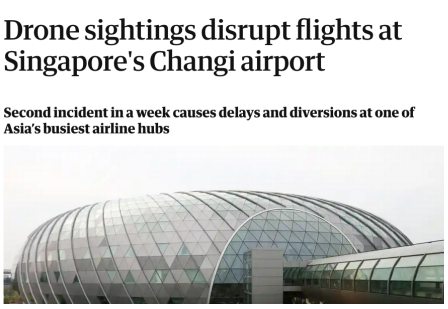
OPTIMISING COUNTER-UNMANNED AERIAL SYSTEMS EFFORTS FOR NATIONAL SECURITY

Saw Ze Dong[1], Liu Rui Yi Winnie[2], Elva Peh[2], David Chong Ruijie[3], Sandra Ng Yi Ling[4] (Mentor)
[1]Dunman High School, 10 Tanjong Rhu Road, Singapore 436895
[2]Nanyang Girls' High School, 2 Linden Drive, Singapore 288683
[3]Victoria School, 2 Siglap Link, Singapore 448880
[4]Defence Science and Technology Agency, 1 Depot Road, Singapore 109679

Abstract
Unmanned Aerial Systems (UAS) refers to an aircraft that is controlled remotely, either by an autonomous or human-controlled system. In this report, we aim to protect a key installation such as Changi Airport from UAS attacks with available technologies such as Radio Frequency Sensors, Radar, Electro-Optical/Infrared Cameras and Radio Frequency Jammers. We model the capabilities of our technologies and propose a solution to be deployed on-site.

Introduction
Historically, UAS have been employed in entertainment, mapping and surveillance, agriculture, and much more.[1] However, due to the portability and autonomous capabilities of UAS, they also have a number of negative use cases.[2] The development of Counter-UAS (C-UAS) technology has been an integral aspect of national defence and security, helping to keep us safe from errant UAS. The negative effects of UAS, such as privacy issues, conflicts in airspaces and UAS attacks can all be mitigated by C-UAS technologies.

Importance of C-UAS
Firstly, C-UAS helps to prevent an invasion of privacy.[2] In areas where critical infrastructure can be found, there may often be large amounts of confidential information on operations and training exercises that can be obtained when an intrusion into these areas occurs. C-UAS detects and stops UAS equipped with microphones and video cameras from infiltrating such areas and transmitting sensitive audio-visual information back to other people, leaking top-secret information that may threaten the security of the country and expose weaknesses in our systems.



Secondly, C-UAS helps to ensure the safety of our airspaces.[2] With the potential to cause structural damage to fast-moving aircraft, resulting in loss of assets and human lives, unregulated UAS are a major threat. C-UAS helps to detect such UAS in controlled airspaces and coordinate immediate protective action to avoid commercial or military aircrafts going close to UAS and ensure the safety of people. For example, in June 2019, UAS sightings near Changi Airport in Singapore caused delays in departures and arrivals of at least 25 scheduled flights.[3] While delays may cause inconveniences for civilians and economic harm to airlines, they may have a much larger impact at military airbases, allowing perpetrators to be able to cause damage to military infrastructure and potentially disrupt crucial functions, delaying the deployment of aerial forces, ultimately disrupting rapid response from the air force to emergencies and threatening national security.

Lastly, C-UAS helps to safeguard people and infrastructure from direct attacks by UAS.[2] UAS warfare is usually carried out in the form of releasing explosives, such as bombs or missiles, or directly crashing into targets. For example, in the Russo-Ukrainian War, a swarm of UAS

were able to fly through conflict waters and strike Russia's Black Sea flagship vessel, the Admiral Markov, causing damage to its hull and radar systems, possibly injuring people onboard.[4] C-UAS is important in sensing such threats and interrupting the UAS' malicious missions as soon as possible, and can help to take over control of the UAS to prevent the release of explosives. This helps to prevent the risk of injuries and fatalities from catastrophic attacks and to prevent major economic damage inflicted on systems and buildings.

Detection Workflow

C-UAS technologies follow a fixed workflow which helps to effectively take down UAS.

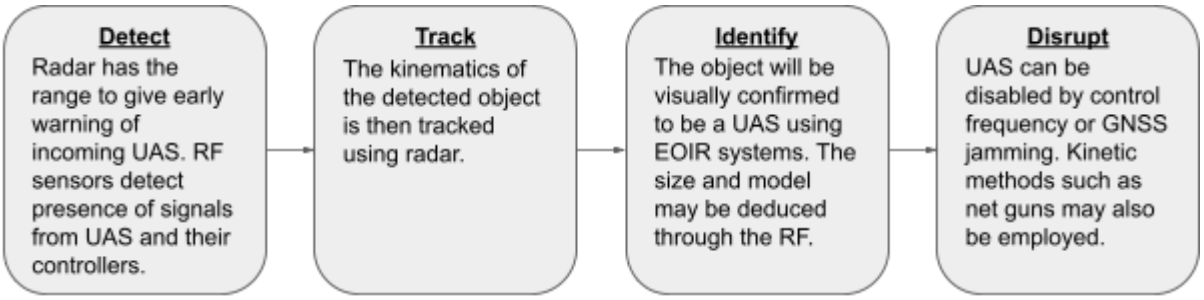


Fig 1.1 Detect-Track-Identify-Disrupt Workflow of C-UAS Measures

These methods being used in conjunction with one another, in this specific sequence, will ensure a high detection rate and low false-positive probability.

Radar

To detect the location and kinematics of the UAS, Doppler radar is used. Objects moving toward and away from the radar will cause a change in frequency of the returning electromagnetic field (EMF) wave, this is modulation. The Doppler effect will cause the EMF of objects moving toward the radar to increase to a higher frequency and vice versa.[7]

Currently, pulse radar is preferred over continuous radar systems due to its lower size profile and cost. However, UAS are often too small to be detected by conventional radar systems' algorithms. Their small radar cross section causes them to be drowned out in background noise. Hence systems have been tuned to detect smaller objects by using higher frequency EMF waves and a lower threshold for background noise.[8] However, UAS continue to be hard to detect and differentiate as they are about the same size as birds. Radar provides limited information to the shape of the target, only the radar cross-section. Hence UAS cannot be easily differentiated from birds with radar alone.

To overcome these issues, Micro-Doppler radar can be utilised. It measures the minute Doppler shifts due to the movement of the propellers on the UAS. The Doppler shift induced by UAS propellers are very distinct due to the high speed, which can be easily distinguished from birds.[9] However, this requires higher frequency EMF waves, thus reducing the radar's effective range. A radar with Micro-Doppler capabilities would hence be most optimal.

Radio Frequency Sensors

After using radar to provide early detection of the UAS, the radar then provides a tracking path to use Radio Frequency (RF) to detect it. UAS and their controllers communicate through RF bands such as: 433MHz, 868MHz, 900MHz, 2.4GHz, 5.8GHz.[10,11]

The UAS communicates with the controller by sending data packets called RF Communication Protocol both ways. A variety of data is also encoded and transmitted over the protocol. The protocol is used to send information about what direction the operator

wishes the UAS to fly. Over the RF band, live video feeds from the camera, the UAS' Global Navigation Satellite System (GNSS) location, altitude and speed data, and typically all other data regarded as flight telemetry are exchanged. This communication can then be detected by antennas on the RF sensor to reveal the presence, location and/or model of the UAS.[5]

There are three types of RF technologies with differing degrees of locational accuracy. The first RF technology uses one sensor to only detect the sector a UAS is in, the second type is capable of detecting and accurately measuring the line of bearing (LOB) of the UAS. Next, multiple RF with bearing can triangulate the position of the UAS, but this method minimally requires 4 sensors in a 3D area.[12] The third type is called Time Difference of Arrival (TDOA) geolocation, where the exact geolocation of the UAS can be determined using 4 anchored sensors calculating the time difference in receiving the UAS' signal.[13]

Unlike radar, RF sensors do not emit any signals thus they reduce power consumption and do not obstruct other communication systems or other delicate devices. RF sensors perform at their best when there is little physical interference. Urban environments with plenty of metal objects and buildings cause RF to diffract, be lost in space etc., causing significant signal loss and hence an RF sensor would not perform at its best.

EOIR (Electro-Optical/Infrared Systems)

After the RF sensor accurately depicts the location of the UAS, EOIR cameras attached to a gimbal will then capture and preserve photos for subsequent forensic analysis or other examination. Images provided by these cameras can be analysed by AI systems, or visually, by a human. Upon receiving the cue, the camera closest to the detected location will locate the moving aerial target, spin around the pivot on the gimbal and start capturing images. EOIR systems span both visible and infrared wavelengths.[14] They use visible light and infrared spectral bands to image the surroundings and detect targets at long range. Hence they can also detect the heat signature or trail of the UAS.[15] This serves as a visual confirmation that would be the last step before the jamming of the UAS. This step is necessary as false-positives could cause needless interference and also cause resources to be wasted.

However, it does face limitations in dark or unfavourable weather conditions. Blurriness or obstruction might make the cameras unable to capture the image, therefore infrared cameras might be a more feasible option in those conditions.[16]

Combination of Methods for Detection

It is insufficient to place the burden of detection entirely upon any one of the detection methods listed above. Often, it is crucial that all 3 of the methods—radar, RF and cameras—must work together to successfully achieve the goal of detecting UAS.

This is because each method has its own capabilities and limitations in terms of its coverage and accuracy. While radar is generally used to provide a large coverage of the area, its ability to sense many different moving objects may also bring about a higher false positive rate.[17] RF provides a smaller coverage area with a higher accuracy rate, along with locating capabilities. Lastly, cameras have the smallest coverage and their footage requires a direct line of sight (LoS) and has a much narrower range but this focused aiming helps to accurately confirm and identify if the object is a UAS. Using either method alone may mean that the area surveyed may be very small causing detection to be ineffective, or prone to raising false alarms, causing a waste of resources or even damage to other infrastructures. By using this workflow, it ensures a process with a large coverage while simultaneously narrowing down the range and increasing the accuracy.[2,5,6]

Hence, a combination of these methods is ideal and helps to allow for a wide area to be protected with high confidence in UAS identification without the requirement for excessive power and equipment as there will be no need to overly deploy such detection systems.

Disruption

By utilising all the methods to detect and locate the presence of UAS, it is then important to disrupt the activity of the UAS to prevent it from entering key installations and accomplishing its malicious mission. Methods such as RF jamming, net guns, UAS vs UAS and UAS takeover and spoofing are often employed in the disruption process to take the UAS down or bring it away from key installations. These common methods each have their pros and cons.

UAS Jamming

UAS jamming works by disrupting communication signals.[18,19] When signals are affected by electromagnetic noise on the same RF band that the UAS operates on, it will no longer be able to remotely receive the instructions as the noise would interfere with the ability to read the data from the controller transmitted over the carrier signals.[19,20,21,22] Thus the pilot loses control of the UAS.

Jammers may come in the form of a handheld gun or a perimeter-based system consisting of noise transmitters placed around a larger area.[23] Handheld systems manned by ground troops can cover blind spots. Jammers are highly advantageous in their high effectiveness when deployed in the perimeter-based form, often being able to drown out all communications over large ranges without needing extensive knowledge of the UAS.

However, UAS that are flown into restricted areas with malicious intent may use frequency hopping (alternating RF bands) as a precaution to make it difficult to pinpoint the frequency of the jamming signal. In such a case, barrage jamming or sweep jamming may be used.[24] Barrage jamming is the practice of transmitting the radio noise over a large range of frequencies to cover a large range of possible RF bands the UAS may communicate on,[25] whereas sweep jamming alternatingly changes the frequency channels that the radio noise is blasted on, choosing narrower channel bandwidths that the UAS is likely to operate on.[24] These methods help to ensure that disruption is still possible with frequency hopping.

However, jamming is a method that may cause disruption to not just UAS, but also all other systems that rely on radio wave communications.[23] In airports, jammers could potentially cause interference in the radio communications between pilots and the control tower.[23] Upon successful disruption by jamming, the behaviour of the UAS is highly unpredictable. Whether it lands immediately, flies back to the operator or shuts down depends on the UAS's sensors and GNSS capabilities (if not disrupted). The UAS can cause collateral damage if it falls to the ground but may provide the opportunity to locate the operator if it flies back.[19,23,26,27]

Overall, while jammers have the potential to have a large coverage and can help to protect a wide area from UAS, there is a need to consider the possibility of damage to other important communications and infrastructure within that area to avoid interrupting over vital activities.

UAS Takeover and Spoofing

Next, GNSS spoofing can be used to take over UAS' navigation. The spoofer works by transmitting GNSS signals that impersonate the real signals to the receiver. This false signal emitted by the spoofer is stronger than the real signal in order to successfully misguide the UAS to the coordinates of the specified landing zone, where it will hover or land.[28]

Standard protection tools such as encryption and certificates to GNSS satellite signals will not be useful in defence against spoofing. Unfortunately, disrupting GNSS signals might disrupt GNSS signals for aircrafts as well.

To access the UAS's video feed, one must bypass the secure and heavily encrypted video protocol; usually Ocusync and Lightbridge in DJI UAS.[29] Since these proprietary protocols are extremely hard to crack, they have a low hijack rate.

UAS vs UAS

This practice uses a defending UAS to take down the target UAS. It is very versatile as many types of methods can be deployed onto the defending UAS based on the situation. Examples include "jamming", or electronic counter-measure (ECM), launching of nets, or simply crashing into the target and exploding to annihilate it. However, UAS vs UAS methods are dependent on the ability of the defending UAS to track and follow the attacking UAS. Furthermore, ECMs mounted on defending UAS have the potential to jam the UAS itself.

Net Guns

A large UAS can be retrofitted with a net to capture the target UAS.[30] The net launcher attached to the UAS is pressurised, which allows it to be launched at the target with force. When the target is in close proximity, the net would be shot out and the propellers of the UAS would be disabled. The UAS will no longer be able to fly, but will still be attached to the net. It would then be brought to the ground or a designated landing spot.[31]

However, using UAS to counter UAS does have its problems. Firstly, UAS are often not easy to control in bad weather. Secondly, the defending UAS is also vulnerable to counter-attacks by the enemy. Conventional electronic and physical means may be employed by the enemy to eliminate the defending UAS. Ground-based methods tend to be easier to control and have a higher rate of success, hence they are more favoured than using UAS.

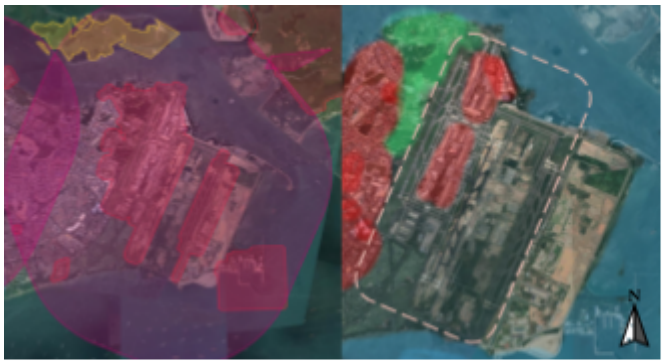
Summary

In short, C-UAS begins with the detection phase, containing the radar to RF sensors to EOIR camera detection systems to ensure that the UAS can be detected in the area to be protected. Following detection and confirmation that the object is indeed a UAS, the UAS' make and model is then identified and compared to a robust database. Lastly, the disruption phase then begins, which may consist of kinetic technologies such as UAS vs UAS and net guns, and non-kinetic technologies such as jamming and spoofing which will all aim to force the UAS to stop its path into the protected areas. However, there are various factors that may impact the effectiveness of these technologies. Many such systems, including radar, RF sensors, RF and GNSS jamming all rely on over-the-air (OTA) signals transmitted in the form of EMF waves. Detection systems would only be useful if signals from the UAS can reach the receiver, and disruption systems likewise. Through employing various mathematical models

to simulate such environmental variables, the coverage of these systems can be reasonably estimated to prevent over- or under-deployment of technologies in the field.

Mapping of Key Installation: Singapore Changi Airport

For the purposes of this simulation, we will take Singapore's Changi Airport as the key installation to be protected by C-UAS systems. In order to ensure UAS do not enter this important region, it is important to detect and disrupt them early and from a further distance away. Hence, this simulation will also involve calculations and classifications for the various environments surrounding Changi Airport.



Terrain	Description of Terrain
Urban: West	Landed properties and apartment buildings.
Foliage: North-West	Vegetation. (generally short trees)
Open Sea: South-East	Almost completely free from obstructions.

Fig 2.1 Annotated Satellite Map of Changi Airport and Surrounding Terrains [32,33]

The UAS Critical Area Map (on left) demarcates a 5km bubble (annotated in purple) around Changi Airport where UAS are not allowed to be flown without a permit. The 4km by 8km perimeter of Changi Airport to be protected where no UAS should be flown at all is in light pink (on right), containing the runways, control tower and various terminals. A colour-coded analysis of the various types of terrain surrounding Changi Airport is also included.

The characteristics of the areas to be protected provide valuable insight into the modelling techniques of RF signals, which will affect how OTA signals may be used in detection using RF signals. An understanding of the effective ability of RF sensors to pick up on RF signals from controllers to UAS and vice versa at varying strengths and under different environmental conditions would be useful in determining the optimal location of the receivers.

Modelling RF Sensors: Physical Modelling

Firstly, calculations were obtained using a simplistic physical LoS model, which assumed that the RF signals are completely obstructed by any buildings and can only pass through open space. The physical model and related variables are defined in Annex A, Figure A.1.

Line of Sight (Open Space) Model

The conditions for LoS to be achieved by either the radar or RF to the UAS are found in Annex A, Table 4. Figure 3.1 provides a visual representation of the physical LoS model. In open space, obstacles such as the building would provide obstruction to the LoS, as demonstrated by the unshaded areas from the dotted to solid line.

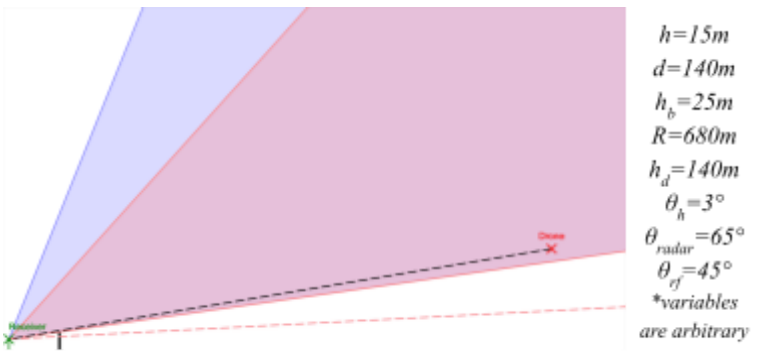


Fig 3.1 Physical Modelling of Line of Sight Model

The UAS would hence only be detectable under this model if it falls within the shaded pink region for RF.

Modelling RF Receivers: Loss Modelling in Open Sea Areas

However, the LoS model does not guarantee detection at excessive distances from UAS to receiver as it is too simplistic. Therefore, various path loss models were identified to more accurately predict how the signal strength changes over distance in various environments. The following table details the various models explored and whether they were chosen for the respective terrains or not. Definitions for the signal loss and power, a full list of the fixed variables used (Table 5) and the respective formulae (Table 6) are found in Annex B.

Model Name	**Terrain**	**Used?**	**Reasoning for Selection**
Free Space Path Loss (FSPL) [36]	Open Sea	Yes	There is largely direct LoS in the open sea, hence the FSPL model is the closest model.
Singapore Environment Loss [37]	Urban	No	The model assumes frequencies of about 27.4GHz which are too high to detect UAS.
COST Hata [38,39]	Urban	No	The model requires the transmitter height (UAS height) to be lower than the receiver height which is unlikely for detecting UAS.
Walfisch-Bertoni (WB) [40,41]	Urban	No	Despite accounting for the losses due to diffraction down to ground level and propagation over rooftops, it becomes less accurate at distances $R < 1000m$, limiting its usage at small ranges. It also cannot accurately model UAS using the 5.8GHz RF channels as frequencies are restricted to 300MHz - 3GHz.
Walfisch-Bertoni Modified (WBM) [41]	Urban	Yes	The WBM Model extends the frequency ranges and provides more accurate losses at distances $R < 1000m$ from WB Model, making this most suitable for Urban areas.
Weissberger's Model [42,43]	Foliage	No	The model is constrained to a foliage depth of no more than 400m, distances beyond that generate unreliable results.
International Telecommunication Union Recommendation (ITU-R) [43]	Foliage	No	
Fitted ITU-R (FITU-R) [43]	Foliage	Yes	The model is applicable for 200MHz to 95GHz, and is optimised for foliage depths more than 400m.

Table 1 RF Propagation Models

Modelling RF Sensors: Estimation of Effective Ranges

As suitable models have been selected to model each of the 3 areas that are mapped out in Figure 2.1, these models are then used to calculate the maximum possible detection distance that the receiver will be effective over, which will once again be useful in determining the placement of the sensors with an understanding of its coverage. In order for these calculations to be conducted, the transmission and receiver powers must first be determined as this greatly affects the losses and distance travelled by the signal. UAS operating on different RF bands have different Effective Isotropic Radiated Powers (EIRP), and these are used as the transmission powers, P_T in Table 2.

Frequency / MHz	Transmission Power (EIRP) / dBm
433	10 [44]
868	14 [45]
900	20 [46]
2400	20 [44]
5800	20 [44]

Table 2 Transmission Power of UAS over Frequencies

A transmission power was not indicated for the GNSS RF bands as the UAS itself does not emit RF signals along that RF band, instead it receives the signals on the band from various satellites and uses that to approximate its location.[47] Therefore, no transmission power can be determined. With these fixed variables, the maximum possible value of B where the UAS can still be detected can then be determined, as well as a plot of how the signal strength varies as the value of B increases.

Modelling RF Receivers: Comparison of Various Areas

The maximum detection distance was obtained from the plot mentioned above which can be found in Annex B, Figures B.1 to B.5. From Table 3, all models agree on the fact that as the transmission distance increases, the signal losses increase i.e. the signal strength decreases until it reaches a point where the receiver can no longer detect it. In general, FSPL presents the most optimistic calculations, indicating that the signals are subjected to much less signal loss as it travels over the Open Sea areas, with FSPL always being more than double of the WBM. This is followed by the FITU-R model and lastly the WBM model with the lowest detection distance. This is as the vegetation modelled by the FITU-R in Foliage areas is less likely to absorb the RF power as opposed to the diffraction due to the buildings in Urban areas.

UAS Operating Frequency / MHz	Maximum detection distance / m		
	FSPL (Open Sea)	FITU-R (Foliage)	WBM (Urban)
433	5410	4170	870
868	4280	3120	810
900	8240	5670	980
2400	3090	2020	720
5800	1280	800	520

Table 3 Maximum Detection Distance of Various Models over Frequencies

The table also shows that the maximum detection distance generally decreases as the frequency increases. This is as all the models indicate a positive correlation between the signal loss and the frequency. The only exception to this case is at the UAS operating frequency of 900MHz, which is due to the much higher UAS transmission power of about 4 times that of 868MHz as the units are in decibels. Therefore, to ensure coverage that protects a similar area, most sensors will need to be placed in Urban areas, slightly fewer in vegetation-dense areas as these obstructions greatly limit the effective range of the RF sensors, and fewest sensors can be placed facing Open Sea areas with little to no obstruction and a wide angle of detection with no obstructions to the LoS.

Similarly to RF sensors, UAS jammers rely on the transmission of RF signals over the air, but these signals travel to the UAS and disrupt the activity of the UAS. After detection, jamming is one of the possible mechanisms to prevent the UAS from advancing further towards key installations.

Communication and Jamming Mechanisms

As RF jamming relies on disrupting the existing communication between the UAS and the controller, it requires significant power to overcome the carrier signal and the excess environmental noise that the RF sensors in the UAS experience. In the case of GNSS jamming, jamming effectiveness is characterised by the carrier-to-noise ratio,[48] expressed as $\frac{C}{N_0}\ dBHz$, where a higher ratio indicates that the carrier signal is higher than the noise, and that reception quality is better and errors are minimal.[22] RF sensors have an initial carrier-to-noise ratio, but the ratio can be affected by jamming to calculate a effective $\frac{C}{N_0}$ ratio ($Eff.\frac{C}{N_0}$). On the other hand, control frequency jamming is characterised by the jamming-to-signal ratio, $\frac{J}{S}$ ratio, where a higher ratio indicates that jamming is more effective.[49]

GNSS Function and Disruption

For the purposes of this study, the focus is placed on GNSS jamming, which jams the RF bands GNSS operates on. Initially, GNSS receivers in the UAS receive various carrier signals from a number of GNSS satellites, and calculates its own position through the transmission times from the different satellites to the GNSS receiver.[50] For the GNSS receiver to identify the satellite that the carrier signal originated from, a special pseudo-random noise sequence (PRN Signal) is integrated into the carrier signal.[50] In order to ensure an accurate estimation of its location, receivers need to acquire a lock onto at least 4 different satellites and have a sufficiently high $\frac{C}{N_0}$ ratio.[50] The calculation for the initial $\frac{C}{N_0}$ ratio without jamming of the GNSS receiver is found in Annex C, Table 7.

Modelling UAS Jammers: Jammer Power Loss

As jamming begins, the GNSS jammer signal experiences signal loss which varies in the various environments. Therefore, the path loss is modelled using the RF propagation models previously identified. However, for Urban areas, instead of the WBM model, the COST Hata Model is adopted instead. This is as the UAS now acts as the receiver instead of as a transmitter in the RF sensors scenario, and the receiver height is now above the transmitter height. This new height configuration is applicable to the COST Hata Model and not the WBM model which led to the change in model.[39,40] The list of fixed variables (Figure C.1, Table 8) and formulae for jammer signal loss (Table 9) have been updated in Annex C.

Modelling UAS Jammers: Effective Carrier-to-Noise Ratio

As the UAS distance to the jammer decreases, the jammer signal loss decreases and the noise levels experienced by the GNSS receivers increase. The $Eff.\frac{C}{N_0}$ ratio decreases, and past a certain threshold, the GNSS receiver loses acquisition of lock onto four satellites, until the UAS loses tracking of its own location,[51] such that the UAS cannot continue determining a flight path towards the key installations and the UAS' mission will be successfully disrupted. The formulae involved in the calculation of $Eff.\frac{C}{N_0}$ (Table 10), as well as the threshold values to lose acquisition of lock onto satellites and to lose tracking (Table 11) are included in

Annex C. The $Eff.\frac{C}{N_0}$ against distance from the GNSS receiver to the UAS were then generated using the determined variables.

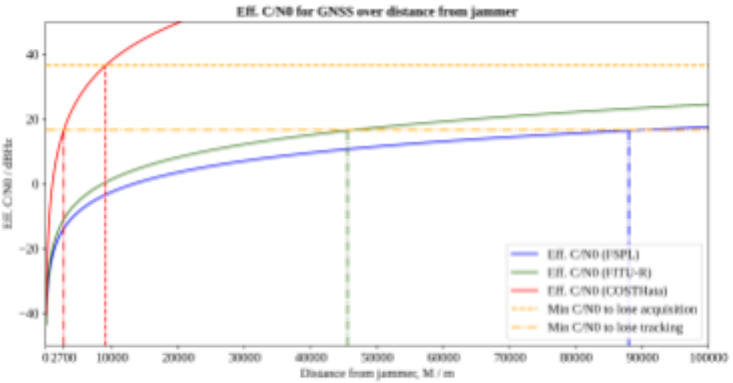


Fig 4.1 Eff. C/N0 for GNSS over Distance from Jammer

From Figure 4.1, it can be observed that as UAS distance from jammer, M, decreases, the $Eff.\frac{C}{N_0}$ decreases. As expected, the COST Hata model for the environment presents the least optimistic value, where the Urban environment limits disruption coverage capabilities to **2.7km** needed to deny location tracking. This is much more limited than the **45km** coverage predicted in Foliage areas by the FITU-R model, and **87km** in Open Sea areas predicted by the FSPL model. Overall, this suggests that jammers are powerful and have the ability to effectively disrupt UAS with a wide area coverage even in obstructed environments. However, jammers will have to be appropriately positioned and directed to avoid impacting other RF-dependent systems and minimise collateral damage.

Conclusion: Optimal Deployment of C-UAS technologies around Changi Airport

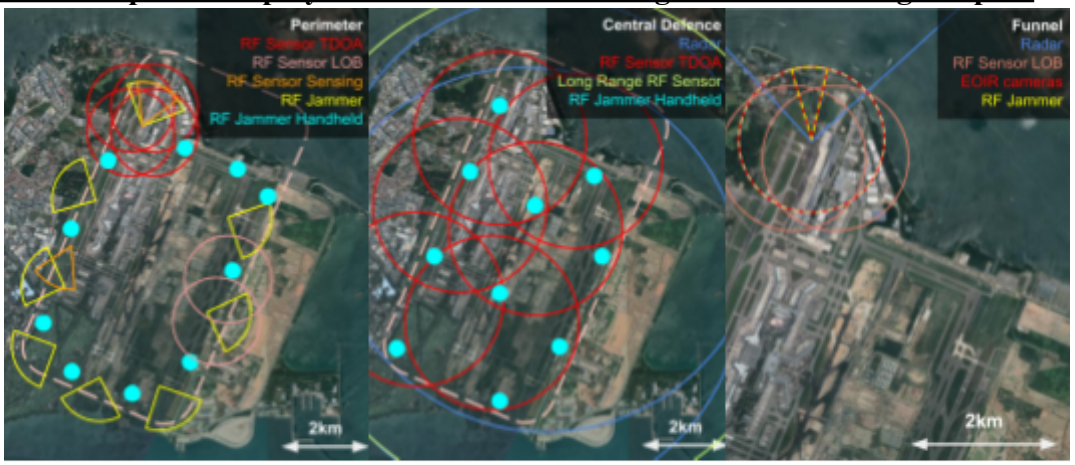


Fig 5.1 C-UAS Systems Deployment on Satellite Map of Changi Airport

Based on our previous analysis and calculations about the effective range of RF sensors and jammers and a study conducted on existing systems at the Singapore Changi Airport, various detection and disruption systems and their ranges were identified to be deployed in our simulation. This list is provided in Table 12, Annex D. We have modelled out 3 possible configurations for deployment of technologies below.

Perimeter

For the perimeter deployment, the widest range of frequencies are available for us to detect UAS on all common UAS communication RF bands using the LOB RF sensors, and the TDOA sensors are able to detect the common 2.4GHz and 5.8GHz RF bands. The 4 TDOA RF sensors are deployed close together with a significant overlap near the runway near Changi Beach such that the overlapping regions provide the capability for multilateration in order to accurately detect the location of the UAS. Apart from that, RF Sensor Sensing are placed at the ends of the same runway. More RF sensors with more informative capabilities are deployed nearer to the Urban and Foliage areas instead of the Open Sea area as UAS

activity is more likely to be much higher from the Urban and Foliage areas. The RF LOB sensors are placed on the side nearer to the Open Sea area to avoid leaving it completely uncovered. All these sensors are placed further out of the perimeter, therefore being able to detect UAS earlier without the need for radar and still providing a sufficiently early warning. Along the entire perimeter, there are regularly mounted RF jammers to effectively disable any UAS attempting to enter the protected airspace. These jammers have full coverage of all UAS frequencies. 10 handheld jammers are deployed all along the perimeter of the airport to cover the blindspots between the stationary RF jammers, and the ground troops with these handheld jammers act as the visual confirmation in place of the EOIR cameras.

Central System

The central system consists of 2 long range radars, a long range RF sensor and 6 TDOA RF sensors. The radar along with the long-range RF sensor provides early warning to any UAS in all directions. However, the long range RF sensor is only compatible with DJI UAS, limiting its functionality. To protect the inside of Changi airport itself, 6 TDOA RF sensors are clustered around the middle. Since the sensors overlap, multilateration calculations can be done to accurately pinpoint the location of the UAS in a 3D space. In order to jam any incoming UAS, 10 handheld jammers are deployed all over the airport, 8 along the perimeter and 2 in the middle. The ground troopers are able to respond to alerts in the control room and act as a second layer of visual confirmation before jamming the drone.

Funnel

The funnel has a Radar with a 60 degree arc and 3km range to provide some early warning of incoming UAS. 2 RF LOB sensors are positioned at the top of the runway, overlapping each other to determine the location of a UAS using triangulation. The coverage of the Radar and the 2 RF LO sensors overlap. In this region, data from both sources can be fused to prevent false positives of UAS detections. The EOIR camera which can rotate is located on the localiser hut near the start of the runway as it is the closest location to the runway the camera can be installed at. The RF jammer is mounted directly on top of the EOIR camera. Since the EOIR camera will visually track the location of the UAS, wherever the camera points at, the RF jammer will also point, increasing the accuracy of the jamming attack.

Conclusion

In conclusion, each of these 3 types of deployment methods each have their pros and cons. Firstly, the Perimeter configuration is able to detect UAS nearing the key installations, and can respond early on. Though it is capable of early detection, there is insufficient coverage in key areas that might need doubling down on. Next, the Central System configuration has the best range and is able to detect all central areas, but there would be a slow response as there are only handheld jammers rather than mounted RF jammers, which would be dependent on human reaction speed of the ground troopers. Lastly, the Funnel configuration minimises UAS interference from the urban areas where UAS are commonly flown and operated. However, though it offers optimal coverage for the urban areas, we also forfeit other areas such as the open sea and foliage. This leaves room for UAS coming from either of these areas to enter and disrupt air traffic.

By understanding the benefits and drawbacks of each system, we are able to efficiently make use of the resources at hand.

Annex A: Physical LoS Modelling

Diagram of Mathematical Variables (RF Receivers)

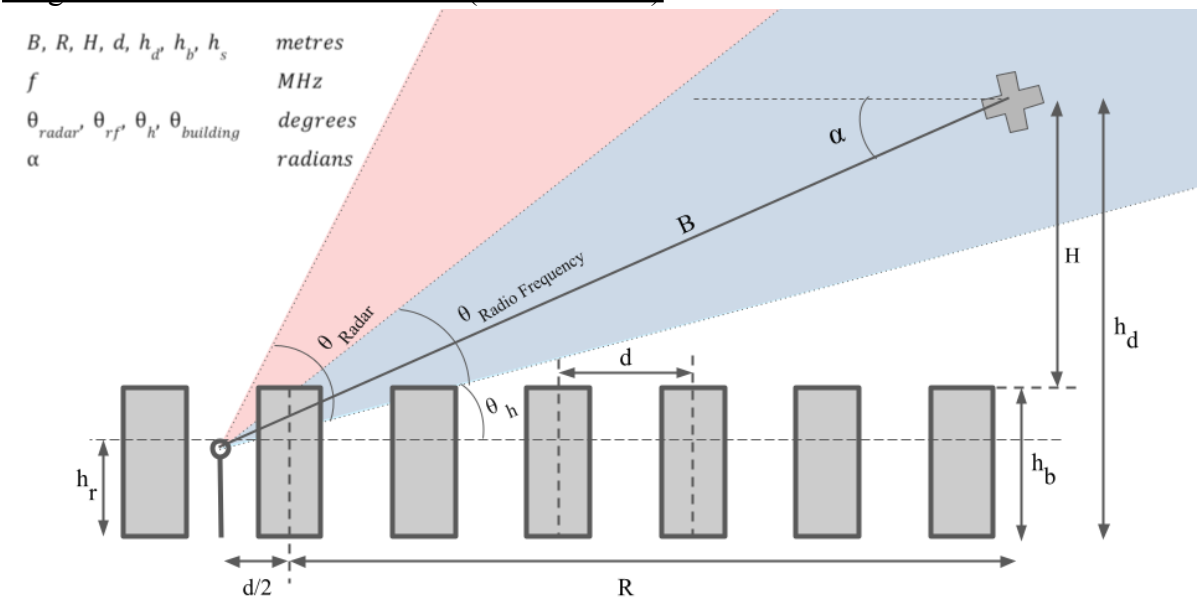


Fig A.1 Diagram of Mathematical Variables for RF Receivers

The diagram represents the UAS as a bolded cross, and the receiver as a circle mounted to a certain height. For the purposes of the physical LoS simulation, the obstruction is modelled as a single building taller than the receiver. While multiple buildings are labelled in this diagram to facilitate calculations in the Urban areas, it is to be noted that only the first building and its related variables will affect the calculations for the physical LoS model as the edge of the first building provides the most obstruction to the LoS. It can also be noted that $B = \sqrt{(h_d - h_m)^2 + (R + \frac{d}{2})^2}$, and the same variables continue to be used for Annex B and Annex C.

Mathematical Conditions for LoS

Note that $\theta_{building} = tan^{-1}(\frac{2(h_b - h_r)}{d})$.

Detected by…	Conditions
Radar	$(\frac{d}{2} + R)tan(max(\theta_h, \theta_{building})) \leq h_d \leq (\frac{d}{2} + R)tan(\theta_h + \theta_{radar})$
RF Receivers	$(\frac{d}{2} + R)tan(max(\theta_h, \theta_{building})) \leq h_d \leq (\frac{d}{2} + R)tan(\theta_h + \theta_{rf})$

Table 4 Fixed Variables and Assumptions for RF Propagation Modelling

Annex B: RF Propagation Modelling

Definitions for Signal Loss and Power

L_{type} represents the loss due to a indicated factor, L_{MODEL} represents the total loss calculated by a indicated model, whereas P_T is the UAS' transmission power and P_R is the signal power received, all in dBm. In general, $P_T - P_R = L_{MODEL} = \Sigma L_{type}$.

Fixed Variables and Assumptions

Fixed Variables	**Reasoning**
$h_b = 15m$	Maximum allowable height of buildings is 3 storeys near Changi Airport, [52] and the maximum floor-to-floor height is 5m. [53]
$d = 10m$	Measurement conducted through Google Maps measurements [32]
$h_r = 10m$	Set to simulate RF propagation model conditions
$h_d = 100m$	While UAS height is not fixed, fixing this value facilitates calculations for B and R. Since $h_d \ll R$ is true in most scenarios, such an assumption has minimal impact on the accuracy of the model
P_T	Refer to Table 1.
$P_R = -90dBm$	This is the minimum detectable signal strength limit, i.e. only signals ≥ -90dBm can be picked up by the receiver determined through operational studies.
F, B (and hence R) are taken as the independent variables to calculate the signal loss.	

Table 5 Fixed Variables and Assumptions for RF Propagation Modelling

Formulae for RF Propagation Models

Model Name	**Formulae**
Free Space Path Loss (FSPL) [36]	$L_{FSPL} = -27.6 + 20lg(f) + 20lg(B)$
Singapore Environment Loss [37]	$L_{SGENV} = L_{FSPL} + 20lg(\frac{2250}{B})$
COST Hata [38,39]	$L_{COSTHATA} = 54.27 + 33.9lg(f) - 13.82lg(h_d) - 3.2\,(lg(11.75h_r))^2 + (44.9 - 6.55lg(h_d))lg(\frac{B}{1000})$
Walfisch-Bertoni (WB) [40,41]	$L_{WB} = L_{FSPL} + L_{msd} + L_{rts}$

	$L_{msd} = 68.9 - 9lg(f) - 9lg(d) + 18lg(\frac{R}{1000}) - 18lg(H) - 18lg(1 - \frac{R^2}{17000000H})$ $L_{rts} = -8.8 + 10lg(f) + 5lg[(\frac{d}{2})^2 + (h_b - h_r)^2] + 20lg\{tan^{-1}[\frac{2(h_b - h_r)}{d}]\}$
Walfisch-Bertoni Modified (WBM) [41]	$L_{WBM} = L_{FSPL} + L_{msd} + min(L_{mr}, L_{rts})$ $L_{msd} \begin{cases} 16.8 + 20lg(R) - 20lg(H) - 10lg(f) - 10lg(d), & for\ \alpha\sqrt{\frac{fd\times10^6}{c}} < 0.4 \\ 0, & for\ \alpha\sqrt{\frac{fd\times10^6}{c}} \geq 0.4 \end{cases}$ $L_{mr} = \frac{2(h_b - h_r)R - dH}{2dH} \times L_{reflection}$, taking $L_{reflection} = 8dBm$ $L_{rts} = -11.5 + 10lg(f) + 5lg[(\frac{d}{2})^2 + (h_b - h_r)^2] + 20lg\{tan^{-1}[\frac{2(h_b - h_r)}{d}] - \alpha\}$
Weissberger's Model [42,43]	$L_{WEISSBERGER} = L_{FSPL} + L_{foliage}$ $L_{foliage} \begin{cases} 1.33(\frac{f}{1000})^{0.284}(R + \frac{d}{2})^{0.588}, & for\ 14m < (R + \frac{d}{2}) \leq 400m \\ 0.45(\frac{f}{1000})^{0.284}(R + \frac{d}{2}), & for\ 0 \leq (R + \frac{d}{2}) \leq 14m \end{cases}$
International Telecommunication Union Recommendation (ITU-R) [43]	$L_{ITU-R} = L_{FSPL} + L_{foliage}$ $L_{foliage} = 0.2(\frac{f}{1000})^{0.3}(R + \frac{d}{2})^{0.6}$
Fitted ITU-R (FITU-R) [43]	$L_{FITU-R} = L_{FSPL} + L_{foliage}$ $L_{foliage} = 0.39(\frac{f}{1000})^{0.39}(R + \frac{d}{2})^{0.25}$

Table 6 Formulae for RF Propagation Models

Variation of Radio Frequency Signal Strength over Distance across Frequencies

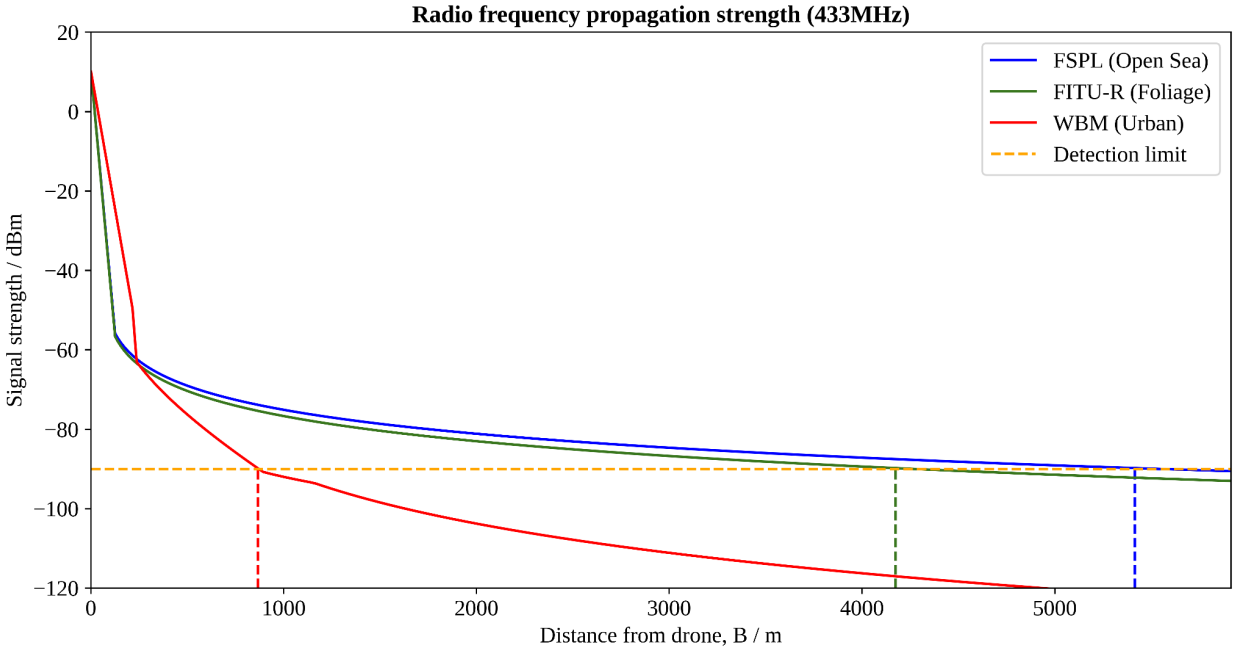


Fig B.1 Radio Frequency Signal Strength over Distance at 433 MHz

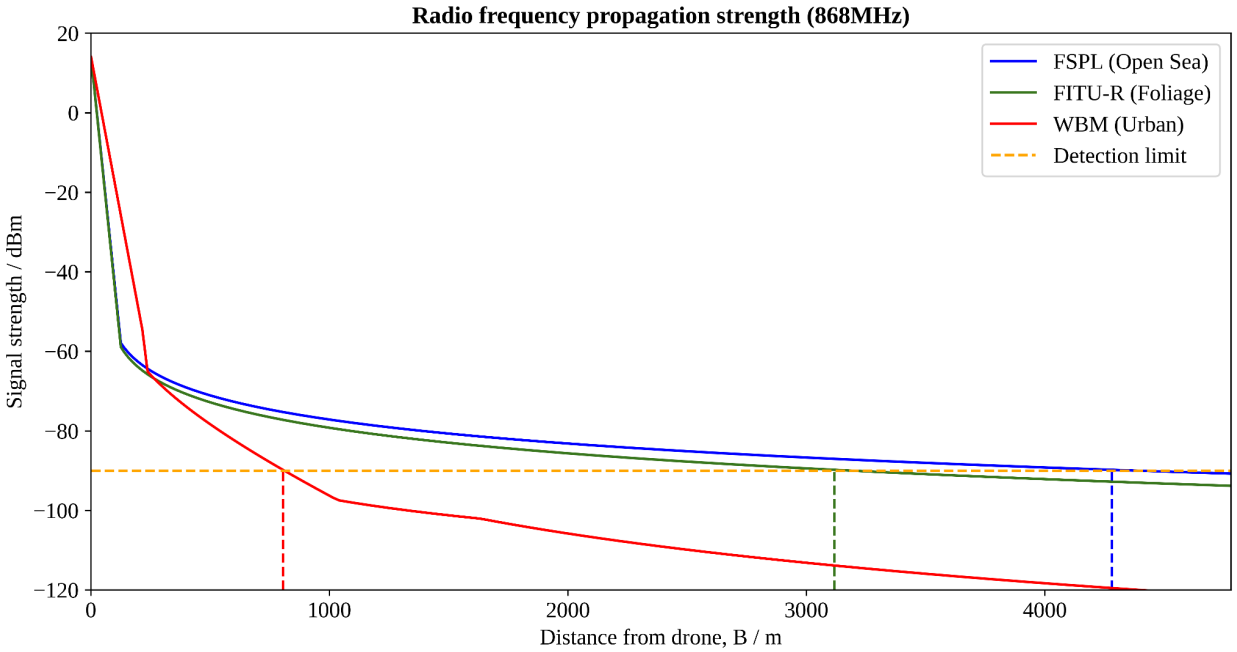


Fig B.2 Radio Frequency Signal Strength over Distance at 868 MHz

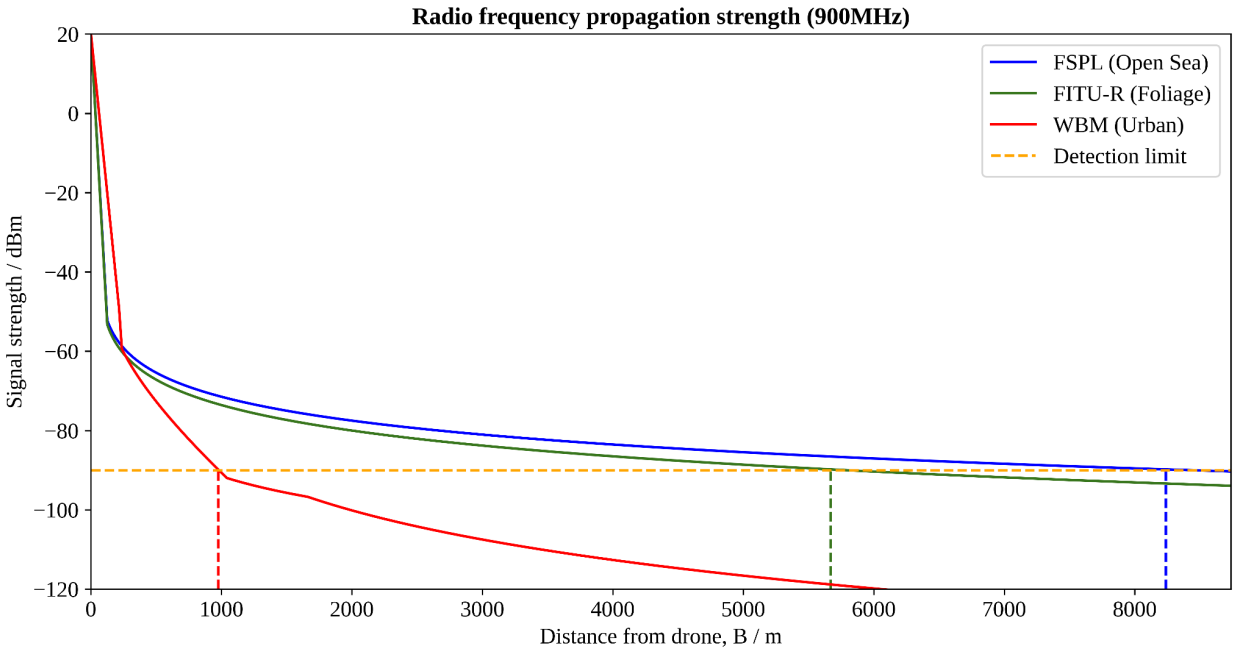


Fig B.3 Radio Frequency Signal Strength over Distance at 900 MHz

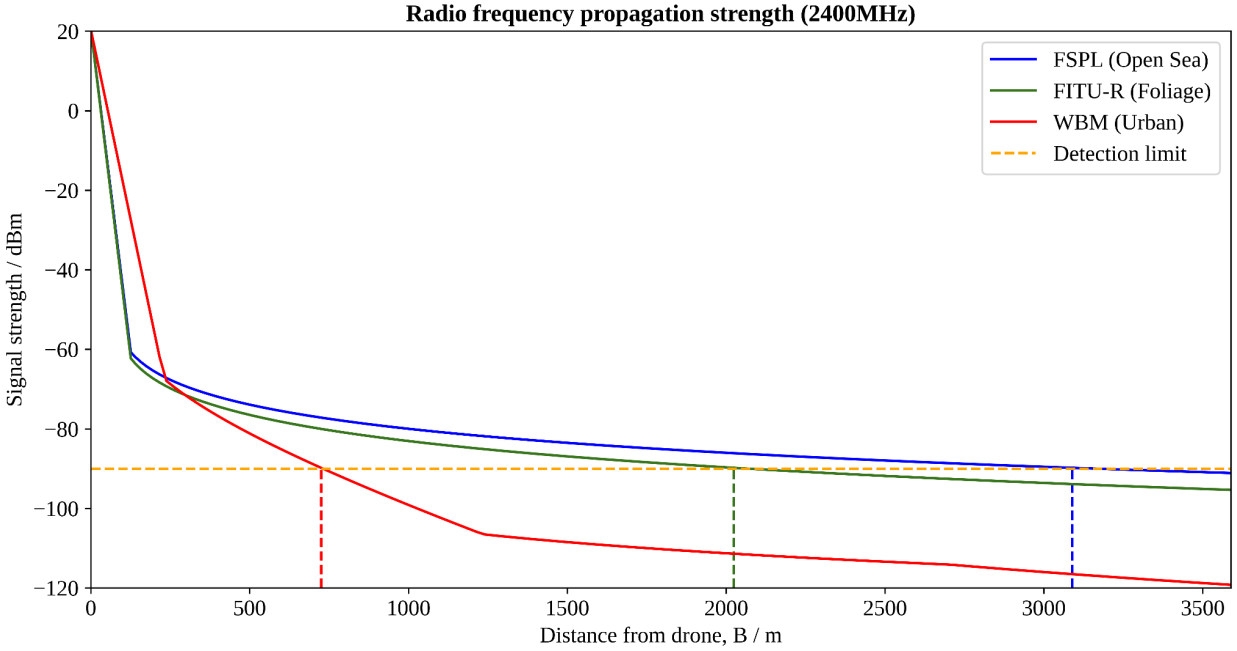


Fig B.4 Radio Frequency Signal Strength over Distance at 2.4 GHz

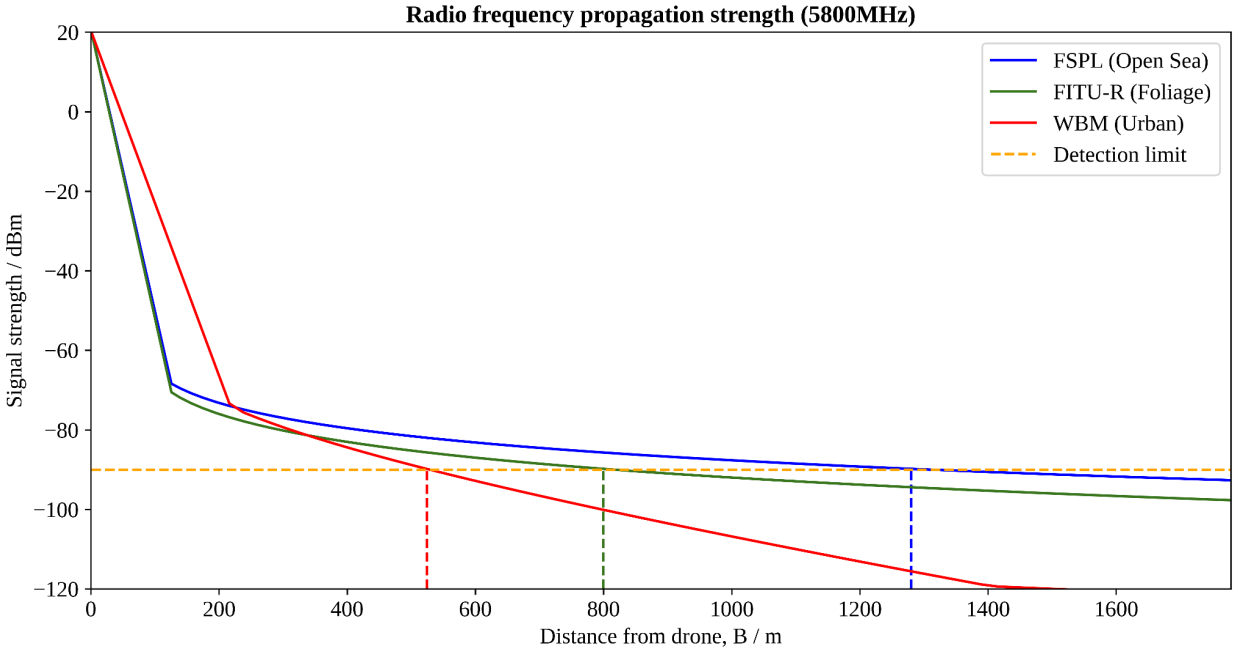


Fig B.5 Radio Frequency Signal Strength over Distance at 5.8 GHz

Annex C: GNSS Jamming Modelling

Initial carrier-to-noise ratio calculation

Fixed Variables	**Reasoning**
$S_{sat} = -130dBm$ [54] (Satellite carrier signal power)	Minimum signal strength from GNSS satellites reaching receiver
$G_{amp} = 29.5dBi$ (Amplifier gain)	Obtained from aircraft GNSS receiver specifications
$k = 1.380649 \times 10^{-23} J/K$	Boltzmann's constant [55]
$T = 295K$ (Noise temperature)	Obtained from aircraft GNSS receiver specifications
$N_T = -173.901dBm/Hz$ (Thermal noise density)	$N_T = 10lg(kT) + 30$ [56][57]
$NF = 2.5dBm$ (Noise figure)	Obtained from aircraft GNSS receiver specifications
$C = -100.5dBm$ (Overall carrier signal power)	$C = S_{sat} + G_{amp}$ [58] (assuming no cable loss)
$N_0 = -171.401dBm/Hz$ (Noise power density)	$N_0 = N_T + NF$ (sum of various noise sources)
$\frac{C}{N_0} = 70.901dBHz$	$\frac{C}{N_0} = C - N_0$ [56] $= S_{sat} + G_{amp} - (N_T + NF)$

Table 7 Fixed Variables and Formulae in Initial Carrier-to-Noise Ratio Calculation

Diagram of Mathematical Variables (RF jammers)

M, D, h_d, h_j	*metres*
G_{amp}, G_R	*dBi*
N	*chips/s*
Q	*(no units)*
P_J, S_{sat}, S_J	*dBm*

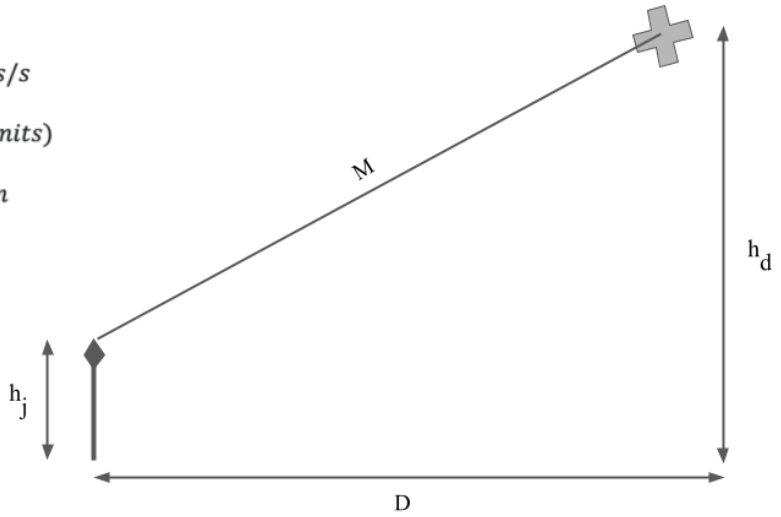


Fig C.1 Diagram of Mathematical Variables for RF Jammers

The diagram represents the UAS as a bolded cross, and a single jammer as a diamond mounted to a certain height. Even though no obstructions are depicted, RF signals from the jammer will still experience severely different losses in the various different environments, and hence the previously identified areas (namely Urban, Foliage and Open Sea areas) still apply to ensure accuracy in the calculated measurements. It is taken that $M = \sqrt{(h_d - h_j)^2 + D^2}$.

Fixed Variables and Assumptions for Jammer Signal Loss

Fixed Variables	**Reasoning**
$P_J = 47.031dBm$ (Jammer EIRP)	As the output power = 8W and jammer gain = 8dBi determined through operational studies, the jammer EIRP is computed to be as such. [59]
$h_j = 10m$	Set to simulate jammer model conditions
$h_d = 100m$	Same assumption as in Annex B to facilitate calculations of D and M.
$f = 1575MHz$	The GNSS jamming is assumed to be on the GNSS L1 band which has a centre frequency of 1575MHz. [60]
M is taken as the independent variable to calculate jammer signal loss.	

Table 8 Fixed Variables and Assumptions for Jammer Signal Loss Modelling

Updated Formulae for Selected RF Propagation Models

Model Name	**Formulae**
Free Space Path Loss (FSPL) [36]	$L_{FSPL} = \ -27.6 + 20lg(f) + 20lg(M)$

COST Hata [38,39]	$L_{COSTHATA} = 54.27 + 33.9lg(f) - 13.82lg(h_j) - 3.2\,(lg(11.75h_d))^2 + (44.9 - 6.55lg(h_j))lg(\frac{M}{1000})$
Fitted ITU-R [43]	$L_{FITU-R} = L_{FSPL} + L_{foliage}$ $L_{foliage} = 0.39(\frac{f}{1000})^{0.39} D^{0.25}$

Table 9 Updated Formulae for RF Propagation Models

Calculation of effective carrier-to-noise ratio

Variables	**Formulae / Reasoning**
$G_R = 5.4dBi$ (GNSS receiver antenna gain)	Determined by operational studies
$Q = 2.22$ (Constant parameter of spectral distribution of external radio emission relative to desired signal spectrum)	Determined by previous studies [51]
$N = 1.023 \times 10^6\ chips/s$ (PRN code rate)	Standard PRN code rate of L1 C/A GNSS band [61]
$S_J\ (dBm,\ variable)$ (Signal strength of jammer reaching GNSS receiver)	$S_J = P_J - L_{MODEL} + G_R$, where L_{MODEL} are the respective path losses that varies with M. [56]
$\frac{J}{S}\ (dB,\ variable)$ (Jamming-to-signal ratio)	$\frac{J}{S} = S_{sat} - S_J$ [62]
$Eff.\frac{C}{N_0}\ (dBHz,\ variable)$ [63,64]	$Eff.\frac{C}{N_0} = -10lg[10^{\frac{-C/N0}{10}} + \frac{10^{\frac{J/S}{10}}}{QN}]$

Table 10 Fixed Variables and Formulae in Effective Carrier-to-Noise Ratio Calculation

Threshold values to cause effect to GNSS receivers

GNSS Receiver Effect	**Fixed $\frac{J}{S}$ ratio**	**Calculated $Eff.\frac{C}{N_0}$ ratio**
Lose acquisition	27.0 [62]	36.561
Lose tracking	47.0 [62]	16.562

Table 11 Threshold J/S and C/N$_0$ Ratio Values to Affect GNSS Receivers

Annex D: Deployment of Detection and Disruption at Singapore Changi Airport

List of Detection and Disruption Systems to be Deployed

System	Range / m	Coverage angle / °	Frequencies / MHz	Quantity
Perimeter				
RF Sensor - TDOA	1000	360	2400, 5800	4
RF Sensor - Line of Bearing	1000	360	433, 868-915, 2400, 5800	2
RF Sensor - Sector	1000	60	433, 868-915	2
RF Jammer	1000	90	433, 868-915, 1575, 2400, 5800	8
RF Jammer (handheld)	500	15	2400, 5800	10
Funnel (Runway)				
Radar	3000	90	-	1
RF Sensor - Line of Bearing	1000	360	2400, 5800	2
RF Jammer	1000	30 (rotatable)	2400, 5800	1
EO/IR	1000	30 (rotatable)	-	1
Central Defence				
Long Range RF sensor	10000	360	2400, 5800	1
Radar	5000	360	-	2
RF Sensor - TDOA	2000	360	2400, 5800	6
RF Jammer (handheld)	500	15	2400, 5800	10

Citations

[1] *Applications and uses for Multirotor drones*. Rise Above. (n.d.). Retrieved November 9, 2022, from https://riseabove.com.au/pages/uav-applications-and-uses

[2] Lykou, G., Moustakas, D., & Gritzalis, D. (2020, June 22). *Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies*. MDPI. Retrieved November 9, 2022, from https://www.mdpi.com/1424-8220/20/12/3537/htm

[3] Guardian News and Media. (2019, June 25). *Drone sightings disrupt flights at Singapore's Changi Airport*. The Guardian. Retrieved November 9, 2022, from https://www.theguardian.com/world/2019/jun/25/drone-sightings-disrupt-flights-at-singapores-changi-airport

[4] Guardian News and Media. (2022, November 1). *Could Ukraine's drone attack on Russian ships herald a new type of warfare?* The Guardian. Retrieved November 9, 2022, from https://www.theguardian.com/world/2022/nov/01/could-ukraines-drone-attack-on-russian-ships-herald-a-new-type-of-warfare

[5] 911 Security. (n.d.). *Drone detection: Everything you need to know: Can drones be detected?* Drone Detection | Everything you need to know| Can drones be detected? Retrieved November 9, 2022, from https://www.911security.com/en-us/knowledg-hub/drone-detection

[6] United States Marine Corps Flagship. (2022, July 14). *Detect, track, identify, defeat: I-CsUAS works to defend against drone*. Retrieved November 30, 2022, from https://www.marines.mil/News/News-Display/Article/3093556/detect-track-identify-defeat-i-csuas-works-to-defend-against-drones-small-unman/

[7] US Department of Commerce, N. O. A. A. (2021, March 5). *NWS Jetstream - how does Doppler radar work?* NWS JetStream - How does Doppler radar work? Retrieved December 19, 2022, from https://www.weather.gov/jetstream/how

[8] Design:zwebs.cn, W. (n.d.). Differences in application between high frequency and low frequency radar level meter. Retrieved December 19, 2022, from https://multisensing.co/html_news/?15-Differences-in-application-between-high-frequency-and-low-frequency-radar-level-meter-15.html

[9] Rahman, S., & Robertson, D. A. (2018, November 26). *Radar micro-doppler signatures of drones and birds at K-band and W-Band*. Nature News. Retrieved December 15, 2022, from https://www.nature.com/articles/s41598-018-35880-9

[10] *Drones and remotely piloted aircraft (UAS/RPAS) - frequencies and radio licences*. Traficom. (n.d.). Retrieved December 19, 2022, from https://www.traficom.fi/en/transport/aviation/drones-and-remotely-piloted-aircraft-uasrpas-frequencies-and-radio-licences

[11] *RF Wireless World*. Drone frequency bands | UAV Drone bands. (n.d.). Retrieved December 19, 2022, from https://www.rfwireless-world.com/Terminology/Drone-frequency-bands.html

[12] *Detection and classification of small UAS for threat neutralization*. DSIAC. (n.d.). Retrieved December 16, 2022, from https://dsiac.org/articles/detection-and-classification-of-small-uas-for-threat-neutralization/

[13] Inpixon. (n.d.). *Time Difference of Arrival (TDOA) multilateration*. Inpixon. Retrieved December 16, 2022, from https://www.inpixon.com/technology/standards/time-difference-of-arrival

[14] What is Eo/ir? What Is EO?/IR? | Teledyne FLIR. (n.d.). Retrieved November 30, 2022, from https://www.flir.com/discover/rd-science/what-is-eoir/

[15] *How does an infrared camera work?* (n.d.). Retrieved December 16, 2022, from https://www.adorama.com/alc/how-do-infrared-cameras-work/

[16] Microsegur. (2021, March 11). *Infrared Light for Security Cameras - Microsegur Blog*. Microsegur. Retrieved December 16, 2022, from https://microsegur.com/en/infrared-light-for-security-cameras/
[17] 911 Security. (n.d.). *Radar Drone Detection | Can drones be detected using a radar?* Retrieved November 29, 2022, from https://www.911security.com/en-us/knowledge-hub/drone-detection/radar
[18] Drone Jamming. (2022, April 12). Netline Communication Technologies. https://www.netlinetech.com/solutions/counter-drone/drone-jamming/
[19] 911 Security. (n.d.). Jammers and Spoofers | Non-Kinetic Counter-Drone Technology. https://www.911security.com/knowledge-hub/counter-drone-technology/jammers-and-spoofers
[20] Corum, C. (2022, January 30). *Contactless 101: Modulation lets radio waves carry data.* CampusIDNews. Retrieved December 13, 2022, from https://www.campusidnews.com/contactless-101-modulation-lets-radio-waves-carry-data/
[21] Carrier Signal. (2020). In *Network Encyclopedia*. Retrieved December 13, 2022, from https://networkencyclopedia.com/carrier-signal/
[22] Froehlich, A. (2021, August 12). *Carrier-to-noise ratio*. Networking. Retrieved December 13, 2022, from https://www.techtarget.com/searchnetworking/definition/carrier-to-noise-ratio
[23] Pilot Institute. (2020, August 6). Drone Jammers: How They Work, Why They Exist, and Are They Legal? https://pilotinstitute.com/drone-jammers/
[24] An Introduction to Jammers. (2022, March 21). JEM Engineering. https://jemengineering.com/blog-an-introduction-to-jammers/
[25] Gaspar, J., Sebastião, P., & Souto, N. (2022). A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities. Sensors, 22(4), 1487. https://doi.org/10.3390/s22041487
[26] The Pros and Cons of Active and Passive Drone Countermeasures – Information Security Buzz. (n.d.). https://informationsecuritybuzz.com/pros-cons-active-passive-drone-countermeasures/
[27] *A primer on jamming, spoofing, and electronic interruption of ... - dedrone*. (n.d.). Retrieved December 16, 2022, from https://blog.dedrone.com/en/primer-jamming-spoofing-and-electronic-interruption-of-a-drone
[28] Kaspersky. (2021, April 26). *Security and drones — what you need to know*. www.kaspersky.com. Retrieved December 6, 2022, from https://www.kaspersky.com/resource-center/threats/can-drones-be-hacked
[29] Kyle, B. (2018, October 15). *DJI OcuSync vs. DJI Lightbridge – What's the difference?* DroneDJ. Retrieved December 12, 2022, from https://dronedj.com/2018/07/27/dji-ocusync-vs-lightbridge/
[30] Kurkowski, S. (2022, April 21). This drone is made to catch other drones with a built-in net gun. DroneDJ. Retrieved November 30, 2022, from https://dronedj.com/2022/04/21/this-drone-is-made-to-catch-other-drones-with-a-built-in-net-gun/
[31] Robin Radar Systems (n.d.). *10 counter-drone technologies to detect and stop drones today*. 10 Counter-Drone Technologies to Detect and Stop Drones Today. Retrieved December 19, 2022, from https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today
[32] *Singapore Changi Airport Satellite Map*. (n.d.). Google Maps. Retrieved December 1, 2022, from https://www.google.com.sg/maps/place/Singapore+Changi+Airport/@1.3521415,103.975908

2,11534m/data=!3m1!1e3!4m5!3m4!1s0x31da17d693d0cde3:0xd6d6dd5e414e4503!8m2!3d1.3644202!4d103.9915308
[33] *Singapore Drone No-Fly Zones Map*. (n.d.). Garuda Plex. Retrieved December 12, 2022, from https://plex.garuda.io/map
[34] (2018a, February 16). *Does Wood Block EMF Radiation?* EMF Academy. Retrieved December 6, 2022, from https://emfacademy.com/does-wood-block-emf-radiation/
[35] (2018b, February 16). *Does Concrete Block EMF Radiation?* EMF Academy. Retrieved December 6, 2022, from https://emfacademy.com/does-concrete-block-emf-radiation/
[36] Kou, Y. (2009, September 19). *Derivation the dB version of the Path Loss Equation for Free Space.* Retrieved December 1, 2022, from https://www.ece.uvic.ca/%7Epeterd/35001/ass1a/node1.html
[37] Soma, P., Ong, L. C., Sun, S., & Yan, M. W. C. (2003). Propagation measurements and modeling of lmds radio channel in singapore. *IEEE Transactions on Vehicular Technology*, *52*(3), 595–606. https://doi.org/10.1109/tvt.2003.811340
[38] Dalela, C., Prasad, M. V. S. N., & Dalela, P. K. (2012). Tuning Of Cost-231 hata Model for Radio Wave Propagation Predictions. *Computer Science & Information Technology (CS & IT)*, 255–267. https://doi.org/10.5121/csit.2012.2227
[39] Singh, Y. (2012). Comparison of Okumura, Hata and COST-231 Models on the Basis of Path Loss and Signal Strength. *International Journal of Computer Applications*, *59*(11), 37–41. https://doi.org/10.5120/9594-4216
[40] Walfisch, & Bertoni, H. L. (1988). A theoretical model of UHF propagation in urban environments. *IEEE Transactions on Antennas and Propagation*, *36*(12), 1788–1796. https://doi.org/10.1109/8.14401
[41] Yamada, W., Sasaki, M., & Kita, N. (2020). Extended Walfisch‐Bertoni Propagation Model to Cover Short Range and Millimeter‐Wave Bands. *Radio Science*, *56*(3). https://doi.org/10.1029/2020rs007161
[42] Weissberger, M. A. (1982). An Initial Critical Summary of Models for Predicting the Attenuation of Radio Waves by Trees. *Electromagnetic Compatibility Analysis Center*. https://doi.org/10.21236/ada118343
[43] Meng, Y. S., Lee, Y. H., & Ng, B. C. (2009). Empirical Near Ground Path Loss Modeling in a Forest at VHF and UHF Bands. *IEEE Transactions on Antennas and Propagation*, *57*(5), 1461–1468. https://doi.org/10.1109/tap.2009.2016703
[44] Infocomm Media Development Authority. (2022, June). *Spectrum Management Handbook*. Retrieved December 6, 2022, from https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/frameworks-and-policies/spectrum-management-and-coordination/spectrummgmthb.pdf
[45] Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard for access to radio spectrum for non specific radio equipment. (2018). In *Harmonised European Standard* (3.2.1). ETSI. https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.02.01_60/en_30022002v030201p.pdf
[46] *FPV System 0.9Ghz 900MHz 100mW Video Transmitter VTX for RC FPV Drone*. (n.d.). aliexpress.com. Retrieved December 6, 2022, from https://nl.aliexpress.com/item/1005003355104526.html?gatewayAdapt=glo2nld
[47] Choudhary, M. (2019, November 1). *How GNSS works?* Geospatial World. Retrieved December 7, 2022, from https://www.geospatialworld.net/blogs/how-gnss-works/
[48] Ornstein, C. (2021, October 18). *Carrier to Noise Ratio: Overview and Applications in Generators*. Ranatec. Retrieved December 8, 2022, from https://ranatec.com/carrier-to-noise-ratio-overview-and-applications-in-generators/
[49] *How much J/S do you REALLY need?* (n.d.). Cyntony Corporation. Retrieved December 8, 2022, from

https://www.cyntony.com/blog/how-much-j-to-s-do-you-really-need-for-jamming-communications
[50] Dewesoft d.o.o. (n.d.). *GPS measurement and recording - GNSS | Dewesoft*. Retrieved December 8, 2022, from https://training.dewesoft.com/online/course/gps-measurement-and-recording-gnss
[51] Kaplan, E. D., & Hegarty, C. J. (2005). *Understanding GPS: Principles and Applications, Second Edition* (2nd Revised ed.). Artech House.
[52] *Street Block Plan: Area Boundary by Changi Heights (Pasir Ris Planning Area)*. (2004, March 3). Singapore Urban Redevelopment Authority. Retrieved December 6, 2022, from https://www.ura.gov.sg/-/media/User%20Defined/URA%20Online/development-control/Street%20Block%20Plans/stb-2004-1.pdf?la=en
[53] Urban Redevelopment Authority. (2022, December 15). *Commercial Building Height*. Retrieved December 8, 2022, from https://www.ura.gov.sg/Corporate/Guidelines/Development-Control/Non-Residential/Commercial/Building-Height
[54] *GNSS: What are the default signal power levels used by PosApp for the GNSS constellations, and why are these values used?* (2018, October 3). Spirent KB Article. Retrieved December 8, 2022, from https://support.spirent.com/SC_KnowledgeView?id=FAQ18565
[55] The Editors of Encyclopaedia Britannica. (1998). Boltzmann constant | Value, Dimensions, Symbol, & Facts. In *Encyclopedia Britannica*. Retrieved December 8, 2022, from https://www.britannica.com/science/Boltzmann-constant
[56] GNSS Solutions: Measuring GNSS Signal Strength. (2010, December). *InsideGNSS*. Retrieved December 8, 2022, from https://www.insidegnss.com/auto/novdec10-Solutions.pdf
[57] *dBW (Decibel-Watt)*. (n.d.). RapidTables. Retrieved December 8, 2022, from https://www.rapidtables.com/electric/dBW.html
[58] A.H. Systems, inc. (n.d.). *Understanding Antenna Gain, Beamwidth, And Directivity*. A.H. Systems, Inc. Retrieved December 8, 2022, from https://www.ahsystems.com/articles/Understanding-antenna-gain-beamwidth-directivity.php
[59] Bevelacqua, P. (n.d.). *Antenna Theory - Effective Isotropic Radiated Power (EIRP)*. Retrieved December 8, 2022, from https://www.antenna-theory.com/definitions/eirp.php
[60] National Telecommunications and Information Administration. (n.d.). *1559-1610 MHz Band*. Retrieved December 8, 2022, from https://www.ntia.doc.gov/files/ntia/publications/compendium/1559.00-1610.00_01MAR14.pdf
[61] Syam, W. (2022, February 27). *Generating GPS L1 C/A pseudo-random noise (PRN) code with MATLAB and C/C++*. Wasy Research. Retrieved December 8, 2022, from https://www.wasyresearch.com/generating-gps-l1-c-a-pseudo-random-noise-prn-code-with-matlab-and-c-c/
[62] Faria, L. A., Silvestre, C. A. M., Correia, M. A. F., & Roso, N. A. (2018). GPS Jamming Signals Propagation in Free-Space, Urban and Suburban Environments. *Journal of Aerospace Technology and Management*, *10*. https://doi.org/10.5028/jatm.v10.870
[63] Glomsvoll, Ø. (2014). Jamming of GPS & GLONASS signals - A study of GPS performance in maritime environments under jamming conditions, and benefits of applying GLONASS in Northern areas under such conditions. *The University of Nottingham*. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2389675/Glomsvoll.pdf?sequence=1&isAllowed=y
[64] Elghamrawy, H., Karaim, M., Tamazin, M., & Noureldin, A. (2020). Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers. *Applied Sciences*, *10*(12). https://doi.org/10.3390/app10124240