information is high

C4 (a) The link is assumed to be the sole means of communicating a particular type of information

(b) The link is assumed to have redundancy and other independent links to communicate the same information exist

4.4.3 Assumptions on UAV systems operations

S1 (a) Vehicle has a primary sense-and-avoid mechanism

(b) Vehicle does not have a sense-and-avoid mechanism

S2 (a) A swarm of UAVs that are conduction a joint operation have an encrypted and digitally authenticated communication protocol with each other

(b) UAV swarms do not have an encrypted or digitally authenticated protocol

S3 (a) One pilot is controlling one UAV

(b) One pilot is controlling multiple UAVs

S4 (a) Pilot and operator are the same person

(b) Pilot is different from the operator and they may not be co-located

S5 (a) Line of sight operation

(b) Beyond line-of-sight operation

S6 Location of operation

(a) Low altitude

(b) High altitude

(c) Urban region

(d) Rural region

(e) Hostile environment

(f) Non-hostile environment

S7 Vehicle has simple internal logic rules to validate the integrity of a message

S8 (a) Vehicle cannot operate autonomously for any duration of time if communication is lost

(b) Vehicle can operate for upto 5 min autonomously after loss of communication

(c) Vehicle can autonomously operate safely indefinitely after loss of communication

4.4.4 Assumptions on baseline security of links

L1 (a) Satellite communication used proprietary encryption technology

(b) Satellite communication does not use encryption

L2 Physical transmission wires can only be tapped by cutting the link entirely. Modification/insertion/deletion of messages is not considered practical

L3 (a) Remote pilot infrastructure at are secure facilities (e.g. military)

(b) Remote pilot infrastructure is not a secure facility

L4 The Cellular communication messages are secure during the transit

L5 (a) An attacking airborne vehicle cannot follow its target

(b) An attacking airborne vehicle can follow and remain in the proximity of the target

L6 Internet is assumed to be safe for communication as long as the appropriate protocols are followed at the end points. However, there are no guarantee on the latency or the reliability of the channel.

L7 ATC and USS facilities are well monitored, guarded, and secure. EM jamming is not possible as a very high power jammer would be required to create the desired effect, and would easily be spotted.

L8 (a) EM jamming is carried out by an outside element

(b) EM jamming is carried out by an inside element

L9 It is not possible to modify or delete LoS messages intended for a moving target.

L10 Assuming appropriate encryption is performed before transmission, the Internet is assumed to be a private mode of communication, where the message cannot be modified or inserted. It can however be deleted.

L11 (a) Bluetooth and WiFi connections are paired safely

(b) Pairing is not guaranteed to be performed safely for Bluetooth and WiFi connections

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Medium	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
Malicious Software	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Active	Extended	Low	Low	Low
	Strategic	Inside	Active	Local	Medium	Low	Low
	Strategic	Inside	Active	Extended	Low	Low	Low
Social Engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Low	Low

Table 4.3: Air traffic control and USS node analysis

4.5 Systems level impact on nodes and links

4.5.1 ATC / USS

For the purposes of this section, since the ATC and USS are similar ground based facilities that provide traffic services, they are Air traffic controllers and their facilities have several different communication links active at any given instant. They involve a significant amount of voice communication through radios, connections to other ATC facilities through telephones, internet and satellite links for real time data streams, and connection to an extensive network of surveillance systems. All the vulnerabilities that exist for these links, can affect the ATC node too. Here we will focus on the node level vulnerabilities. **Assumptions**: A1(b), A2, A3(a), A4, A5, C1(b), C2(a), C3(a), S1(a), S6(f), S7, S8(c), L7 and L8(a).

- EM jamming can be used to prevent any of the wireless communication from occurring. They may be strategic or opportunistic, require an external attacker with the appropriate equipment, and an active attack. Strategic EM jamming is when a particular time period or set of communications need to be blocked, whereas an opportunistic attack would just pick any of the frequencies in use, and make it unavailable. Local attacks involve only one ATC facility, whereas extended attacks may involve several nodes. In all, the likelihood of any of these attacks are very low. It requires very high power to jam the signals coming from these major aviation infrastructures that are well monitored and protected. Also, the impact of jamming is also limited since there is so much redundancy in the system.

- Equipment malfunction for ATC involves physically damaging the wireless receivers/ transmitters or physical wiring. They are carried out by agents external to the system, lead to an active interference in the communications and may affect one or many ATC facilities. As expected, performing any of these sabotage operations is very hard due to the secure nature of these facilities. Multiple redundancies makes the impact of any such malfunction also low.

- Malicious software can lead to messages getting modified, delayed, deleted or even transmitted to a third-party eavesdropper. The software is always introduced from inside the system and actively disrupts communication. In general, introducing a malicious software for opportunistic purpose is very unlikely, as the ATC is one of the safest elements of the UAS comm infrastructure and has a suite of software that can protect it from malicious attacks. However, as with any software system, a determined strategic attacker may be able to introduce some malware (often with

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Medium	Medium	Medium
	Opportunistic	Outside	Active	Extended	Low	Medium	Low
	Strategic	Outside	Active	Local	High	Medium	High
	Strategic	Outside	Active	Extended	Low	Medium	Low
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Malicious Software	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Active	Extended	Low	Medium	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Opportunistic	Inside	Passive	Extended	Low	Low	Low
	Strategic	Inside	Active	Local	Medium	Medium	Medium
	Strategic	Inside	Active	Extended	Low	High	Medium
	Strategic	Inside	Passive	Local	Medium	Low	Low
	Strategic	Inside	Passive	Extended	Low	Low	Low
Social engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Passive	Local	Medium	Low	Low
	Strategic	Inside	Active	Local	Low	Medium	Low
	Strategic	Inside	Passive	Local	Medium	Low	Low

Table 4.4: UAS operator

a combination of some social engineering to obtain access to these systems) on one such system, justifying the label of medium for the likelihood of this event. The impact is however low for all cases, as these malicious lines of codes will easily get detected by the security systems.

- Social engineering attacks involve impersonation to gain access to the control tower or facilities, or atleast some amount of deception to get physically close to set up malicious hardware, or physically damage the infrastructure. It may be opportunistic or strategic, but is very unlikely to occur, and has a low impact.

4.5.2 Pilot

The pilot or operator of a UAS would maintain some form of communication with the ATC, to resolve traffic conflicts, and with the vehicle, in order to provide control inputs or transfer other forms of mission data. There is significant variability in the types of connections that are maintained and the data that is transferred. Some remote pilot facilities, like the ones used by the military, have security considerations incorporated in their design itself, and have state-of-the art encrypted and authenticated channels. Amateur or even commercial organizations may involve a light-weight setup at remote locations to perform simpler tasks like monitoring an agricultural service drone. We emphasize that in practice, the operator and the pilot-in-command may be different people, located at different locations. This may necessitate additional pilot-operator communication. The primary difference between the analysis of these separate nodes would be the difference in tasks (tactical control versus setting higher level goals) and the time scale for decision making (order of seconds versus minutes or hours). In most cases, loss of communication between the operator and pilot-in-command, or a full attack on the pilot-in-command node is not catastrophic, since the operator can continue to make tactical decisions and complete the mission even if it is not performed optimally. In Table 4.4, we consider the node to be an operator.
Assumptions: A1(b), A2, A3(a), A5, C1(a), C2(a), S1(a), S4(a), S5(b), S7, S8(b), L3(b), L8(a)

- Typically the operator is stationary at a fixed location. The ease of attack may vary significantly between a military control station and others. Military operators and their nodes will have a low probability of EM jamming as it would no be possible to get into close physical proximity while avoiding detection even for a strongly motivated attacker. So we restrict ourselves to the more typical commercial, or

hobby remote operator. The attack motivation may be strategic or opportunistic. Also the attack scope may be local and limited to one operator, or may be extended and cover several operators and the pilot (if they are not the same person and located in a different place). Extended attacks are difficult to coordinate and very unlikely. However, it is relatively straightforward to attack one node by placing a jamming transmitter in the neighborhood. It is further easier if the attacker is well motivated and has an incentive to disrupt the communication system.

- The equipment of the remote operator can be attacked with strategic or opportunistic intent. We only consider local scope because for this analysis, if the operator and pilot are in different locations, they can be analyzed independently. Likelihood of physically damaging the equipment is low, although the impact may be higher if a strategic attack is carried out with clear intentions.

- Malicious software attacks on the operator node can be used to interfere with the command and control of the vehicle or eavesdrop on sensitive mission payload (for e.g images that map natural resources in a region). They may be active, meaning they interfere in the communication, or passive by eavesdropping and sending the information outside the system. The scope of the software may be local to the UAS operator node or may be designed to spread and create an extended attack. The likelihood of all the possibilities are typically low, but depends on the other links that it is connected to. Since software can be easily transmitted into the node via the links, the node is only as secure as the weakest link. The weakest link would be the internet, which is open to the world, and does not have a dearth of motivated attackers. This gives a medium likelihood to a strategic local attack on the node (assuming at least one very weak link). Even in such cases, extended attacks are harder, since the outside attacker may not know the details of the other elements of the system in order to spread the malware. The impact of malicious software depends on how much it spreads (local versus extended), and how determined the attacker is (strategic versus opportunistic).

- A socially engineered attack on the UAS pilot/operator node would involve involve setting up eavesdropping equipment near the operator (which leads to a passive attack) or other human-oriented strategies like impersonation leading to incorrect command instructions (active attack). These attacks may further be strategic or opportunistic. Passive eavesdropping attacks have a medium likelihood, especially if some of the links used (e.g LoS voice) are not encrypted. However, their impact on the system is low. Strategic active attacks are difficult to carry out, but do have a medium impact. Phishing attacks are also possible on the operator, who may provide valuable information to an attacker impersonating some one else.

4.5.3 Unmanned Vehicle

A special characteristic of the vehicle, in comparison to the other two nodes (ATC and pilot) is that it is a mobile target for attacks. This makes most attacks more challenging to carry out from an engineering view point, but also lead to higher impact as the vehicle is the most critical part of the mission. There is a wide variation in the functional capabilities of the vehicles. For instance, hobby drones, commercial inspection vehicles, delivery drones, and military surveillance drones. The ease for attacking these different

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Medium	Low	Low
	Opportunistic	Outside	Active	Extended	Low	High	Medium
	Opportunistic	Inside	Active	Local	Low	High	Medium
	Strategic	Outside	Active	Local	Medium	Low	Low
	Strategic	Outside	Active	Extended	Low	High	Medium
	Strategic	Inside	Active	Local	Low	High	Medium
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Malicious Software	Opportunistic	Inside	Active	Local	Medium	Medium	Medium
	Opportunistic	Inside	Active	Extended	Low	Medium	Low
	Opportunistic	Inside	Passive	Local	Medium	Low	Low
	Opportunistic	Inside	Passive	External	Low	Low	Low
	Strategic	Inside	Active	Local	Medium	Medium	Medium
	Strategic	Inside	Active	External	Low	High	Medium
	Strategic	Inside	Passive	Local	Medium	Low	Low
	Strategic	Inside	Passive	External	Low	Low	Low

Table 4.5: Vehicle

types of drones is different. Further the operating altitudes, and regions also differ. Some may be low level operations in urban settings, making it vulnerable for jamming from the ground, whereas the high altitude surveillance drone
Assumptions: A1(a-b), A2, A3(a), A5, C1(a), C2(a), S1(a), S5(b), S8(a), L8(a-b)

- EM jamming can be strategic or opportunistic. Local attack targets one node, or just one small area of airspace where the signals are jammed. Extended attacks are harder to perform than local attacks, as coordination over multiple nodes, or jamming larger volumes of airspace needs significant technical effort and motivation. Hence extended attacks have a low likelihood of occurrence. Strategic local attacks are the easiest to perform as the attacker is well motivated, and jamming a a low flying vehicle (which is the case for many applications) or small geographical areas is easy to perform. A similar jamming attack by a motivated individual over larger geographical areas is possible, but requires more effort. Jamming a volume of airspace is easier to achieve, since a transmitter can be placed on the ground. To continuously jam a moving vehicle, one would require the jamming transmitter to be in constant motion and close proximity to the target. It may be possible to achieve it in the, with a jammer on a mobile platform such as a drone itself, but requires significant technological advances to track and follow a target. To summarize, inside attacks require aerial jamming and target tracking, and are low likelihood, high impact attacks. Attacks that are local jam a small region of airspace, and have medium likelihood and low impact as the vehicle can fly out of that region soon. The extended attacks are low likelihood events, but have a high impact.

- Equipment malfunction is is hard since the drones are usually stored safely, or under supervision of the operator or pilot. Hence the likelihood of damaging onboard comm equipment is very low.

- Malicious software is said to be strategic if they intend to affect specific parts of the communication system, or have an intended target vehicle. Opportunistic attacks are agnostic to the vehicle and just intend to create any form of disruption. Software modifications can have very high specificity, and a strategic attacker can achieve very precise disruptions that can have significant impact. Active attacks disrupt the communication, whereas passive attacks have very low impact as they share the mission specific information to outside agents. In an extended attack, the software is designed to spread from the initial point of introduction to several other elements (which could be other vehicles or the operator) making them very high

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Equipment malfunction	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Medium	Low
Eavesdropping	Opportunistic	Outside	Passive	Extended	High	Low	Medium
	Strategic	Outside	Passive	Extended	High	Medium	High
Message Modification	Strategic	Outside	Active	Local	Low	Medium	Low
Message Deletion	Strategic	Outside	Active	Local	Low	Medium	Low
Message Insertion	Opportunistic	Outside	Passive	Extended	High	Low	Medium
	Strategic	Outside	Passive	Extended	High	Medium	Medium

Table 4.6: Line of Sight communication: digital and voice communications

impact attacks. All of these attacks on the vehicle however would require a point of entry for the software. This is possible by physical tampering of the hardware, during software updates, or through other communication links like internet, wifi or bluetooth. The more secure vehicles do not have these non-secure links such as to the internet and only maintain internal links with trusted elements of the system.

4.5.4 Line of Sight: Digital communications and Voice

Line of sight communication using radio waves is used by present air traffic controllers to maintain contact with pilots through voice. In addition, an extensive network of ground stations can also used for surveillance and maintaining digital communication with a moving vehicle (ACARS or CPDLC). The traditional voice link connects ATC to pilots of manned aircraft and has no inherent security features: it is neither-authenticated nor encrypted.

References: [68, 10, 67, 62]

Assumptions: A1(a-b), A3(a), A5, C1(a-b), C2(a), C3(a-b), C4(a-b), S7, S8(b), L5(a), L9

- Equipment malfunction is not easy, as there is usually some form of surveillance or monitoring of these ground stations. While damage to a ground station may impact coverage, it is usually not a major concern as there is redundancy. In fact at any geographical location in continental USA, more than one ground station can usually track and communicate with a target through line of sight. Because the disruption is very limited, and possibly for a short duration only before backup systems come online, only strategic attackers, with a clear intent or motivation would perform these attacks.

- The weakest element of voice communication through radios is that all conversations are public knowledge. In fact there are so many free sources that record these ATC communications and publish it on the internet. These attacks are easy to perform and just setting up a single receiver equipment would allow the monitoring of several frequencies, that are used to connect multiple vehicles, operators or pilots and ATC personnel. However, since its a passive attack, it has almost no direct impact on the mission. However, important information regarding the location of operations and nature of mission could be very critical for military applications. Thus the impact of a strategic eavesdropper may be higher than an opportunistic one. Even digital communications using CPDLC, which is currently used by commercial aircraft are not encrypted.

- Modifying a message requires sophisticated equipment that can decipher, delete parts of it (through some for of EM interference), and transmitting the modified message at a higher power. This is challenging for voice communications, because

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Equipment malfunction	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Medium	Low
Eavesdropping	Strategic	Outside	Passive	Extended	High	Medium	High
Message Modification	Strategic	Outside	Active	Local	Low	Medium	Low
Message Deletion	Strategic	Outside	Active	Local	Low	Medium	Low
Message Insertion	Strategic	Outside	Passive	Extended	High	Medium	Medium

Table 4.7: Wired networks

deleting a part of a message is going to increase ambient noise making the new transmission hard to decipher. The same holds for digital decoders. Destructive interference puts a constraint on the physical location an attacker must be at in relation to the transmitter and receiver. This practically makes it impossible to perform the attack on a moving aerial vehicle.

- Message deletion faces the same challenges as message modification, namely location constraints and a moving target, that makes it not a serious threat.

- With no authentication and encryption for voice, message insertion is very easy to perform. Usually, the impact is not significant because the inserted message can be heard by all parties, and it would become apparent that the channel is compromised. Instruction read backs, which is a standard practice in all radio communication acts as another layer of security. If Line of Sight was used for digital communication, then adding encryption and authentication could make it very hard to insert messages. However, Controller Pilot Data Link (CPDLC) does not have any encryption standards.

4.5.5 Wired networks

Wired networks can be used between the Air Traffic Controllers, pilots and operators of UAVs. It is not a feasible mode to communicate with a flying vehicle. The Federal telecommunication network (FTN) is used currently by the ATC facility to coordinate operations with other facilities and the FAA command center. Remote pilots or operators can potentially tap into this network, through a regular telephone call, or a cellular intermediary to maintain contact with the controllers. Private wired networks, although an expensive infrastructure have far less security vulnerabilities than wireless links. A major disadvantage is that they require significant expenses to expand and connect new remote pilot facilities. These links can be used for obtaining clearances, as well as strategic and tactical conflict resolution.
Assumptions: A1(b), A4, A5, L2

- Wired networks are hard to tamper, and depending on the location of the damage, the effect could be local or extended.

- Eavesdropping, message modification, deletion and insertion are not possible unless there is an intermediate device that is inserted in the wired network. Even if that is done, then communication must not be encrypted for any of these attacks.

4.5.6 Internet

The internet is an extremely large scale, decentralized amalgam of software protocols and physical hardware that can serve as a communication channel for all connected devices.

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Network protocol	Opportunistic	Outside	Passive	Local	Low	Low	Low
	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Passive	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low

Table 4.8: Internet link (used for time-insensitive communication)

It is relatively straightforward for all the nodes to connect to the internet, either through broadband cable service if available, or through cellular or satellite links. Because of the decentralized nature of the internet, it would typically not be used for time sensitive communication, since there are no delay performance guarantees for that network. A possible use case for the internet would be for a vehicle to upload data that it obtained during a mission to the cloud, or for it to submit reports of the weather conditions experienced during flight. In general, since the internet is a system external to the UAS architecture, modifying its security properties is not easy. While using the internet link for communication improves functionality, it also inherits all the classic security and threats that face the internet ecosystem.

Assumptions: A1(b), A5, C1(b), C2(b), C4(b), L6, L10

Protocol based attacks on the internet can involve a range of denial of service type of disruption. In these, several properties of the internet protocols are exploited to use up a resource and make it unavailable for the intended user. There are several different forms of a denial of service attack. However, the likelihood and impact of these attacks on the internet as a UAV communication link is very low. There are two reasons for this. The first is that internet security is a relatively mature field, with a host of defense techniques and algorithms already in place. Secondly, because of the inherent unreliability of the internet link of time-sensitive tasks, the disruption is unlikely to have mission critical impact. It would be highly inadvisable to use the internet for critical communication between the system elements. The attacks could be passive, with the only intent being eavesdropping on the communication, or actively trying to prevent the communication. Eavesdropping is virtually impossible with security, firewalls and encryption at all layers. Overall, assuming that the information transmitted using an internet is not time sensitive (but still requires confidentiality), and the users of the system are aware of that, it is a very low risk link. However, the moment availability of the link becomes an issue, or performance guarantees are required, then the the likelihood and impact of an active, strategic attack on the link rises to a 'Medium' level.

While the only atomic attack on the internet link is the network protocol attack, there could be several secondary effects that are induced from that attack. Message insertion, deletion and eavesdropping could be induced by the network protocol attack.

4.5.7 Satellite Communications: GPS and Datalink

Satellites can be used for two purposes. One is to obtain GPS coordinates, and the other function is to serve as a datalink. The UAS obtains signals from atleast four GPS satellites, that are in its direct line of sight to triangulate and obtain the position. Data-link services are provided by different commercial entities using their own proprietary protocols and satellite infrastructure. The data-link is currently used for communicating flight path instructions between pilots and ATC, communication with the company (operating airline), live weather information, and for ancillary entertainment and internet service for the passengers. There is wide variety in the requirements for the communication channel in terms of latency, and streaming rate for the data.

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	-	-	-	-	-	-	-
Message deletion	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Message modification	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	High	Medium
Message insertion	-	-	-	-	-	-	-

Table 4.9: Satellite communication: GPS

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	Opportunistic	Outside	Passive	Local	Medium	Low	Low
	Strategic	Outside	Passive	Local	Medium	Low	Low
Message deletion	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Message modification	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Message insertion	Opportunistic	Outside	Active	Local	Low	High	Medium
	Opportunistic	Outside	Active	Local	Medium	High	High

Table 4.10: Satellite communication: Datalink

In this attack, a modified message is sent to the receiver in the vehicle, that makes the vehicle believe it is in a different location. Modifying a GPS message can be done only with a specific receiver in mind. Hence, it is performed only with a rational intent. To spoof a GPS message, one requires a transmitter in close proximity to a flying UAV. That could be due to a UAV that's Inside or Outside the system. Spoofing is very delicate, involving transmittion of specific fake messages at particular time instants. It is not possible to do it for multiple aerial vehicles at the same time.

In oceanic airspace, where there are no ground stations for Line of Sight communications, satellite datalinks are a crucial means of communication. This may also be the case for vehicles flying at low altitudes (as LoS range increases with altitude). In such cases, the current protocol (CPDLC) offers very low levels of security against message insertion, and eavesdropping.

References: [40]

Assumptions (GPS): A1(a-b), A2, A3(a), A4, A5, C1(a), C2(a), C3(a), C4(a), S1(a), S8(b), S6(f) , L1(b)

Assumptions (Datalink): A1(b), A2, A3(a), A4, A5, C1(a), C2(a-b), C3(a-b), C4(a-b), S1(a), S8(b), L1(b)

- GPS is indispensable for most aerial vehicles. There is no notion of eavesdropping on that signal, because it is publicly broadcasted by the satellites. Deleting GPS messages at the link level (recall that jamming is a node level attack) requires destructive interference which can only be done while remaining in close proximity to the target. The impact of strategically deleting it would be that that vehicle may be forced to land immediately or rely on its inertial navigation systems. If the deletion is timed appropriately, it may lead to mission failure, hence the medium impact. Modifying the message is more challenging than deletion, however its impact is even more severe. In fact the cause of the capture of a US Senteniel drone by Iran is attributed to GPS modification. It is not meaningful to discuss message insertion, because the original GPS signal is always present, and adding additional sources does not necessarily mean anything.

- Datalink communication, specifically CPDLC in oceanic airspace is enabled via satellites. These signals are non-encrypted and non-authenticated. Eavesdropping however would require some receiver in the vicinity of the vehicle, and it may not be accessible easily. Deleting or modifying messages pose the same issues as with the GPS signal, namely proximity to a moving target which is not easy. Modifying

or deleting critical messages by a strategic attacker has the same effect for datalink (unlike the GPS, where a deleted message might require the vehicle to assume lost signal and follow a standard protocol). Inserting messages, although easy because of no encryption or authentication, may be hard to achieve since the transmitter needs to be physically close. The impact remains high though.

4.5.8 UAV-UAV ad-hoc communication networks

UAVs can create a decentralized, ad-hoc communication network to coordinate and perform tasks. As an example, a group of vehicles that are performing a joint task of search and rescue, could ensure that they communicate with each other through this network. They can share information that they individually acquire or alert others of already scanned regions. In other applications, only one of the vehicles may be in direct LoS contact with the operator or ground station. In that case all other vehicles can use the UAV-UAV network to maintain communication with the operator. As a final example, these UAV ad-hoc networks can be used to provide wireless connectivity (either cellular, or internet) to terrestrial users across a wide geographic region. The advantage of this communication link is that they are extremely flexible, can dynamically adapt to variable number of connected vehicles, and require no additional infrastructure that is specific to the mission.

The distributed nature of ad-hoc networks requires each connected vehicle to perform certain network routing tasks. Protocols dictate how the nodes will communicate with each, which paths to follow to connect vehicle A to vehicle B (in general, there will not be a 1-hop path), and keep track of the overall network topology (what are the vehicles that each one is connected to). These suite of distributed protocols typically assume cooperation from all agents in the system. For instance, every node in this ad-hoc network (a vehicle) is expected to dutifully forward packets it is supposed to, present a true picture of the other nodes visible to it, and not modify the relayed message. Depending on how flexible the architecture is, the ad-hoc network may be secure, meaning only authenticated vehicles may join it (for instance, they might have to be owned by the same company, or operator), or more open and flexible, where any vehicle in the vicinity could offer to pool resources and join the ad-hoc network (for collision avoidance and transmitting location and maneuvering intentions). Both formats may be operational simultaneously for different applications. Sharing mission critical data may be possible only in an authenticated ad-hoc network, whereas traffic information is an open network. Naturally, the threat levels vary for both. For an authenticated ad-hoc network, only Inside attacks, where the attacker is a member of the system is possible. On the other hans, both Inside and Outside attacks are feasible for an open ad-hoc network.

References: [21]

Most forms of DoS attacks requires the attacker to be inside the system, active, and can only control a local element.

Assumptions: A1(a), A5, C2(a-b), C4(a), S2(a), S8(c), L5(b)

- Eavesdropping is possible by an Outside member in case of open ad-hoc networks or by an in Inside agent in case of an authenticated network. They are all passive, extended attacks. In all permutations, the impact is low, except for a strategic outsider, who may be able to benefit. The likelihood of an outside strategic eavesdropper on an open network is High, and Low for a authenticated network.

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	Opportunistic	Inside	Passive	Extended	Low	Low	Low
	Opportunistic	Outside	Passive	Extended	Low	Low	Low
	Strategic	Inside	Passive	Extended	Medium	Low	Low
	Strategic	Outside	Passive	Extended	Medium	Medium	Medium
Message deletion	Strategic	Inside	Active	Extended	Medium	Medium	Medium
Message modification	Strategic	Inside	Active	Extended	Medium	Medium	Medium
Message insertion	Opportunistic	Inside	Active	Medium	Low	High	Medium
Network protocol	Strategic	Inside	Active	Extended	Medium	High	High
	Strategic	Inside	Passive	Extended	Medium	Low	Low

Table 4.11: UAV - UAV ad-hoc networks

Considering both extremes, we categorize it as Medium. For an attacker with no strategic intentions, likelihood of eavesdropping on these highly mobile networks is low.

- Message deletion and modification can be performed only by an Inside member of the network for both open and authenticated systems. It is very easy to perform the attack if the attacker vehicle happens to be an intermediate relay for that signal. However, if other vehicles become aware that the message got deleted or modified, then they may change the route structure and avoid the attacker node (If an attacker wants to sustain that attack in spite of these routing changes, they would have to perform a network protocol attack). These attacks are only carried out with a strategic motivation, are active, and can have an extended scope. Again, since the networks can be open or close, there is a wide variation in the ease of an adversary being a part of the system, an we classify it as Medium likelihood.

- Inserting messages can be done easy if the network is open, and can be done with any motivation (e.g, transmitting a fake location to disrupt UAS operations). These are easy to perform and can have a High. If the network is authenticated, it is less likely, but the impact remains High.

- Network protocol attacks are extremely dangerous as they are are conducted by Inside members, and exploit the decentralized nature of the ad-hoc network to provide the attacker with controlling authority. By nature of attacking the protocols that affect all agents that are a part of the network, they are extended attacks. They are also highly motivated strategic attacks, and carried out from within the system. Active attacks aim to disrupt the communication links, whereas a passive attack may try to reroute all communications through the attacker vehicle in order to eavesdrop. There are relatively few methods to identify and eliminate the attacker in these decentralized systems, making their impact very high. Network protocol attacks indirectly can lead to eavesdropping, message modification, and message deletion.

4.5.9 Cellular Networks

Mobile phone networks, or cellular networks offer reasonable coverage at low altitudes, and in urban areas. Vehicles and remote pilots or operators can leverage this extensive network of existing infrastructure for UAS communication. Another possibility is that drones aid in providing 5G coverage to remote regions, by acting as base stations (e.g., a drone version of project Loon).

Cellular communication has its own vast body of literature related to security and vulnerabilities in such systems. A complete overview of those issues is presented in several

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Network protocol	Strategic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Passive	Local	Low	Low	Low
	Strategic	Outside	Passive	Extended	Low	Low	Low

Table 4.12: Cellular networks

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Network protocol	Strategic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Passive	Local	Low	Low	Low

Table 4.13: Bluetooth and WiFi

references. The extent of vulnerabilities, ease of carrying out attacks, and impact vary for 2G, 2.5G, 3G and 4G networks.
Assumptions: A1(b), A4, A5, C1(b), C2(b), C4(b), S8(c), L4

- Eavesdropping, message modification, message deletion, and message insertion are concerns in cellular networks, but sufficient techniques have been already developed and used to eliminate most of that threat. For details on the security measures that are already existing, see [17].

- Network protocol based attacks are only performed by strategic, outside agents. They can eavesdrop (be passive) or be an active attack. The scope can be local or extended. The most common form of attacks on cellular networks involve affecting the availability of the channel, to either one particular user, or several through Denial of Service attacks. The impact of such loss in channel availability can have an impact on the communication links, in the order of minutes before they get detected and neutralized.

References : [71, 17, 58, 54, 44, 49, 20]

4.5.10 Bluetooth and Wifi networks

Two common standards for communications that are relevant for UAS are IEEE 802.11 for WLAN/WiFI and IEEE 802.15 for Bluetooth communication. The range of Bluetooth ranges from ten to a a few hundred meters. Any two bluetooth devices can be connected through a process of pairing. Multiple (upto seen) devices can be connected through a type of ad-hoc Bluetooth network known as piconet. All Bluetooth devices operate in one of the 4 security modes. The latest version operates on Level 4, which has service level enforced security with encryption. Still pairing remains the most vulnerable process in a Bluetooth connection. Depending on the antenna used, the range for WiFi can be extended for upto 20 miles, but the power consumption is high. WiFi can not only be used by devices to connect to the internet, but also other Wide Area Networks. A typical 802.11 attack involves packet capture followed by de-authentication of link. The protocol explicitly provides for a de-authentication frame, that allows the router to tell a device that it has been deemed rouge and is de-authenticated. It is followed by the malicious agent then authenticating the link and gaining control.
Assumptions: A1(b), A2, A3(a), A5, C1(a), C2(a), L11(b)

Bluetooth attacks can be prevented to a large extent by ensuring that the pairing process is done safely, a strong password is used, and the Bluetooth network is hidden from public. There is an element of social engineering that could be leveraged to carry out these attacks during the pairing stage. WiFi networks on the other hand have some in built

vulnerabilities that can be exploited, and detecting them are challenging. high degree of motivation is required to carry out these attacks, and they are consequently strategic, and not opportunistic. They are carried out by external actors (outside membership), local in scope and may be active (to disrupt communication) or passive (for eavesdropping). Both are equally hard to perform, but the impact of an active attack is higher.

References: [38] provides a full overview of Bluetooth attacks and vulnerabilities.

4.6 Sensitivity to Assumptions

Certain assumptions (or operating conditions) increase the impact of the attack. Higher the number of these active factors, higher is the impact of the attack

- C2(a): Communication leading to a control action
- C4(a): No redundant way to convey the same information
- C3(b): High privacy requirement
- C1(a): Time sensitive communication
- S1(b): Vehicle does not have a sense and avoid mechanism
- S8(a-b): Limited autonomy of the vehicle after the loss of communication

The presence of any one of the them suffices to increase the impact level to medium, and two or more of these factors lead to a high impact.

The likelihood of the attack depends on the potential benefits and the ease of carrying out the attack. Our assumptions can affect both these factors. The impact of an attack determines the potential benefits. The ease of the attack is determined by factors like

- A1: Is the attacker external or internal to the system. Internal attacks are relatively easier
- A2: Resource limited attackers have more challenges
- A3: The number of attackers (similar to A2)
- S2: Baseline level of authentication in the UAV-UAV d hoc network
- S5: Beyond LoS operations will make it harder for the pilot or operator to identify the onset of an attack
- L1-11: All the assumptions on baseline security determine the ease of carrying out an attack.

4.7 Non-intentional disruptions

Several attacks are not intentional and are rather disruptions. These disruptions are due to factors external to the system, and may have a local or extended scope. In Table 4.14, we present some disruptions and a description.

Disruption	Description	Scope	Likelihood	Impact	Risk	Papers
Atmospheric condition	Static in the atmosphere, rain, or hail can affect the propagation characteristics of EM waves	Extended	Low	Medium	Low	
Satellite not in view	A satellite may not be in direct LoS from a vehicle	Extended	Medium	Medium	Medium	
Ground interference	Operations at low altitudes could create unexpected interference for wireless signals with the ground	Local	Low	Low	Low	
Obstruction to Line of Sight	Low altitude ops and operations in urban regions can obstruct the LoS between vehicle and other receivers/transmitters	Local	High	Medium	High	[42]
Aircraft Shadowing	Aggressive maneuvering, which is possible in several UAS can create an artificial shadowing effect, where a part of the aircraft itself blocks the LoS communication between the vehicle and the other communication node.	Local	Low	Low	Low	[65]
Human error	Software bugs, incorrect operation of equipment, or any of the factors that degrade pilot or operator performance	Extended	Low	Low	Low	
Network congestion	If an external network, like cellular, or WiFi is used for UAS communication, congestion on those networks could affect UAS operations	Extended	Medium	Medium	Medium	[37]

Table 4.14: Non-intentional disruptions

Chapter 5

Mitigation Strategies

5.1 Outline

In this chapter, we consider defense strategies against attacks on UAV communications. We present three ideas:

1. The high and medium risk cases from Chapter 4 (Table 5.2 and Table 5.1) are discussed. This is one of the main reason for performing the threat analysis- identification of high risk attacks.

2. An overview of the defense and mitigations strategies

3. A detailed analysis of detection and mitigation strategies against the atomic attacks discussed earlier. Further, the feasibility and effectiveness of these strategies, along with the trade-offs are also presented.

5.2 The high and medium risk cases

The specific attack combinations that lead to high and medium risk are extracted from Chapter 4 and presented in Table 5.1 and 5.2. There are several interesting insights to draw from these tables:

- The classification of a threat as high or medium risk is a strong function of the system capabilities and mission requirements. These are captured as the assumptions in Chapter 4.

- The high risk attacks are all strategic in their motivation.

- It is interesting that eavesdropping, even though passive can become a high risk attack. This can happen in situations where the information transmitted contains valuable payload information, like readings from a sensor network or trajectory data about secret military operations.

- The UAS operator is the only nodal element that has a high risk attack. The ATC., or the USS node is typically an established facility, and the mobile nature of the vehicle makes it a relatively safer element.

Element	Atomic Attack	Motivation	Membership	Method	Scope
UAS operator	EM Jamming	Strategic	Outside	Active	Local
Line of Sight Link	Eavesdropping	Strategic	Outside	Passive	Extended
Wired networks	Eavesdropping	Strategic	Outside	Passive	Extended
Satellite datalink	Message Insertion	Strategic	Outside	Active	Local
UAV-UAV ad-hoc network	Network protocol	Strategic	Inside	Active	Extended

Table 5.1: High Risk

Element	Atomic Attack	Motivation	Membership	Method	Scope
UAS Operator	EM Jamming	Opportunistic	Outside	Active	Local
	Malicious software	Strategic	Inside	Active	Local
		Strategic	Inside	Active	Extended
Vehicle	EM Jamming	Opportunistic	Outside	Active	Extended
		Opportunistic	Inside	Active	Extended
		Strategic	Outside	Active	Extended
		Strategic	Inside	Active	Extended
	Malicious Software	Strategic	Outside	Active	Local
		Strategic	Outside	Active	Local
		Strategic	Outside	Active	Local
Line of Sight Comm	Eavesdropping	Opportunistic	Outside	Passive	Extended
	Message Insertion	Opportunistic	Outside	Active	Extended
		Strategic	Outside	Active	Extended
Wired Networks	Message Insertion	Strategic	Outside	Passive	Extended
Satellite Communication (GPS)	Message modification	Strategic	Outside	Active	Local
Satellite Communication (Datalink)	Message insertion	Opportunistic	Outside	Active	Local
UAV-UAV ad-hoc network	Eavesdropping	Strategic	Outside	Passive	Extended
	Message deletion	Strategic	Inside	Active	Extended
	Message modification	Strategic	Inside	Active	Extended
	Message insertion	Opportunistic	Inside	Active	Extended

Table 5.2: Medium Risk

- There are significantly more attacks on nodes and links that are in the medium risk category than a higher risk category. This is expected in any system with good design (i.e realistic assumptions in our case).
- The Internet, cellular, and Bluetooth are communication links that are neither medium nor high risk elements for this particular set of assumptions. However, it is also worth mentioning that they do not satisfy a lot fo requirements for communication links. For instance, even thought he internet may be relatively risk-free due to the whole suite of encryption technologies, it does not offer a low latency or continuous availability- factors that may be critical for a certain application, thus making it unsuitable for the application.

5.3 General Defense Strategies

Table 5.3 outlines broad defense strategies that can be employed against attacks. Several mitigations strategies fall into these major categories, and differ in their implementation depending on the specific node or link being protected. In the next section, we describe some of the more specific instances in which these strategies are realized.

5.4 Defense Strategies Against Atomic Attacks

We list the atomic attacks, and summarize an outline of the defense against them (Table 5.4). Specifically, we list out atomic attacks and present two types of defenses: Detection (D) and Mitigation (M). Detection involves techniques that can identify when an attack is occurring, and that can be used to initiate counter measures. This is a more

Defense strategy	Implementation
Physical security	CCTV, restricted access to facilities, secure surroundings, hardware casing
Encryption	Public or private keys, one time passwords
Authentication	Digital signatures, Certificate Authorities
Hardware upgrades	Directional sensors to detect jamming, better casing for EM shielding,
Software	Firewalls, Malware protection, anti-virus, compartmentalization of sub-systems
Improved Algorithms	Evading a region of EM jamming, frequency hopping
Redundancy	Multiple sensors, multiple communication channels, sacrifice efficiency for read backs or acks

Table 5.3: General defense strategies

active approach where attacks are allowed to happen and then defended against. On the other hand, Mitigation strategies are more preemptive and passive- these are designed to prevent the attacks from happening in the first place. Further, all the detection and mitigation strategies are effective to varying degrees, and also differ in the practicality and ease in implementation.

The trade offs involved in selecting appropriate defense strategies for each atomic attack are discussed below:

- EM jamming attacks can render a particular frequency useless for communication. This typically means that one can detect the jamming, and then shift to another frequency, or physically move away from the jamming zone. The easiest way to detect EM jamming is by measuring an increase in the power of the received signal. Further, directional antennas can identify the source of the jamming signals and are highly effective in detecting the onset of jamming. Some other methods like detecting a change int he statistical properties of the received signal can augment detection process, but are less effective. These detection strategies require the use of directional antennas and recievers, which may be impractical to place on a vehicle due to power and weight constraints. However, they are well suited for ground infrastructure, such as USS, ATC, and Remote Pilot locations. Mitigation involves shifting between a set of frequencies in order to make it immune from low power, frequency specific jammers. However, the best defense mechanism for ground stations is physically monitoring the neighborhood for jamming devices, and for aerial vehicles to fly out of a hostile zone.

- Equipment malfunction can be detected using on board fault diagnosis software. These are relatively cheap to implement and are effective in detecting malfunctions. However it is important to note that detection will not be sufficient if the equipment and its function is critical. The most effective way to mitigate these attacks is via redundancy- i.e. having multiple alternate equipment to perform the same task. While this is a standard practice in manned aircraft design, UAVs do not necessarily incorporate such design principles due to weight limitations. Another

Atomic attack	Defense Strategies	Ease	Effectiveness	Ref
EM jamming	D: Power approach (increase, direction)	Medium	High	[14, 70, 59, 45]
	D: Channel characteristics (RF fingerprinting, statistical methods)	Medium	Low	
	M: Frequency hopping	Medium	Medium	
	M: Physical security for ground installations	High	High	
	M: Avoid flying in known hostile territory	Medium	High	
Equipment malfunction	D: Fault diagnostics	High	High	[9, 55, 6, 57]
	M: Physically robust hardware	Medium	High	
	M: Fault tolerant control	Medium	Medium	
	M: Redundancy	Low	High	
Eavesdropping	D: Detection is not possible	-	-	[56, 11]
	M: Encryption	Low	High	
Message deletion	D: Using digitally signed (authenticated) acknowledgments	Medium	High	
	M: Redundancy	Medium	Medium	
Message modification	M: Hashing the message with a secret key before transmission	Medium	High	
Message insertion	D: Sanity checks	High	Low	
	M: Digital signatures to authenticate trusted devices	Medium	High	
Malware/spyware	Out of scope for this work	-	-	[51, 18]
Network protocol	D and M: Algorithms mentioned in the references	Medium	Medium	[32]
Social engineering	D: sanity checks	Low	Low	[36]
	M: User education	Medium	Medium	
	M: Improved procedures	Medium	Medium	
	M: Redundancy	Medium	Medium	

Table 5.4: Defense against atomic attacks

approach would be to have physically robust hardware that is not easy to modify, tamper or physically break. This could involve having protective outer casing, integrated solid state devices that are not easy to tamper for an opportunistic attacker. Finally, on the algorithmic front, fault tolerant control algorithms would enable partial functionality of the vehicle in case of failures to limit damage to the vehicle, environment or payload due to the attack.

- Eavesdropping cannot be detected for wireless communications. For a wired system involving a physical tapping of the wires, it may be possible to detect it through a physical inspection. Mitigation involves encryption of the communication. This is not a very feasible technique, as scaling ti would require the maintenance of a public key infrastructure. However, the effectiveness is very high and this could motivate its usage for extremely sensitive communication links that have valuable payload information.

- Message deletion can be detected reliably if the recipient sends digitally signed acknowledgments to the user. Note that it is important for the *ack* message to be digitally signed by the intended recipient, else the attacker will delete the message and send a false acknowledgment. The only challenge in implementation is maintaining the digital signatures fo all trusted devices in the system using a Certificate Authority (CA). We are unaware of how to mitigate the deletion of messages, especially when they are between two static nodes, and the attacker can conveniently position the interference device at an appropriate location to delete a message. Once detected, the only alternatives are to re-send the message using either the same channel, or a different one.

- Message modification can be hard to detect, but hashing the message, or encrypting it is a reliable method to prevent any modification. However, the challenge would be to invest and maintain a key sharing infrastructure.

- Message insertion is hard to detect using any physical means. An approach would be to use logical consistency checks, or sanity checks to attest to the validity of the transmitted message. For instance, a control command to roll inverted, or to fly into an obstacle detected by on board sensors would seem to suspicious. However, it is very difficult to consistently detect fraudulent messages, and hence the effectiveness is low. Digital signatures, and or the presence of valid certificates issued by a CA would be highly effective.

- Detection and mitigation for malwares, spywares, Trojans, worms and other malicious software is out of scope of this work. We refer the readers to a huge body of work on computer security in the Internet and other networks systems for further information.

- Depending on the wireless ad-hoc network that is employed, and the attack, there are several detection and mitigation strategies. An overview of these are provided in the reference. They very in their effectiveness and ease of implementation.

- Socially engineered attacks are difficult to detect, and rely on sanity checks to identify malicious or suspicious behavior. These algorithms are not too effective

either. Mitigation can involve several approaches, which should be employed simultaneously. However, human error, bias, and psychological manipulation remains a vulnerability.

Chapter 6

Case Study: Drones for Package Delivery

6.1 Outline

We present two case studies to demonstrate the applicability of our threat analysis framework. We consider the UAV for transportation (drone delivery) application under two different levels of automation - Level 1 (human assistance) and Level 3 (conditional automation). The UTM blueprint document [1] is our primary reference to set up the two scenarios.

The approach we present is applicable to the analysis of any specific operating framework. The steps involved are:

1. Description of the UAS architecture, operating principles, vehicle capabilities, mission profile, and communication requirements.
2. Outlining the communication architecture, and the nodes and links involved in the system.
3. Analysis to check if the technology used to realize a link satisfies the requirements.
4. Evaluation of likelihood, impact and risk of different atomic attacks on the communication links, along with a summary of the assumptions.

6.2 Case study: System Description

Unmanned aerial vehicles can be used to transport several kinds of goods, like retail packages or emergency supplies. It is estimated that 4 billion packages were ordered for delivery online in Europe in 2017 [3]. The potential scale fo the system is enormous, with even a drone delivery of 1% of these packages leading to 14,000 drone flight for every daylight hour on an average [1]. The two cases compare the present day technology (Level 1 automation) with a future goal (Level 3 automation). These levels of automation, and technological requirements to achieve each level is discussed in [1] (and reproduced in Figure 6.1).

6.2.1 Overview of the system architectures

First we describe the two levels of automation that we consider.

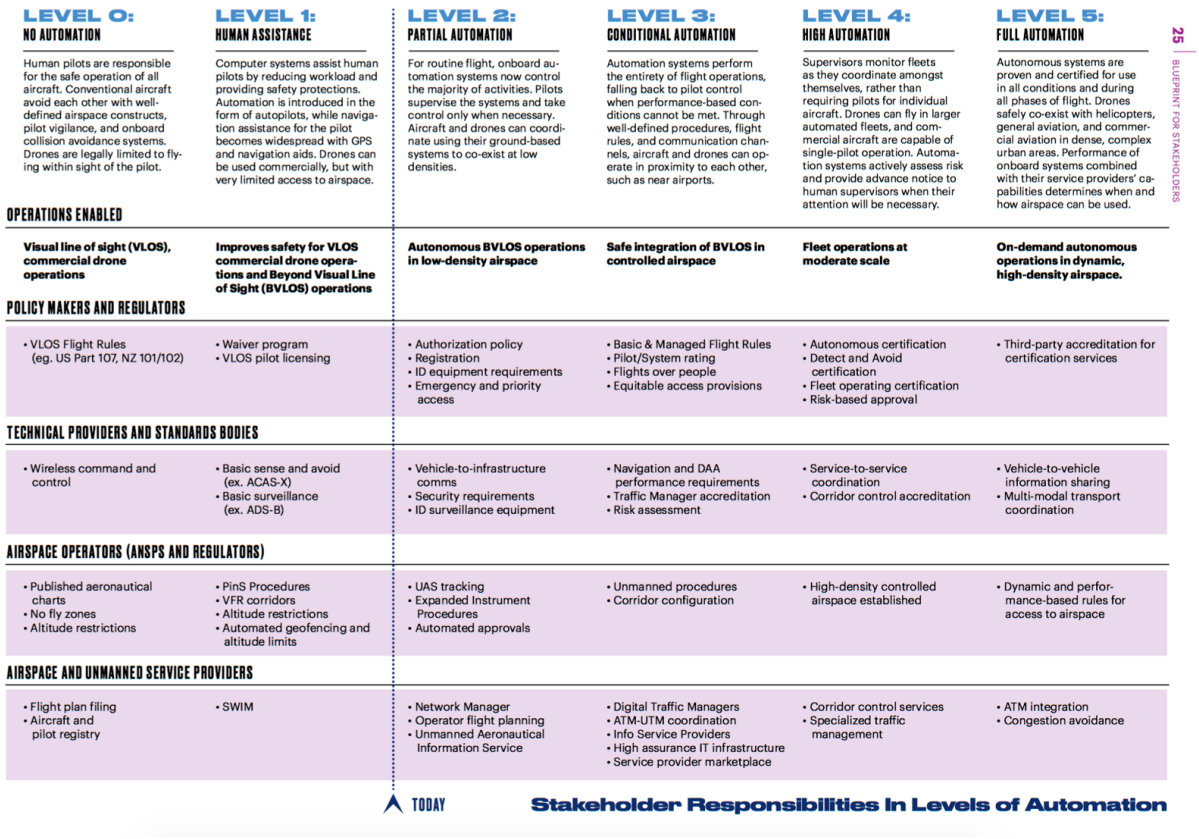

Figure 6.1: Description of different levels of UAS automation [1]

Human assistance (Level 1)

The human pilot remains solely responsible for the safe and efficient operations of the vehicle, and automation is provides to reduce some pilot workload. For instance, the vehicle can send images and videos of its surroundings to the pilot, communicate its GPS location, attitude and speed to the pilot. The pilot can use this information to make a control decision and transmit that back to the vehicle. There is no autonomous decision that is made without the human in the loop. This level of automation can improve the safety in Visual Line of Sight operations, while also enabling beyond LoS operations.

Conditional Automation (Level 3)

A Level 3 automated system performs routine tasks autonomously, and reverts the control back to the human only when performance or safety conditions are not met. The automation has the right to relinquish control at any instant, and present it to the human pilot. For instance, vehicles can be expected to perform waypoint based navigation, perform conflict resolution at a tactical level, and autonomously land. The role of the human is supervisory in nature, but could become significant if the automation relinquished control during un-expected events.

The level of maturity of the autonomous system determines the capabilities of the vehicle (Table 6.1), and combining it with the mission requirements determines the operational procedures that will be used (Table 6.2)

Property	**Level 1 : Human assistance**	**Level 3: Conditional Automation**
Conflict Resolution	Very basic functions like ADS-B and ACAS-X	Sensors to detect cooperative and un-cooperative targets and resolve multi-vehicle conflicts
Duration of autonomous operation	Less than 5 minutes	Indefinite, unless the required navigational performance cannot be met
Lost communication protocol	If not restored within a few minutes, navigate to and land at the nearest pre-determined landing spot	Continue mission as long as safety and performance thresholds are met
Navigation performance	Limited by pilot skill and sensor accuracy	Can follow specific 4d trajectories with a specified performance threshold

Table 6.1: Assumptions on vehicle capabilities

Property	**Level 1 : Human assistance**	**Level 3: Conditional Automation**
Visibility requirements	VFR conditions to enable 'sense-and-avoid' as there is limited onboard vehicle capabilities	No requirements as vehicles can communicate their location and intent to coordinate conflict resolution autonomously
Accessible Airspace	Separate airspace for UAS operations. Not integrated with other ops	Integrated operations of manned and un-manned vehicles in the same airspace (ops near existing airports are possible)

Table 6.2: Assumptions on system operations

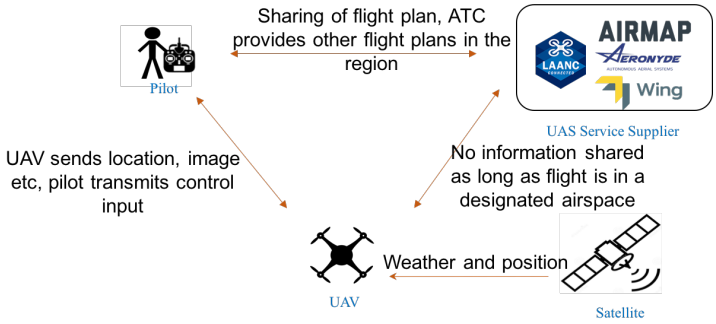

Figure 6.2: Level 1 Communication architecture

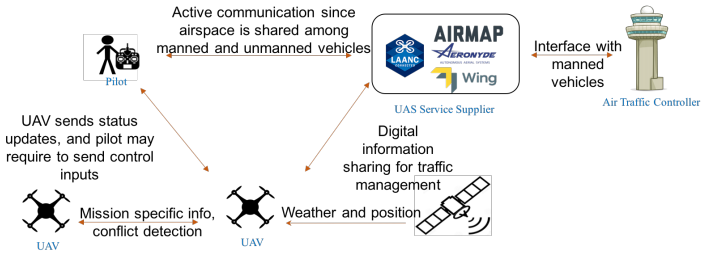

Figure 6.3: Level 3 Communication architecture

6.2.2 Communication Architecture for the Two Systems

The first system is the Level 1 automation, where the human pilot is provided with minimal assistance to simplify repetitive tasks. The pilot, USS, and the vehicle are considered as nodes in the communication network. The communication links, and their functions are described in Figure 6.2. In this report, we use pilot or operator interchangeably, as they refer to the same person.

In comparison to the Level 1 automation case, with Level 3 automation, the vehicle is capable of co-sharing the airspace with other manned traffic, requiring an active communication between the vehicle and the USS, and also between the USS and the ATC facility. In addition, the vehicle is also capable of interfacing with other vehicles for information exchange, or collision avoidance. These links are highlighted in Figure 6.3.

The comparison between the function of the links in the two cases is shown in Table 6.3.

On the whole, a Level 1 system is limited by vehicle capabilities to maintain required navigational standards, that does not enable it to be integrated into the manned airspace. Further, the pilot-vehicle link is the most critical, as it enables the vehicle to share its current state, and the pilot can decide on the control action based on all available information. The role of the USS is also limited, and separation is the responsibility of the pilot. It is important to note that the GPS link is very important for this architecture, as there is limited autonomy on the vehicle, and the location of the vehicle is one of the most important variables that a pilot would require to know to make control decisions. Further, there is no communication between the USS and the conventional ATC system that is designed for the manned vehicles, as they do not share the same airspace.

A Level 3 system is takes almost all the routine workload away from a controller,

Link	Human assistance (Level 1)	Conditional automation (Level 3)
Pilot - UAV	Only means of command and control, so is critical	Not critical for normal operations, but critical during off-nominal events
Pilot - USS	Limited information like flight plan (not real time)	Must be continuously maintained since ATM-UTM coordination is required
ATC - UAV	Not present	Information sharing for traffic management, and possible control actions
UAV - Sat (GPS) - UAV	Location, weather	Location, weather
UAV - UAV	Not present	Conflict resolution

Table 6.3: Role of each communication link for the two different levels of automation.

making the vehicle more self sufficient. While this reduces the reliance on the pilot-vehicle link, it creates an additional requirement in the form of a USS-vehicle link. Since the vehicle has greater capabilities, it is more integrated into the airspace, and will require some form of tactical control for traffic management at times. It is important to note that if a vehicle with Level 3 autonomy was operating in similar flight environments as a Level 1 vehicle, then there would be no requirement on the USS-vehicle link, while reducing the reliance on the pilot-vehicle link simultaneously. Another link, that is not present in Level 1 systems is the vehicle-vehicle link, or in general a link between the vehicle and other infrastructures. In our case study, we will restrict this to a UAV-UAV link, whose purpose is conflict resolution (similar to TCAS used in commercial airplanes). Finally, the USS coordinates with the ATC to share the airspace with manned aircrafts in a safe and efficient manner.

6.2.3 Requirements and Other Assumptions on the System

In this section, we present the assumptions on the attacking agents, the nodes and for the links. Then, we present the requirements on each of the communication links in the two scenarios.

The assumptions on the attacking agent are common for both the scenarios. They are

1. Attacker is external to the system
2. Attacker is limited to commercially available tools
3. There is only one attacker
4. Natural disasters, or poor designs are not considered attacks
5. Opportunistic attacks are carried out only if low levels of effort are needed to implement them

Requirements	Pilot-UAV	Pilot-USS	UAV-Satellite
Availability	High	Low	High
Continuity	High	Low	High
Integrity	High	High	High
Confidentiality	Medium	Low	Low
Authenticity	High	High	High

Table 6.4: Requirements on the communication links for Level 1 automation

Requirements	Pilot-UAV	Pilot-USS	UAV-USS	ATC-USS	UAV-Satellite
Availability	Medium	Medium	Medium	High	Medium
Continuity	Medium	Medium	Medium	High	Medium
Integrity	High	High	High	High	High
Confidentiality	Medium	Low	Medium	Medium	Low
Authenticity	High	High	High	High	High

Table 6.5: Requirements on the communication links for Level 3 automation

A few other assumptions that are made on the nodes are

- USS facilities, ATC facilities and other ground stations: These are physically well secured, and use high power high power antennae for radio communications. Thus EM jamming is not possible.
- Remote pilot facility: Since they are a part of a commercial delivery operation, they are located at secure, well established facilities, making EM jamming hard. Further, we assume that one pilot only controls one vehicle, as the automation in both cases are not sufficient to allow a single pilot to manage a fleet of vehicles.
- GPS: The vehicles are expected to operate in uran regions, and in the vicinity of tall buildings. Thus the satellites may not be in the line-of-sight for several minutes. This is to be expected when navigating in urban environments. Further, multi-path issues may reduce the accuracy of the location measurements too.

The requirements on the communication links, in terms of the availability, continuity, integrity, authenticity, and confidentiality (refer to report 1) vary in both cases. We present the requirements in Table 6.4 and 6.5.

Specific assumptions on the links in Level 1 automation are

1. Pilot-USS link: Information is not time sensitive, does not result in a control action, is not necessarily confidential or private, and there are several redundant ways to communicate the information
2. Pilot-vehicle link: The transmitted information is time sensitive, results in a control action, should be encrypted and authenticated, and there are no alternate way to communicate the desired information

Specific assumptions on the links in Level 3 automation are

1. Pilot-USS link: The information transmitted is moderately time sensitivity, can result in a control action, should be encrypted, and multiple alternatives exist to convey the message.

2. Pilot-vehicle and USS-vehicle link: This information is also moderate time sensitivity, can result in a control action, and should be encrypted and authenticated. While there are no alternate direct paths between the pilot-vehicle or USS-vehicle, a one-hop alternate is possible, since the pilot, ATC, and the vehicle are all connected.

3. USS-ATC link: This is a safety critical link, and is both time-sensitive and can lead to control actions.

6.2.4 Technology to realize the communication links

While Tables 6.4 and 6.5 present the desirable properties of a link, there may be several technologies that satisfy these requirements to physically realize the link. Let us consider the first case (with L1 automation). The pilot-UAV link is very critical for the safe operation of the system. A Line-of-sight radio link is used to achieve it. Given the urban operations of the vehicle, several such relay stations (or ground stations) would eb required to provide coverage in such terrain. The pilot-USS link is not time sensitive, and is only used to uni-directional transfer of flight plans from the pilot to the USS. The Internet, cellular connections, a wired phone call, or even a satellite phone can be used for this purpose. The GPS link is a direct line-of-sight connection, and atleast four satellites should be visible from the vehicle to acquire its position.

Let us now consider the level 3 automation case. With increasing autonomy, the vehicle capabilities are higher, and there is less reliance on communication for operational safety. The pilot-UAV link remains the primary mode to control the vehicle in case of un-expected events, however, it is used sparingly for time-sensitive control actions due to significant vehicle capabilities. The USS also can communicate with the vehicle directly to issue emergency maneuvers, and the vehicle constantly updates the USS of its intent and position. While these links are not time-critical, it is important to maintain them for the safe integration of UAVs in dense airspaces. The role of the pilot-USS link is also more pronounced than the Level 1 case, as there is an active flow of trajectory information between the two. The USS-ATC communication is not expected to be used continuously, but is critical for coordinating the manned and unmanned vehicular operations. We consider the case where all the three communication channels: UAV-USS, UAV-Pilot, Pilot-USS, are all realized using cellular links. Cellular links typically do not provide any guarantee on continuity and availability, but it is sufficient for this particular application. The communication between UAVs is a direct line-of-sight link, which is used for the purpose of tactical conflict resolution. We assume multiple redundant wired, or wireless medium of communication between the USS provider and the ATC.

6.3 Case Study: Risk Assessment

We evaluate the risk of different atomic attacks on the two cases based on the assumptions in Section 6.2. For each of the nodes and links in the communication system, we a comment on the Motivation, Membership, Method and Scope of different atomic attacks.

6.3.1 Level 1 automation

We analyze three nodes: USS, Pilot and the UAV (Tables 6.6, 6.7 and 6.8 respectively), and four links: Line of Sight, Internet, Satellite Communication (GPS), and cellular

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
Malicious Software	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Active	Extended	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Low	Low
	Strategic	Inside	Active	Extended	Low	Low	Low
Social Engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Low	Low

Table 6.6: Level 1 node: USS

Atomic attack	**Motivation**	**Membership**	**Method**	**Scope**	**Likelihood**	**Impact**	**Risk**
EM jamming	Opportunistic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Local	Low	High	Medium
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Local	Low	High	Medium
Malicious Software	Opportunistic	Inside	Active	Local	Low	Medium	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	High	Medium
	Strategic	Inside	Passive	Local	Low	Medium	Low
Social engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Medium	Low
	Strategic	Inside	Passive	Local	Low	Low	Low

Table 6.7: Level 1 node: UAS operator

networks (Tables 6.9, 6.10, 6.11 and 6.12 respectively).

For the USS node, the attacks can be strategic or opportunistic. Some attacks like EM jamming and equipment malfunction are conducted by agents external to the system (outside members) whereas social engineering and malicious software attacks can only be carried out by authorized agents internal to the system. In general, the likelihood of any of the attacks on the USS is low; these are usually secure facilities and have sophisticated equipment to detect intrusion making it hard to physically attack the system. Further, the power of the EM ways transmitted from these facilities is typically high, making jamming difficult. Interestingly, the impact of these system failures is also low, as there are several internal redundancies, established protocols for these failures, and alternate means of communication.

The UAS operator in this case is affiliated with a package delivery company, which has its well established infrastructure for the base station. This makes all the atomic attacks: EM jamming, equipment malfunction, malicious software, and social engineering difficult to perform. However, the impact of these attacks on the system, if they occur are different. In general, strategic and active attacks have a higher impact than opportunistic and passive attacks.

The analysis of the likelihood and impact at the vehicle node is a very strong function

Atomic attack	**Motivation**	**Membership**	**Method**	**Scope**	**Likelihood**	**Impact**	**Risk**
EM jamming	Opportunistic	Outside	Active	Local	Medium	High	High
	Opportunistic	Outside	Active	Extended	Low	High	Medium
	Strategic	Outside	Active	Local	Medium	High	High
	Strategic	Outside	Active	Extended	Low	High	Medium
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Malicious Software	Opportunistic	Inside	Active	Local	Low	Medium	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Medium	Medium	Medium
	Strategic	Inside	Passive	Local	Medium	Low	Low

Table 6.8: Level 1 node: Vehicle

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Equipment malfunction	Strategic	Outside	Active	Local	Low	High	Medium
	Strategic	Outside	Active	Extended	Low	High	Medium
Eavesdropping	Opportunistic	Outside	Passive	Extended	Low	Low	Low
	Strategic	Outside	Passive	Extended	High	Low	Medium
Message Modification	Strategic	Outside	Active	Local	Low	High	Low
Message Deletion	Strategic	Outside	Active	Local	Low	High	Low
Message Insertion	Opportunistic	Outside	Passive	Extended	Low	High	Medium
	Strategic	Outside	Passive	Extended	High	High	High

Table 6.9: Level 1 link: Line of Sight (digital communications)

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Network protocol	Opportunistic	Outside	Passive	Local	Low	Low	Low
	Opportunistic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Passive	Local	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low

Table 6.10: Level 1 link: Internet

of the level of automation. EM jamming remains a very potent high impact attack, as it has the ability to disconnect the vehicle, with limited self-navigation capabilities from communicating with both the Pilot and the Satellite (for GPS signals). The likelihood of such an EM attack is is quantified as medium if a local region of airspace is targeted, and low if it targets an extended airspace.

The LoS link enables the vehicle to communicate with the Pilot, typically using radio waves. Since these are critical to the control and navigation of the vehicle, any disruption of the link is mission critical and has a high impact. Assuming that the messages are encrypted and authenticated, eavesdropping leads to a minimal impact on safety.

The Internet link can be subject to strategic network protocol attacks from outside agents, While the scope may be local or extended, the likelihood of carrying out such attacks is low as it would a require very sophisticated suite of techniques to modify the protocols. The use of the internet link for non-critical purposes further makes the impact of the dysfunctional (i.e attacked) link minimal.

There is no notion of eavesdropping a GPS signal. Message deletion, modification and insertion of GPS signals requires significant technological and practical challenges (location of the attacker, synchronization etc), making it feasible only for an opportunistic attacker. While the likelihood of such an attack is low, the impact is high, as it is the sole mode of navigation for a vehicle with limited autonomy.

In the Level 1 case study, the cellular link is used only for communicating between the pilot and the USS. Encryption, proprietary technology, and a distributed architecture make attacks on cellular links technologically challenging and unlikely. In addition, the impact on the system is also minimal as the link is not critical for safety at a tactical level.

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	-	-	-	-	-	-	-
Message deletion	Strategic	Outside	Active	Local	Low	High	Medium
Message modification	Strategic	Outside	Active	Local	Low	High	Medium
Message insertion	Strategic	Outside	Active	Local	Low	High	Medium

Table 6.11: Level 1 link: Satellite communication (GPS)

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Network protocol	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Passive	Local	Low	Low	Low
	Strategic	Outside	Passive	Extended	Low	Low	Low

Table 6.12: Level 1 link: Cellular networks

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Low	Medium	Low
	Opportunistic	Outside	Active	Extended	Low	Medium	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Extended	Low	High	Medium
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Extended	Low	High	Medium
Malicious Software	Opportunistic	Inside	Active	Local	Low	Medium	Low
	Opportunistic	Inside	Active	Extended	Low	Medium	Low
	Strategic	Inside	Active	Local	Low	Medium	Low
	Strategic	Inside	Active	Extended	Low	High	Low
Social Engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Low	Low

Table 6.13: Level 3 node: USS

6.3.2 Level 3 automation

In Level 3 automation, the nodes are : USS, Vehicle (UAV), Pilot (or operator), and the ATC. The cellular links are used between the Pilot, vehicle and the USS. The USS and ATC communicate using wired links, UAVs coordinate with other vehicles through LoS links, and a satellite link is used to obtain GPS position.

The USS is generally well secure, and the likelihood of an attack is low. However, since the USS coordinates shared access with the manned vehicle airspace, and has the ability to issue control actions to the vehicle, the impact of an attack can be significant. While there is some degree fo redundancy and resillience, strategic attacks with an extended scope can result in maximum impact. Interestingly, the risk metrics for the USS node in the case of a Level 3 automation is higher than a Level 1 automation. This might seem counterintuitive as increase in automation is leading to higher risks. However, it is important to realize that with increase in the automation, the nature of the mission, and the operating procedures also change. Now, the role of the USS is not passive, but rather active integration and coordination of the manned and unmanned vehicles with the ATC, pilots and the vehicle itself. Thus, attacks on the USS may translate into malicious control action to the vehicles.

While the pilot node has similar characteristics to the Level 1 scenario, the impact of an attack is only categorized as medium. This is because of significant improvements in the vehicle capability in case of lost communications. Further, a loss of communication with the ATC need not always be catastrophic as well.

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Local	Low	Medium	Low
Malicious Software	Opportunistic	Inside	Active	Local	Low	Medium	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Medium	Low
	Strategic	Inside	Passive	Local	Low	Medium	Low
Social engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Medium	Low
	Strategic	Inside	Passive	Local	Low	Low	Low

Table 6.14: Level 3 node: UAS operator/ Pilot

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Medium	Medium	Medium
	Opportunistic	Outside	Active	Extended	Low	Medium	Low
	Strategic	Outside	Active	Local	Medium	Medium	Medium
	Strategic	Outside	Active	Extended	Low	Medium	Low
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Medium	Low
	Strategic	Outside	Active	Local	Low	High	Medium
Malicious Software	Opportunistic	Inside	Active	Local	Low	Medium	Low
	Opportunistic	Inside	Passive	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	High	Medium
	Strategic	Inside	Passive	Local	Low	Low	Low

Table 6.15: Level 3 node: Vehicle

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
EM jamming	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
Equipment malfunction	Opportunistic	Outside	Active	Local	Low	Low	Low
	Opportunistic	Outside	Active	Extended	Low	Low	Low
	Strategic	Outside	Active	Local	Low	Low	Low
	Strategic	Outside	Active	Extended	Low	Low	Low
Malicious Software	Opportunistic	Inside	Active	Local	Low	Low	Low
	Opportunistic	Inside	Active	Extended	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Low	Low
	Strategic	Inside	Active	Extended	Low	Low	Low
Social Engineering	Opportunistic	Inside	Active	Local	Low	Low	Low
	Strategic	Inside	Active	Local	Low	Low	Low

Table 6.16: Level 3 node: ATC

Increase in the autonomy level has a direct impact on the risk metrics for the vehicle node. Equipment malfunction or Malicious software can have greater impact than the Level 1 case because of the vehicle's interactions with manned vehicles in the same airspace. However, the effect of EM jamming is not as significant, due to lower need for communication, and several other stand-alone systems for navigation and conflict resolution.

The role of the ATC is primarily to provide separation for manned vehicles. Although it has the ultimate authority for the safety of the vehicles using its airspace, it plays a supervisory role over the USS, and only interfaces if required. The nature of the communication may be strategic (for e.g. changes in runway configuration at urban airports may require the restructuring of the airspace for the unmanned vehicles) or tactical (for e.g. a manned aircraft deviating from its trajectory due to an emergency). In terms of likelihood, all the attacks are low probability events. The impact is also low, since these are physically secure facilities with several redundant systems, increased on-board conflict resolution capabilities, and pre-established protocols that the USS may follow in case of lost communications with the ATC.

The role of satellites is the same in case of Level 1 and Level 3 automation. While there are significantly more navigational capabilities in the Level 3 vehicle, they rely on ground based beacons (e.g. VORs) for localization, and are not as accurate as GPS. Hence, the loss of a GPS signal, while not catastrophic, would prevent the vehicle from meeting the required navigational performance and revert the control back to the pilot. This could be a cause fo concern, as a new trajectory under lower performance requirements might

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	-	-	-	-	-	-	-
Message deletion	Strategic	Outside	Active	Local	Low	High	Medium
Message modification	Strategic	Outside	Active	Local	Low	High	Medium
Message insertion	Strategic	Outside	Active	Local	Low	High	Medium

Table 6.17: Level 3 link: Satellite communication (GPS)

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	Strategic	Outside	Local	Low	Low	Low	Low
Network protocol	Strategic	Outside	Active	Local	Low	High	Medium
	Strategic	Outside	Active	Extended	Low	High	Medium
	Strategic	Outside	Passive	Local	Low	Low	Low
	Strategic	Outside	Passive	Extended	Low	Low	Low

Table 6.18: Level 3 link: Cellular networks

Atomic attack	Motivation	Membership	Method	Scope	Likelihood	Impact	Risk
Eavesdropping	Strategic	Outside	Passive	Local	Low	Low	Low
Message deletion	Strategic	Outside	Active	Local	Low	Low	Low
Message modification	Strategic	Outside	Active	Local	Low	Low	Low
Message insertion	Strategic	Outside	Active	Local	Low	Low	Low

Table 6.19: Level 3 link: Wired links

render the vehicle incapable of performing the required mission.

Cellular networks, especially 5G provide a novel infrastructure to provide connectivity for operations in low-altitude urban airspace. While there are limitations of such a medium for communication, notably the high latency, no performance guarantees, and potential congestion due to non-aviation communications, they suffice for the requirements of the Vehicle-USS-Pilot links in a Level 3 automation setting. Significant technological barriers exist for performing an attack on a cellular network, and they are only performed by a strategic attacker. The likelihood of the attacks are low, but the impact may be high when the attack is active, as it affects all three links: Pilot-USS, USS-Vehicle, and Pilot-Vehicle simultaneously.

Wired networks enable one of the safest (and most expensive) forms of communication. We assume that there are several possible links between the ATC and the USS facility, one of which would be a possible physically wired network architecture. In such cases, any of the attacks: eavesdropping, message deletion, message modification, and message insertion would be nearly impossible to perform. Further, because of several other ways to communicate between the ATC and USS, both of which have significantly advanced infrastructure, the impact will be minimal in case of such attacks.

6.4 Conclusions

We apply our risk assessment framework to analyze two possible architectures for communications. There are a few remarks we make regarding specializing the general framework for specific architectures

- The level of automation directly determines operational flight rules. For example, a low level of automation would not allow the unmanned vehicles to share the same airspace with the manned vehicles.

- The requirements on the communication links and the architecture are dependent on both the mission profile, and the technological capabilities. For example, package delivery would typically occur in densely populated areas, where tall buildings can affect the availability of the GPS signal. However, if there are limitations in technology like visual navigation, the GPS link becomes very crucial to ensure safety. The reliance on GPS decreases as on-board technology and alternate navigation capabilities improve.

- The likelihood of an attack is solely determined by the technological and practical challenges in carrying out the attack. Improvements in the vehicle or infrastructure technology would make it more challenging for an attacker (especially opportunistic ones) to disrupt the system. Sometimes, operational policies may also change the likelihood of an attack. For instance, if a UAVs fly at altitudes greater than a few thousand feet, then EM jamming from a ground station becomes extremely unlikely.

- The impact of an attack is qualitative. For this analysis, we consider a crash, or the inability to complete the mission as a high impact.

Our analysis reveals the different risks that accompany the two architectures. The key conclusions are:

- Although the ATC node is an addition to the Level 3 architecture, it does not add any additional risk to the system. This is expected, since the ATC is typically a robust infrastructure facility.

- The reliance, and consequently the risk associated with the GPS link is lower in a Level 3 system versus a Level 1 system. This is a direct consequence of increased vehicle capabilities for autonomous navigation in a GPS denied environment.

- The risks associated with the Pilot-Vehicle link is lower with the Level 3 automation in relation to the Level 1 scenario. In case of link failures, the effects are not necessarily catastrophic with increased automation.

- The important role of the USS in the Level 3 architecture results in a greater risk profile at that node. This is due to their active role in ensuring coordination with the ATC, Pilot, and the vehicle in ensuring safe utilization of the airspace.

A possible approach to risk mitigation would be to investigate at all the high and medium risk scenarios, and develop strategies to reduce the likelihood or the impact of that attack. Some possible strategies could include:

- Adding redundancy, i.e. multiple means of communicating the same information between two nodes. For example, in the Level 1 architecture, the low requirements on the Pilot-USS link make it easy to provide multiple means like cellular, wired phone calls, internet or LoS to maintain the link.

- Increasing the technological capabilities of the system. Assuming the operational rules are kept the same, increasing autonomy will potentially reduce the risks. For instance, if everything was the same as the Level 1 case, and the vehicle was just upgraded to have more autonomy, then the risks on the Pilot-Vehicle and the GPS link will decrease.

Bibliography

[1] Blueprint for the sky. `https://www.utmblueprint.com`. Accessed: 2019-03-04.

[2] Mq-9 reaper. `http://www.ga-asi.com/predator-b`. Accessed: 2019-05-25.

[3] PostEurop. `https://deliver4europe.eu/facts-figures/`. Accessed: 2019-03-04.

[4] David Alejo, Jose A Cobano, Guillermo Heredia, and Aníbal Ollero. Collision-free 4d trajectory planning in unmanned aerial vehicles for assembly and structure construction. *Journal of Intelligent & Robotic Systems*, 73(1-4):783–795, 2014.

[5] Rafhael Amorim, Huan Nguyen, Preben Mogensen, István Z Kovács, Jeroen Wigard, and Troels B Sørensen. Radio channel modeling for uav communication over cellular networks. *IEEE Wireless Communications Letters*, 6(4):514–517, 2017.

[6] Remus C Avram, Xiaodong Zhang, Jacob Campbell, and Jonathan Muse. Imu sensor fault diagnosis and estimation for quadrotor uavs. *IFAC-PapersOnLine*, 48(21):380–385, 2015.

[7] Mohammad Mahdi Azari, Fernando Rosas, Kwang-Cheng Chen, and Sofie Pollin. Ultra reliable uav communication using altitude and cooperation diversity. *IEEE Transactions on Communications*, 66(1):330–344, 2018.

[8] Ezedin Barka, Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Abderrahmane Lakas, Carlos T Calafate, and Juan-Carlos Cano. Union: a trust model distinguishing intentional and unintentional misbehavior in inter-uav communication. 2018.

[9] Francois Bateman, Hassan Noura, and Mustapha Ouladsine. Fault diagnosis and fault-tolerant control strategy for the aerosonde uav. *IEEE Transactions on Aerospace and Electronic Systems*, 47(3):2119–2137, 2011.

[10] Sourabh Bhattacharya and Tamer Başar. Game-theoretic analysis of an aerial jamming attack on a uav communication network. In *American Control Conference (ACC), 2010*, pages 818–823. IEEE, 2010.

[11] Lowell Campbell and Daniel Robertson. Encrypting communications between wireless mobile units, September 14 2004. US Patent 6,792,112.

[12] Yu Ming Chen, Liang Dong, and Jun-Seok Oh. Real-time video relay for uav traffic surveillance systems through available communication networks. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pages 2608–2612. IEEE, 2007.

[13] Hongmei Deng, Wei Li, and Dharma P Agrawal. Routing security in wireless ad hoc networks. *IEEE Communications magazine*, 40(10):70–75, 2002.

[14] David J Dillman. Method and apparatus for using anti-jam technology to determine the location of an electromagnetic radiation source, January 4 2005. US Patent 6,839,017.

[15] George Elmasry, Diane McClatchy, Rick Heinrich, and Boe Svatek. Integrating uas into the managed airspace through the extension of rockwell collins' arinc cloud services. In *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2017*, pages 3B1–1. IEEE, 2017.

[16] Ivan Evtimov, Kevin Eykholt, Earlence Fernandes, Tadayoshi Kohno, Bo Li, Atul Prakash, Amir Rahmati, and Dawn Song. Robust physical-world attacks on deep learning models. *arXiv preprint arXiv:1707.08945*, 1, 2017.

[17] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke. Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, 2017.

[18] Simson Garfinkel, Gene Spafford, and Alan Schwartz. *Practical UNIX and Internet security*. " O'Reilly Media, Inc.", 2003.

[19] Rania Ghatas, Devin P Jack, Dimitrios Tsakpinis, James L Sturdy, Michael J Vincent, Keith D Hoffler, Robert Myer, and Anna Dehaven. Unmanned aircraft systems detect and avoid system: End-to-end verification and validation simulation study of minimum operational performance standards for integrating unmanned aircraft into the national airspace system. In *17th AIAA Aviation Technology, Integration, and Operations Conference*, page 3278, 2017.

[20] Vasileios Gkioulos, Stephen D Wolthusen, and Athanasios Iossifides. A survey on the security vulnerabilities of cellular communication systems (gsm-umts-lte).

[21] Lav Gupta, Raj Jain, and Gabor Vaszkun. Survey of important issues in uav communication networks. *IEEE Communications Surveys & Tutorials*, 18(2):1123–1152, 2016.

[22] Kim Hartmann and Christoph Steup. The vulnerability of uavs to cyber attacks-an approach to the risk assessment. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, pages 1–23. IEEE, 2013.

[23] Daojing He, Sammy Chan, and Mohsen Guizani. Communication security of unmanned aerial vehicles. *IEEE Wireless Communications*, 24(4):134–139, 2017.

[24] Daojing He, Sammy Chan, Yinrong Qiao, and Nadra Guizani. Imminent communication security for smart communities. *IEEE Communications Magazine*, 56(1):99–103, 2018.

[25] Horst Hering, G Kubin, et al. Safety and security increase for air traffic management through unnoticeable watermark aircraft identification tag transmitted with the vhf voice communication. In *Digital Avionics Systems Conference, 2003. DASC'03. The 22nd*, volume 1, pages 4–E. IEEE, 2003.

[26] Vinay M Igure, Sean A Laughter, and Ronald D Williams. Security issues in scada networks. *computers & security*, 25(7):498–506, 2006.

[27] Raj Jain and Fred Templin. Requirements, challenges and analysis of alternatives for wireless datalinks for unmanned aircraft systems. *IEEE Journal on Selected Areas in Communications*, 30(5):852–860, 2012.

[28] Raj Jain, Fred Templin, and Kwong-Sang Yin. Wireless datalink for unmanned aircraft systems: Requirements, challenges, and design ideas. In *Infotech@ Aerospace 2011*, page 1426. 2011.

[29] Ahmad Y Javaid, Weiqing Sun, Vijay K Devabhaktuni, and Mansoor Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 585–590. IEEE, 2012.

[30] Imad Jawhar, Nader Mohamed, and Hafsa Usmani. An overview of inter-vehicular communication systems, protocols and middleware. *JNW*, 8(12):2749–2761, 2013.

[31] Yazdi I Jenie, Erik-Jan van Kampen, Joost Ellerbroek, and Jacco M Hoekstra. Taxonomy of conflict detection and resolution approaches for unmanned aerial vehicle in an integrated airspace. *IEEE Transactions on Intelligent Transportation Systems*, 18(3):558–567, 2017.

[32] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.*, pages 113–127. IEEE, 2003.

[33] Andrew J Kerns, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014.

[34] Mahfuza Khatun, Hani Mehrpouyan, David Matolak, and Ismail Guvenc. Millimeter wave systems for airports and short-range aviation communications: A survey of the current channel models at mmwave frequencies. 2017.

[35] Yoohwan Kim, Juyeon Jo, and Monetta Shaw. A lightweight communication architecture for small uas traffic management (sutm). In *Integrated Communication, Navigation, and Surveillance Conference (ICNS), 2015*, pages T4–1. IEEE, 2015.

[36] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. Advanced social engineering attacks. *Journal of Information Security and applications*, 22:113–122, 2015.

[37] Xingqin Lin, Vijaya Yajnanarayana, Siva D Muruganathan, Shiwei Gao, Henrik Asplund, Helka-Liina Maattanen, Mattias Bergstrom, Sebastian Euler, and Y-P Eric Wang. The sky is not the limit: Lte for unmanned aerial vehicles. *IEEE Communications Magazine*, 56(4):204–210, 2018.

[38] Angela Lonzetta, Peter Cope, Joseph Campbell, Bassam Mohd, and Thaier Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3):28, 2018.

[39] Wired Magazine.

[40] Mohamed Slim-Ben Mahmoud, Nicolas Larrieu, and Alain Pirovano. An aeronautical data link security overview. In *Digital Avionics Systems Conference, 2009. DASC'09. IEEE/AIAA 28th*, pages 4–A. IEEE, 2009.

[41] T Mamatha. Network security for manets. In *International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-2*. Citeseer, 2012.

[42] David W Matolak and Ruoyu Sun. Unmanned aircraft systems: Air-ground channel characterization for future applications. *IEEE Vehicular Technology Magazine*, 10(2):79–85, 2015.

[43] Mustapha Mouloua, Richard Gilson, Eleni Daskarolis-Kring, Jason Kring, and Peter Hancock. Ergonomics of uav/ucav mission success: Considerations for data link, control, and display issues. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 45, pages 144–148. SAGE Publications Sage CA: Los Angeles, CA, 2001.

[44] Mohammad Mozaffari, Ali Taleb Zadeh Kasgari, Walid Saad, Mehdi Bennis, and Merouane Debbah. Beyond 5g with uavs: Foundations of a 3d wireless cellular network. *arXiv preprint arXiv:1805.06532*, 2018.

[45] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou. A survey on jamming attacks and countermeasures in wsns. *IEEE Communications Surveys & Tutorials*, 11(4):42–56, 2009.

[46] Eric Mueller and Matt Jardin. 4d operational concepts for uav/atc integration. In *2nd AIAA" Unmanned Unlimited" Conf. and Workshop & Exhibit*, page 6649, 2003.

[47] Manh-Dung Nguyen, Naipeng Dong, and Abhik Roychoudhury. Security analysis of unmanned aircraft systems. Technical report, 2017.

[48] Washington Y Ochieng, Knut Sauer, David Walsh, Gary Brodin, Steve Griffin, and Mark Denney. Gps integrity and potential impact on aviation safety. *The journal of navigation*, 56(1):51–65, 2003.

[49] Yongsuk Park and Taejoon Park. A survey of security threats on 4g networks. In *Globecom Workshops, 2007 IEEE*, pages 1–6. IEEE, 2007.

[50] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. 2004.

[51] Charles P Pfleeger and Shari Lawrence Pfleeger. *Security in computing*. Prentice Hall Professional Technical Reference, 2002.

[52] Mark L Psiaki and Todd E Humphreys. Protecting gps from spoofers is critical to the future of navigation. *IEEE Spectrum*, 10, 2016.

[53] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of computer security*, 15(1):39–68, 2007.

[54] Fabio Ricciato, Angelo Coluccia, and Alessandro D'Alconzo. A review of dos attack models for 3g cellular networks from a system-design perspective. *Computer Communications*, 33(5):551–558, 2010.

[55] Michael J Roemer and Liang Tang. Integrated vehicle health and fault contingency management for uavs. *Handbook of Unmanned Aerial Vehicles*, pages 999–1025, 2015.

[56] Aloke Roy. Secure aircraft communications addressing and reporting system (acars). In *20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219)*, volume 2, pages 7A2–1. IEEE, 2001.

[57] Iman Sadeghzadeh and Youmin Zhang. A review on fault-tolerant control for unmanned aerial vehicles (uavs). In *Infotech@ Aerospace 2011*, page 1472. 2011.

[58] Xuemin Shen. Device-to-device communication in 5g cellular networks. *IEEE Network*, 29(2):2–3, 2015.

[59] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C-H Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: A tutorial. *IEEE wireless Communications*, 18(2):66–74, 2011.

[60] Ashutosh Singandhupe, Hung Manh La, David Feil-Seifer, Pei Huang, Linke Guo, and Ming Li. Securing a uav using individual characteristics from an eeg signal. *arXiv preprint arXiv:1704.04574*, 2017.

[61] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2011.

[62] Tim H Stelkens-Kobsch, Andreas Hasselberg, Thorsten Mühlhausen, Nils Carstengerdes, Michael Finke, and Constantijn Neeteson. Towards a more secure atc voice communications system. In *Digital Avionics Systems Conference (DASC), 2015 IEEE/AIAA 34th*, pages 4C1–1. IEEE, 2015.

[63] Paul E Storck. Benefits of commercial data link security. In *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2013*, pages 1–6. IEEE, 2013.

[64] Martin Strohmeier, Matt Smith, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Crowdsourcing security for wireless air traffic communications. In *Cyber Conflict (CyCon), 2017 9th International Conference on*, pages 1–18. IEEE, 2017.

[65] Ruoyu Sun and David W Matolak. Initial results for airframe shadowing in l-and c-band air-ground channels. In *Integrated Communication, Navigation, and Surveillance Conference (ICNS), 2015*, pages X1–1. IEEE, 2015.

[66] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86. ACM, 2011.

[67] Joy Wang, Patricia Deutsch, Linda McCabe, and Ravi Jain. Integration of unmanned aircraft system (uas) voice communications into the faa national airspace (nas). In *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2017*, pages 1E1–1. IEEE, 2017.

[68] Xiaoming Wang, Kai Li, Salil S Kanhere, Demin Li, Xiaolu Zhang, and Eduardo Tovar. Pele: Power efficient legitimate eavesdropping via jamming in uav communications. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*, pages 402–408. IEEE, 2017.

[69] Computer World.

[70] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang. Jamming sensor networks: attack and defense strategies. *IEEE network*, 20(3):41–47, 2006.

[71] Yong Zeng, Jiangbin Lyu, and Rui Zhang. Cellular-connected uav: Potentials, challenges and promising technologies. *arXiv preprint arXiv:1804.02217*, 2018.

[72] Yong Zeng, Rui Zhang, and Teng Joon Lim. Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Communications Magazine*, 54(5):36–42, 2016.

[73] Shuowen Zhang, Yong Zeng, and Rui Zhang. Cellular-enabled uav communication: Trajectory optimization under connectivity constraint. *arXiv preprint arXiv:1710.11619*, 2017.

Appendix A

Literature Review

- [4]: Particle Swarm Optimization algorithm to resolve conflicts for a swarm of UAVs performing a task. UAVs are indoor, and their locations are estimated using VIACOM cameras. No discussion on communication and data links.

- [5]: Communication channel availability and reliability for LOS application between drone and cellular ground station (LTE networks, 800Mhz). UAVs are typically flown with a max height of 100 to 150 m AGL. Reliable communication link between pilot/controller and drone is important. Cellular networks can be used to provide control and non-payload communication or data communication. Authors quantify a few parameters related to signal reception, and highlight that more reception is possible at higher altitudes.

- [7]: Framework for analyzing air to ground links. Gives optimal height for minimizing the probability of an outage- also analytic expression.Example situation: Multiple UAVs providing terrestrial network for internet connectivity. Need to decide optimal altitudes so that signal loss is minimized. Involves UAV-UAV, UAV-Ground and Ground-Ground communication. An A2G channel benefits from a lower path loss exponent and lighter small-scale fading compared to a G2G link, while having a longer link length which deteriorates the received SNR. For a specific scenario with a communication range of 1000m with a low transmit power, the optimal UAV altitude for a direct communication was shown to be 1300m, and 700-2000m for relaying communications.

- [8]: UAV comm networks are energy constrained; need to keep computational complexity in mind when designing secure protocols. Context-aware trust-based solution to distinguish between intentional and unintentional UAV misbehavior. Applicable to UAV-UAV communication, where each maintains a state awareness and trust level of other UAVs. Gives overview of cryptography-based and trust-based inter-UAV communications, and present new method to maintain trust in a context-aware scenario. This paper contains a good overview of the attacks on UAV-UAV links.

- [10]: Game theoretic approach for how a swarm of UAVs can identify and isolate a rogue UAV that is jamming them. COntains several references to papers that describe how a UAV can move away from a region where there is jamming. Several proposed solutions: special node to drain attackers energy, frequency hopping. Op-

timal solution- move away from the jamming region. But that is slightly complex in aerial setting since the attacker can also move. Hence game theoretic approach.

- [13]: Survey paper on routing in MANETS. UAV-UAV communication. Black hole problem and a proposed solution. Mostly on MANETS and how routing protocols work- route tables, etc. Mainly focused on how to compromise a routing protocol for MANETS.

- [15]: Rockwell Collins' cloud based WebUAS service. Overview of the different components that make up the 'engine elements', which enable the authentication of a UAS operation- fenced areas, weather, recommendation systems etc. Overview of the factors that must be considered before approving a proposed UAV mission/flight plan.

- [16]: Shows experimentally that small, non-perceptible changes in the input can be strategically used by an attacker to manipulate a deep neural network's output. Eg: Small changes in a stop sign can make a vision system not classify it as a 'stop' anymore. Different from other papers on robust Deep Learning, since they do not engineer un-physical bit manipulations, but rather look at physical stickers/graffiti etc that can cause errors in the classifier.

- [19]: Validation of a detect and avoid algorithm for UAS. Measurement results of ADS-B, air to air Radar, and Active Surveillance Transponder warning effectiveness under different test scenarios. Conclusion: ADS-B performed best for DAA applications.

- [21]: Survey of issues in UAV-UAV communication networks. Comparison of several architectures - static, dynamic and hybrid ways to implement a routing protocol. Presents tables that have important comparisons- 1. MANET vs VANET vs UAVNET. 2. UAC comm/architecture requirements for Internet delivery, Sensing, Attack. 3. Applicability of protocols to UAV networks 4. Energy usage of several protocols.

- [22]: Risk assessment of specific UAVs: MQ-9 Reaper, AR Drone, RQ-170 Sentinel. Examples of attacks: Sentenial by Iranian military forces, key-logging virus in air force base in Nevada. The two important operational connections 1) the bidirectional information flow between the communications system and the ground control station 2) The information flow from the environment to the sensors. Focus is not several aspects of communication. A)Environment: Mountainous, low lands, coast etc. B) Comm links: Different frequency bands used for sat-com and LOS with associated risk assessment tables (integrity, confidentiality and availability). C) Sensors: GPS, cameras, radars - their availability and integrity. D) Data storage and fault handling. The example drones are assessed on all these dimensions. Overall, a very good reference on a framework to asses actual drones. Limitations: No consideration of mission profile, or specific flight plan.

- [23]: Presents an overview of the types of attacks on UAV communications (likes eavesdropping, DoS etc) but major focus on two types of attacks and their countermeasures. 1) GPS jamming and spoofing. Countermeasures include monitoring total power of received signal, multi-antenna defense, and cryptography (military

application). 2) IEEE 8022.11 wireless attacks. Used or WLAN, Ad-hoc networks, civilian UAVs like parrot drones. Attacks is de-authentication (arried out by packet capture), followed malicious agent authenticating the link and gain control. Countermeasure is to use encryption. Example: WPA2 encryption, with a key length of atleast 20. Another option is to disable the broadcast of service set identifier (SSID) and make the access point hidden. Last option- restrict system access to only pre-registered MACs

- [24]: Focus on GPS spoofing, ways to carry it out, and countermeasures for smart infrastructures. Overview of broader concepts (Requirements- confidentiality, availability, authenticity, etc and Typical attacks- DoS, man-in-middle, Viruses, SQL injection, Social engineering) also provided. WHen GPS signal simulator is used, if it is out of phase with actual GPS signal, it is considered as noise by reciever. However, when power is increases, it overshadows true signal and spoofing occurs. Can create problems with inbuilt safety mechanism- For example DJI drones have geofencing functions that prevent operations near airports, but this can be misled due to spoofing. Security against spoofing: 1) characteristics of signal- detect power, monitor clock drift as signal comes to receiver, unnatural correlation distortions. 2) Redundancy- use IMUs 3) Cryptography

- [25]: Securing voice communication using an audio watermark. Play a coded set of signals that can be used by receiver for authenticating the user of the channel. This is not perceptible to the humans using the voice channel, wont be any need to use aircraft call sign also (frees up the frequency). No discussion on key sharing, practicality of changing all existing radios.

- [29]: Overview paper on analyzing the cyber physical threat for UAV communications and is a very good reference. Discussion on the types of comm links, why UAV comm is different from vehicular comm networks and MANETS, examples of attacks on drones, attacks on confidentiality, integrity and availability. Finally presents likelihood, impact and risk tables for the attacks. Limitation: Focus only on the software based attacks. No discussion on attacks that are hardware dependent, or un-intentional degradation of communication channels based on environmental factors. An ideal paper to start as a baseline to extend.

- [31]: Taxonomy development for the aircraft conflict detection and avoidance problem. Examples of dimensions for classification: type of surveillance, coordination level, avoidance measure time scale, autonomy level. Consider all possible permutations - discussion on likely and improbably cases. Final discussion on multi-layered approach to ensure separation.

- [34]: Characterizes the communication frequency band of 30-300 Ghz (mm-wave) in the context of potential aviation application. THe current limitations are- high path loss, severe shadowing, phase noise, high power. However, some of them may be useful, especially for the new UAS applications,if certain technological challenges are overcome. The paper characterizes the path loss and other related quantities, shows that they are similar to the 28GhZ band which can be implemented in 5G mobile networks.

- [35]: Simple approach to integrating UAS into airspace- use mobile phones to file and receive clearances for a flight plan. The system ensures that there are no

conflicts with the existing UAS plans before approving. Procedural separation is ensured consequently. Air traffic controller, UAS and the pilot all communicate through the cloud. Some aspects of authentication regarding the MAC address of the drone/pilot, using HTTPS (which is standard anyways now) are discussed.

- [40]: Computer security assessment of aeronautical data links. Data links used for-air traffic management, airline ops, passenger usage of internet. Provided through-Very high freq data link (VDL) WiMAX for traffic in terminal areas or SATCOM. Several security mechanisms mentioned: symmetric or public key encryption, has functions, digital signature, emails ecurity, IP security , web security, network traffic control, traffic monitoring, key agreement scheme, public key certificates, ACARS security, ATN security, tunneling, route discovery. Algorithms and protocols that achieve these are also mentioned. Layers of the internet are also mentioned, although mechanisms for each layer are not clearly specified. .

- [41]: MANET security via encryption. Elliptic key cryptography, distributed intrusion detection system and a certificate authority is used. Not the best reference for MANET security.

- [42]: Very informative article on characterization of the air-ground channel for UAS applications. Previous bodies do not consider the special aspects of UAS- operation in cluttered, low altitude environments, dynamic motions and a high density of operations. Causes the A-G channel to be more dispersive, incur larger terrestrial shadowing attenuation, and rapidly changing A-G characteristics. Presents some results from measurements in hilly and suburban areas on the channel path loss by fling a UAV at altitudes of 500-2000 m.

- [43]: Discussion of human factors issues in UAV/UCAV (C=Combat) usage. Non mathematical or a highly technical paper, and very old too (2001). Key points: 1) Low latency needed to make control inputs from a remote location. 2) High bandwidth for enabling video streaming, which is typically used to perform controls. 3) Since low latency-high bandwidth comm is usually unavailable, need to rely on automation, and develop control algorithms for the same.

- [46]: Paper describing integration of UAS into NAS via conformance to a 4d flight plan. Presents block diagram for control architecture that enforces 4d plan generation and conformance. Another block diagram indicating all the communication links, and quantities that must be shared between atc facilities, pilots drones, and sensors. Presents an example test bed that shows a lot of the comm links that can be present in the system.

- [60]: Pilot authentication for Pilot-UAV comm link using the pilots EEG signal. IEEE 802.15.4 protocol is used in the MAC layer. The encryption algorithm is fixed by the protocol, but the 128-bit key that must be used by the Advanced Encryption Standard (AES) is not specified. This paper proposes to use a 'unique' feature extracted form the pilots EEG as the key. The UAV is pre-programmed on the ground with the key generated from the user. In effect, this is a secure way to pair a UAV to a ground controller. Not clear why this is different from a randomly generated key that is used for encryption during the pairing step before launching the UAV.

- [62]: Securing voice communication. A model that has three sub-systems: Speaker identification, voice pattern anomaly detector (stress detector) and aircraft conformance monitor. This system is to be installed at both the cockpit and the ground based controllers end. Simulations are proposed to study effectiveness, but results are not presented in this paper.

- [63]: Protected ACARS is proposed as a method to ensure security of ATC (ACARS) data link. CPDLC ATC clearances are not authenticated, and pilots trust them implicitly. PACARS uses elliptic key cryptography. Advantages: software only solution, no additional latency. While this is not a big threat to current airline ops, with fully automated digital messaging between UAS-ATC, PACARS-type can be considered.

- [64]: Crowd sourcing is presented as a potential way to independently verify the information from the ADS-B system. Websites like flightradar24 and fligataware use ADS-B receiver data from the roofs of thousands of individual buildings to track the location of aircraft. These multiple receivers can be used to provide estimates of aircraft location when the ADS-B communication link is subject to attacks like message injection. modification or deletion. Different degrees of redundancy or cross-validation can be provided based on how many receivers can get the aircraft signal.

- [65]: Presents experimental results for loss in Air-Ground signal quality due to UAV shadowing. Loss: around 15 dB for L-band and 28 dB for C-band in hilly terrain

- [68]: Identification of a suspicious UAV through intentional monitoring communications from the UAV. Power efficient jamming scheme is developed to monitor the messages from the suspicious UAV by a legitimate patrolling UAV. This is a technique to identify loss of integrity in UAV-UAV communication when the node (UAV) is compromised.

- [67]: Multiple architectures to integrate UAV voice communication into the National Voice System (NVS) which is a part of NextGen. These are ways in which UAS operators can talk to the ATC just like manned aircraft operators. Of course, there is no need that all of them have to talk, but that the option must be present so that it may be used if needed. Problem: UAS operator in a region diff from UAS, different from location of ATC. UAS pic needs to be able to access the secure Federal Telecommunication Infrastructure (which will carry the VoIP based next gen voice communications). Challenge: latency, security, frequency, access requirement, and fault redundancy. Components: Local Radio Node, ATC voice nod, remote radio node. 4 different architectures by which UAS pilot can interface with the secure NVS. Involves G-G links, A-G links. Several cases are covered and pros and cons are discussed. Interesting paper from the point of view of implementation and integration of UAS voice.

- [72]: Challenges in UAV aided wireless communication. Useful for providing connectivity in mountainous regions, unexpected or limited duration communications, alternate in case of natural disasters. UAVs for : coverage, relaying, data collection from sensors. Control and non-payload comm (low latency, low bandwidth required): protected L and C band. Also can have secondary backups (eg. via

satellites). Data comm (high delay, high bandwidth accepted): can use existing LTE networks, or mm waves. UAV-Ground channel: air-frame shadowing during maneuvers, multi-path issues, reflection diffraction and scattering by mountains, 2-ray models for comm (over desert or sea), Rician fading model(random scattering). UAV-UAV channel: Doppler shift due to high velocities, mm wave is higher frequency and can be subject to higher Doppler shifts.