DATT Summit
National Harbor, MD
April 25-28, 2016.

Testing GPS Susceptibility to Spoofing Attacks

Tim Klimasewski[1] Lisa Perdue[2]

[1]Spectracom, tklimasewski@spectracom.com

[2] Spectracom, lperdue@spectracom.com

Abstract Spoofing as it applies to GNSS/GPS is an attempt to deceive the GNSS/GPS receiver by broadcasting signals that the receiver will use instead of the live sky signals. A test system for spoofing allows analyzing the three major factors to consider in a spoofing attack: time synchronization to the signals to be spoofed, power level of the spoofing signal compared to the live sky signals, and accuracy of the position obtained by the spoofing signal to that of the actual position of the device being attacked.

Receivers should indicate when something out of the ordinary is happening during a spoofing attack, but if the overall system using the receiver does not monitor or attempt to use these indications, it is difficult to identify a spoofing attack. Understanding how a receiver will respond in a spoofing attack is the key to detecting spoofing. For example, it could be assumed by a navigation system designer that using multiple GNSS systems will prevent a spoofing attack consisting of only GPS. This is only true if the receiver is set up to monitor this type of information.

The spoofing test system allows full control over time synchronization, power levels, and position variation in a completely closed system that will not interfere with actual GNSS signals. Each of these variables is described in detail and a sample of receiver test results presented. Test results include variations of time, power, and position and effects of varying these on three popular, widely-used GNSS receivers. Tests are performed using GPS only and also various combinations of GNSS systems (GPS, QZSS, BeiDou, Galileo, GLONASS) to understand if multi-GNSS is an effective method to overcome spoofing attacks. Using the information obtained by using a spoofing test system, a system using GNSS signals for navigation can fully utilize all information available to enable spoofing detection. Using a spoofing test system will allow a user to better understand the receiver and harden the system against spoofing attacks.

Keywords GNSS, spoofing, hardening, test

1. Introduction

Spoofing as it applies to GNSS/GPS is an attempt to deceive the GNSS/GPS receiver by broadcasting signals that the receiver will use instead of the live sky signals. Spoofing is different than jamming. Jamming is easier for a receiver to detect, and while it can disrupt the receiver, it cannot re-locate it. A spoofing system can be used as an attack on systems that use GNSS for precise timing or navigation. A spoofing system can also be used for researching defense against an attack from unmanned autonomous vehicles. Current research is on-going to determine if a spoofing system can be used to overtake an enemy drone so it can be re-directed in defense of an attack.

A spoofing test system can be used to understand how the system using a GNSS/GPS receiver reacts in a spoofing situation in order to develop mitigation techniques and countermeasures to thwart a spoofing attack. This paper describes the spoofing test system and how it is used to test receiver systems. Understanding the behavior of the receiver when faced with a spoofing attack is key to hardening the receiver for resilient applications of position, navigation and timing (PNT).

2. Spoofing Test System

A spoofing test system can have two different configurations. The first configuration based on a live sky antenna, with one GNSS/GPS simulator and one synchronization system. The simulator is used to spoof the live sky signals in a controlled environment but this test system gets very complicated quickly. It is hard to determine exact power levels and difficult to track a moving vehicle. The second configuration is a full laboratory test system and consists of two simulators and one synchronization system. One simulator acts as the live sky signal and the other as the spoofer. It provides full control over time synchronization, power levels, and truth versus spoofed positions. Using two simulators and a synchronization unit is the preferred method to test the receiver system in order to harden against spoofing attacks.

The test system used in this paper consists of two Spectracom GSG-series simulators, one Spectracom SecureSync synchronization unit, and an RF combiner. A PC is used to control the individual simulators, the RF switch and to monitor the receiver under test. Figure 1 illustrates this test system.

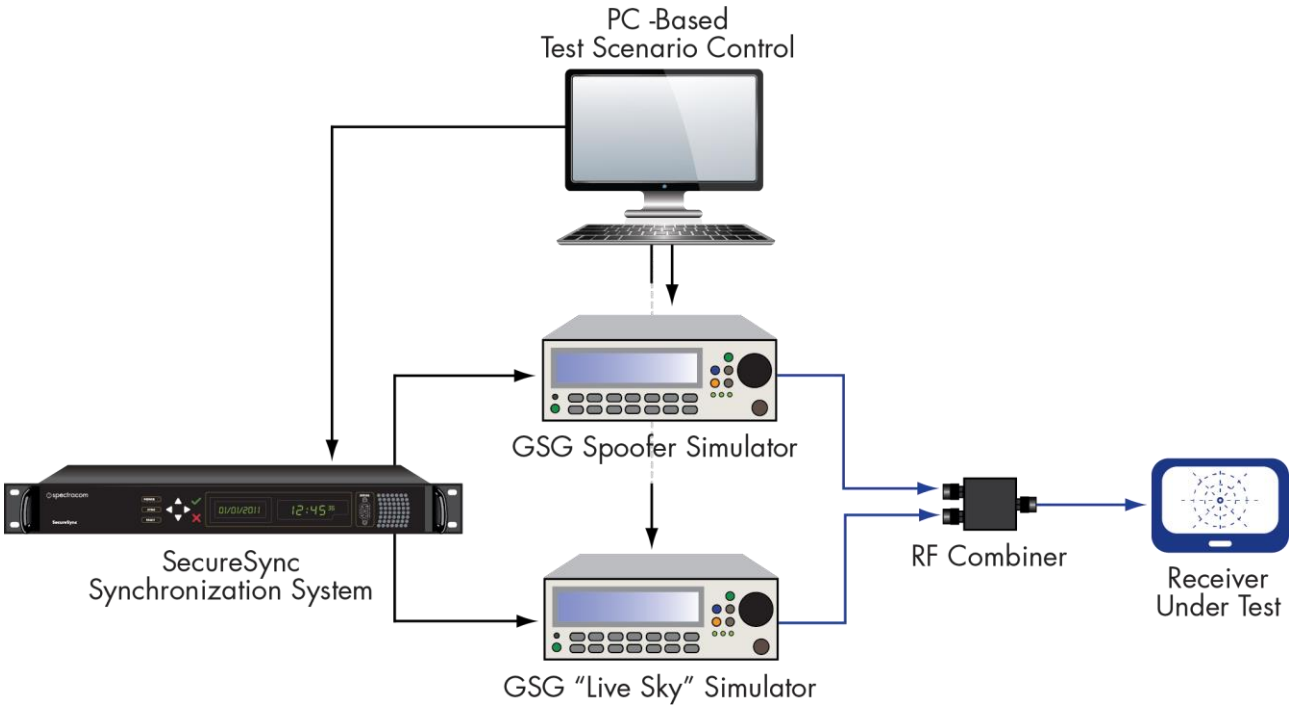


Figure 1 Spoofing Test System

2. Parameters

There are several parameters that can be varied to help understand how vulnerable a specific receiver system is to the spoofing threat. Each of these parameters can be varied independently of the other parameters allowing design of a comprehensive test plan. These parameters are Time, Position, and Power level. Figure 2 shows these parameters.

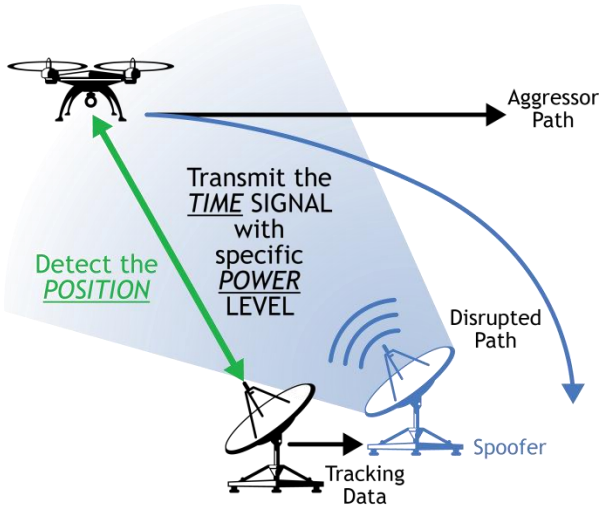


Figure 2 Important Parameters

2.1 Time

The timing accuracy of the spoofing signals to the live signals. Utilizing separate outputs from the synchronization unit the PPS offset can be varied. These PPS signals are used as triggers to the GPS simulators and therefore cause an offset in time between the two RF signals. This offset is controllable to the nanosecond level. Figure 3 shows the interface in the synchronization system for applying the offset.

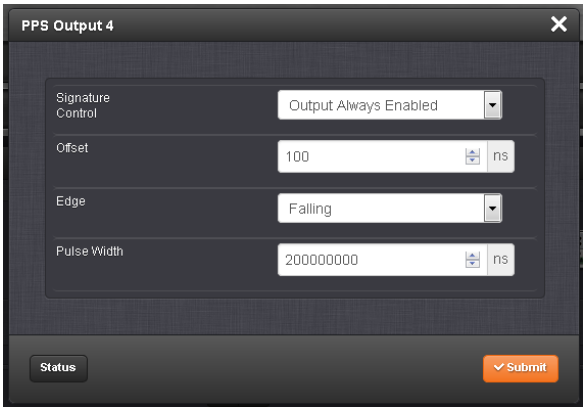


Figure 3 SecureSync PPS Offset Interface

Another time-parameter to consider in the test design is the capture time. This is how long the spoofing signal is applied before attempting to re-direct the receiver.

2.2 Position

The position provided by the spoofer must be accurate to that of the receiver to be spoofed. Exactly how close the spoofer must be to the receiver position is a variable parameter and can be different based on receiver settings, receiver manufacturer, and initial conditions (moving vs. stationary).

Using two simulators allows full control of the two positions so many different test cases can be designed and executed to understand the receiver limitations. The more accurate the spoofer must be to successfully take control of the receiver, the more difficult it will be for an attacker to spoof the receiver. Figure 4 shows an example of the two different positions with a 500m offset.

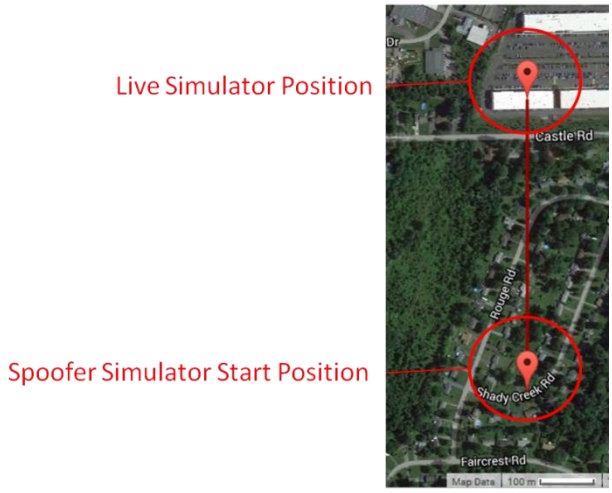


Figure 4 500m Position Offset

2.3 Power

The spoofing signal should be greater than the live signal in order to capture the receiver. The spoofing test system allows full control of the power levels to determine how much greater the power should be. Too much power will jam the receiver. The test system allows testing of the receiver to try and determine if there are any indicators given by the receiver when a signal only a few dB higher than the transmitted signal is received.

3. Test Cases

Several test cases were designed to observe the effects of varying the critical parameters and attempting to spoof the receiver.

Four TIME offset test cases were created. For these cases the position offset was 0 meters and the power level of the spoofer was 2dB higher than the live sky simulator. Offsets of 1 nanosecond, 100 nanoseconds, 500 nanoseconds, and 1.5 microseconds were tested.

Three POSITION offset test cases were created. For these test cases the time offset was set to 1 nanosecond and the power level of the spoofer was 2dB higher than the live sky simulator. Offsets of 50 meters, 250 meters, and 500 meters.

Three POWER offset test cases were created. For these test cases the time offset was set to 1 nanosecond and the position offset is set to 0 meters. Offsets of 2dB, 1dB, and 0dB were tested.

Finally there was a test created for multi-GNSS. In this case the live sky simulator was set to simulate GPS and GLONASS. The spoofer was set to GPS-only. The position offset was set to 0 meters, the time offset was set to 1 nanosecond, and the power level of the spoofer was 2dB higher than the live sky simulator.

Figure 5 is shows the test cases.

Fig. 5 Test Cases

4. Test Execution

The test set up was configured to execute the following sequence:

- **T=0 Start Automated Test Scenario**
  - Live Sky Only (static position)
  - Spoofer is not switched in
- **ΔT=3min Enable Spoofer**
  - Combine Live Sky with the Spoofer set to the starting position
  - Spoofer is automatically switched in
- **ΔT=5sec Initiate Spoofer Trajectory**
  - Spoofer position begins to change via the simulator's predefined scenario:
    - 90 degree heading; 10m/s speed
    - Allows a 5 second capture time
- **ΔT=30sec and ΔT=60sec Automated Data Measurement**
  - Results from receiver's reported position are logged for analysis

Using this sequence tests can be performed in a repeatable and consistent manner, helping to understand the receiver and how its performance is affected when a spoofing attack is attempted.

5. Test Results

Three receivers were used to perform the test cases.

- Septentrio AsteRx3 OEM Receiver (R1)
- Ublox NEO-M8N (R2)
- Inventek USB-GPS / SiRFstarIII (R3)

The test results can be analyzed by comparing the logged positions from the receiver at 30 seconds and 60 seconds after the movement has started. The results summary for 2D position is shown in Table 1. Each case is categorized as not spoofed, partially spoofed, or fully spoofed. Not spoofed (No) means the position did not changed from the live sky position. Partially spoofed (P) means the position was changed but was not that of

the live sky simulator or the spoofer. Fully spoofed (Yes) means the receiver position was that of the spoofer. N/A indicates mode not available in the receiver.

Full test results are given in Appendix A. At 30 seconds the spoofer 2D position is 300 meters away from the live sky position. At 60 seconds, it is 600 meters away. The altitude of live sky and spoofer position remains the same, so any deviation from 0m is due to the spoofing signals.

		R1	R2	R3
TIME	1ns	Yes	Yes	Yes
	100ns	Yes	Yes	Yes
	500ns	P	P	Yes
	1.5us	No	No	No
POSITION	50m	Yes	Yes	Yes
	250m	Yes	P	P
	500m	P	P	P
POWER	2dB	Yes	Yes	Yes
	1dB	Yes	Yes	P
	0dB	P	No	P
MULTI-GNSS	Multi-GNSS with GPS Spoof	No	No	N/A

Table 1. Test Results Summary

6. Phase Compensation

The spoofing test system can also be adapted to use in live over-the-air spoofing scenarios at special test sites. When attempting to spoof a live moving vehicle it is important to also consider the phase shift in the signal as it travels from simulator to the vehicle to be spoofed. The GSG simulator can be commanded to compensate for this distance by utilizing a clock model built into the simulator. This time of flight compensation function is available in the simulator.

7. Conclusion

The Spoofing Test System allows for better characterization through systematic repeatable tests of receiver performance in the presence of a spoofer. By monitoring the available parameters given by the receiver it may be possible to identify and even overcome a spoofing attack. Monitoring loss of lock, receiver noise, IMU system, and estimated position error are possible parameters to observe but each receiver may report different indications. Receivers may also have different modes of operation to test and observe the results.

Observed results provide insight into how different receivers respond to the same threat. More test cases can be created and performed using the features of the spoofing test system in order to fully characterize a receiver and how it responds to a spoofing attack.

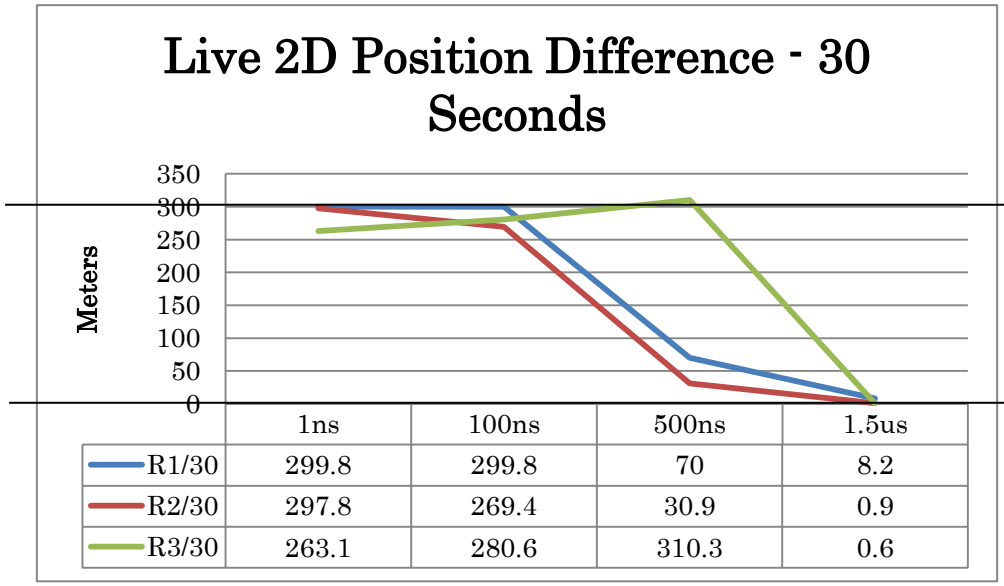
Biographies

Tim Klimasewski – is the marketing director for Spectracom, a leading provider of precision positioning, navigation and timing technology. Since Tim graduated from the University of Rochester in 1987 with a degree in Chemical Engineering, he has worked in high tech markets such as military electronics, instrumentation and process control. He lists GPS as one of coolest innovations of our lifetime.

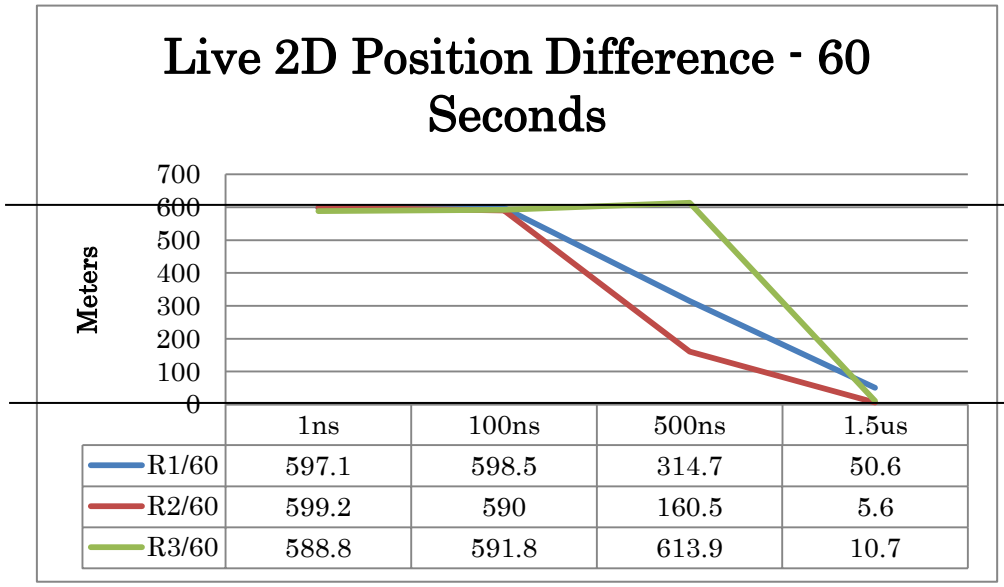
Lisa Perdue is an applications engineer at Spectracom and a specialist in GNSS simulation. She has more than 15 years of navigation and RF systems experience, including 10 years of Naval Service.

Appendix A.

Time Offset Results

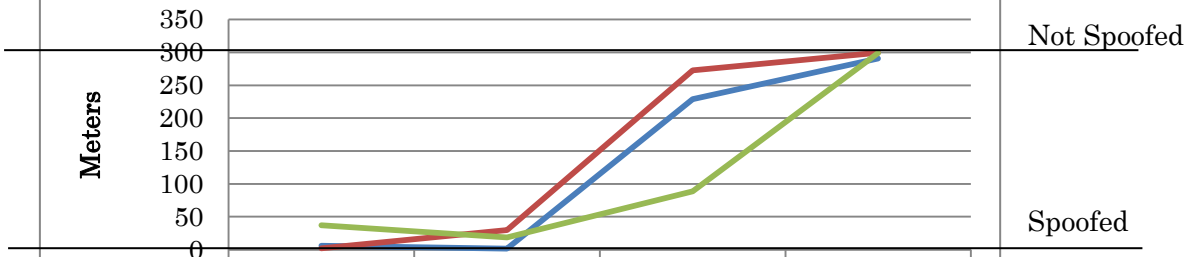


	1ns	100ns	500ns	1.5us
R1/30	299.8	299.8	70	8.2
R2/30	297.8	269.4	30.9	0.9
R3/30	263.1	280.6	310.3	0.6



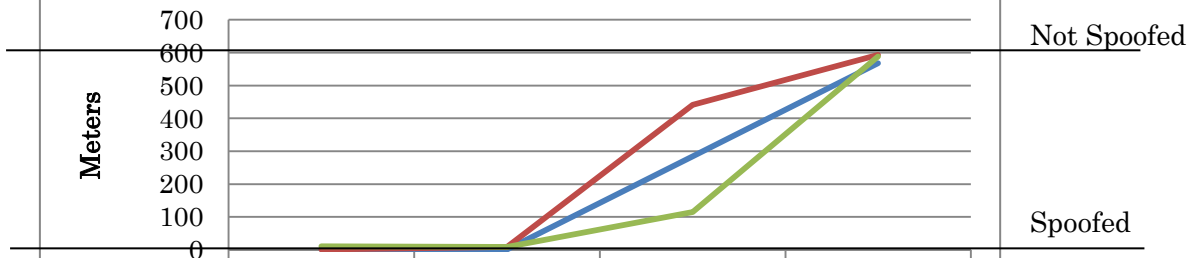
	1ns	100ns	500ns	1.5us
R1/60	597.1	598.5	314.7	50.6
R2/60	599.2	590	160.5	5.6
R3/60	588.8	591.8	613.9	10.7

Spoofer 2D Position Difference- 30 Seconds



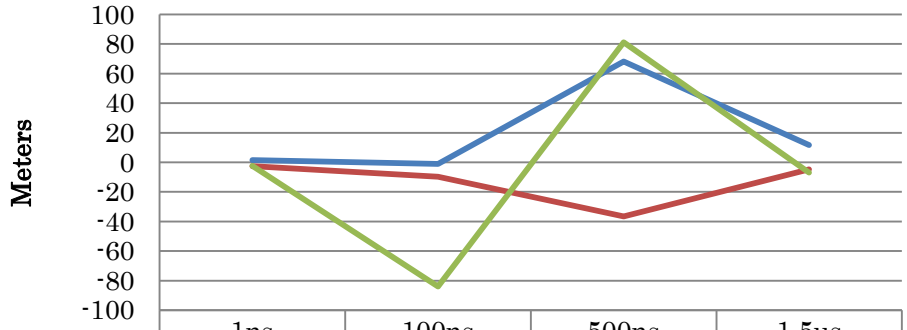
	1ns	100ns	500ns	1.5us
R1/30	5.7	1.2	228.7	291
R2/30	1.9	29.7	272.8	299.6
R3/30	37.1	18.6	88.5	298.9

Spoofer 2D Position Difference - 60 Seconds



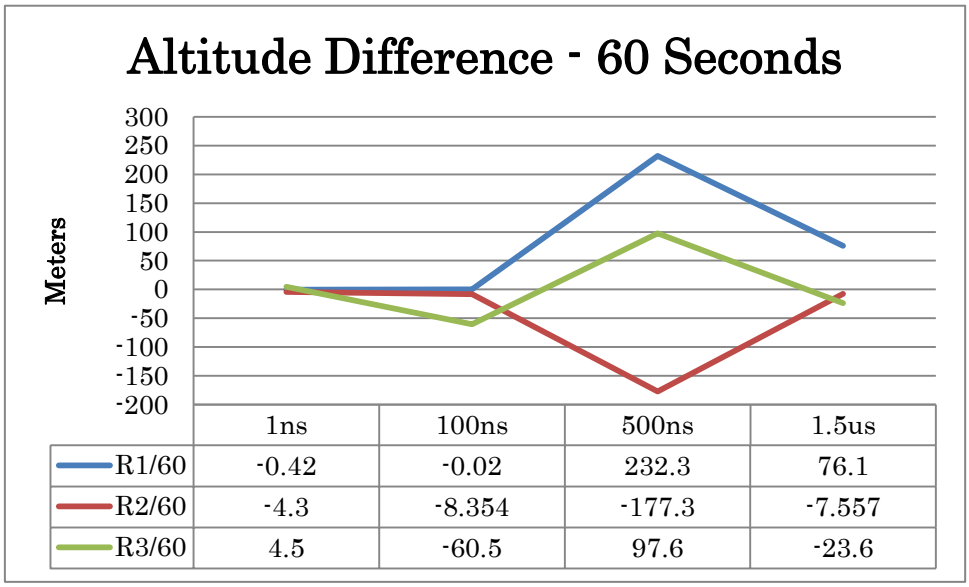
	1ns	100ns	500ns	1.5us
R1/60	1.6	0.4	284.2	568.1
R2/60	1	8.8	441	593.4
R3/60	11.1	9.1	115.2	588.6

Altitude Difference - 30 Seconds



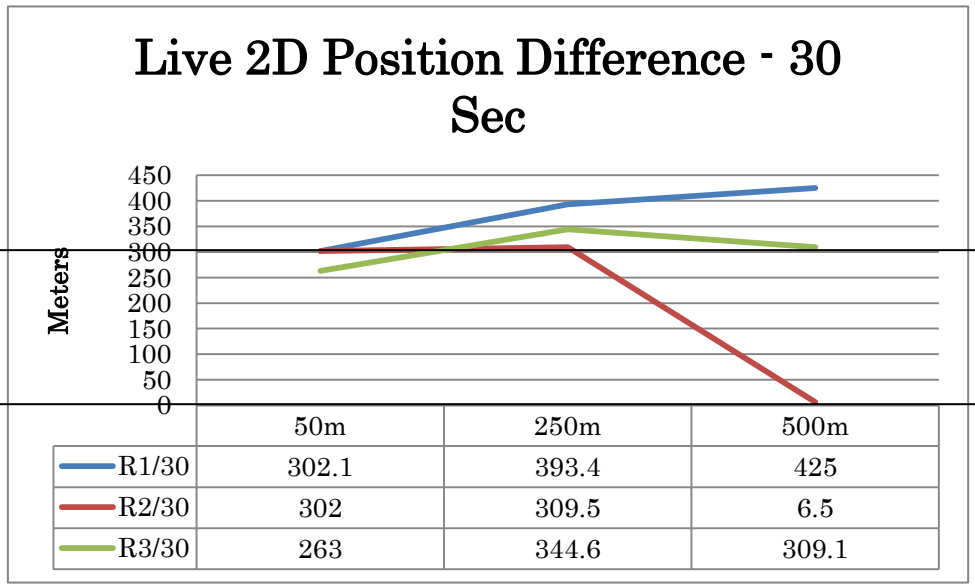
	1ns	100ns	500ns	1.5us
R1/30	1.57	-1.09	68.21	11.72
R2/30	-2.5	-9.789	-36.6	-4.7
R3/30	-2.4	-83.9	81.2	-7

DATT Summit
National Harbor, MD
April 25-28, 2016.

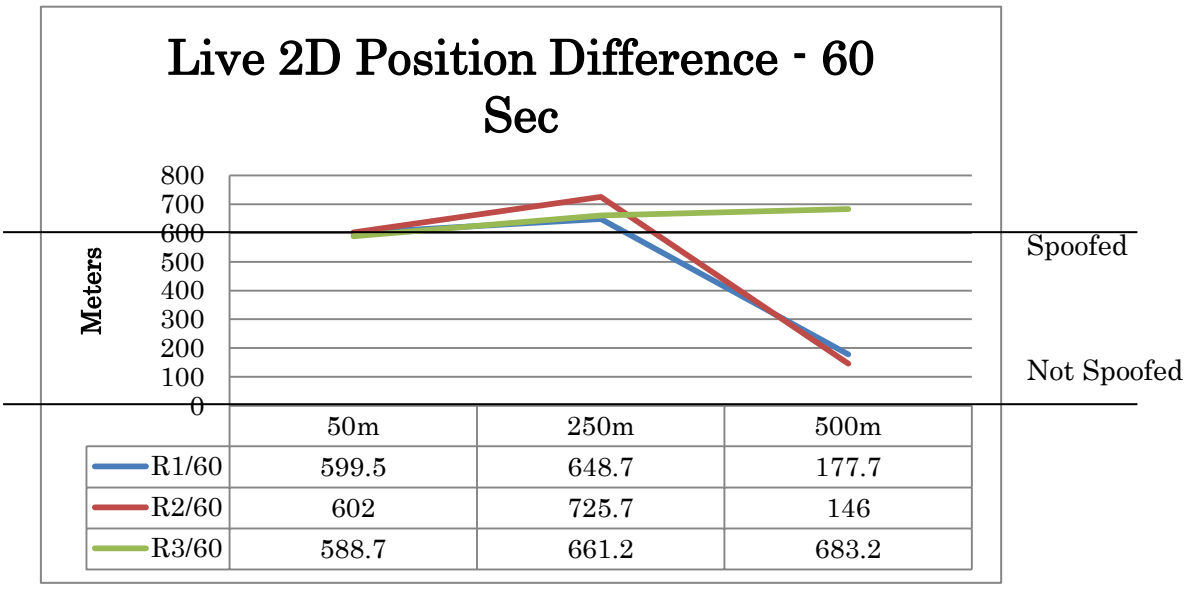


	1ns	100ns	500ns	1.5us
R1/60	-0.42	-0.02	232.3	76.1
R2/60	-4.3	-8.354	-177.3	-7.557
R3/60	4.5	-60.5	97.6	-23.6

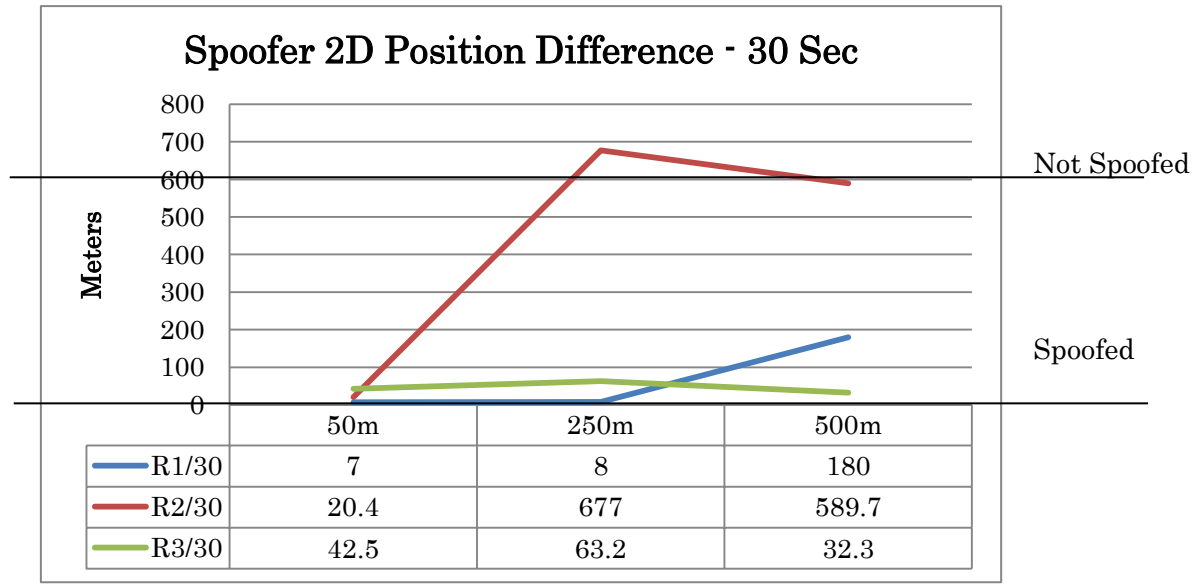
Position Offset Results



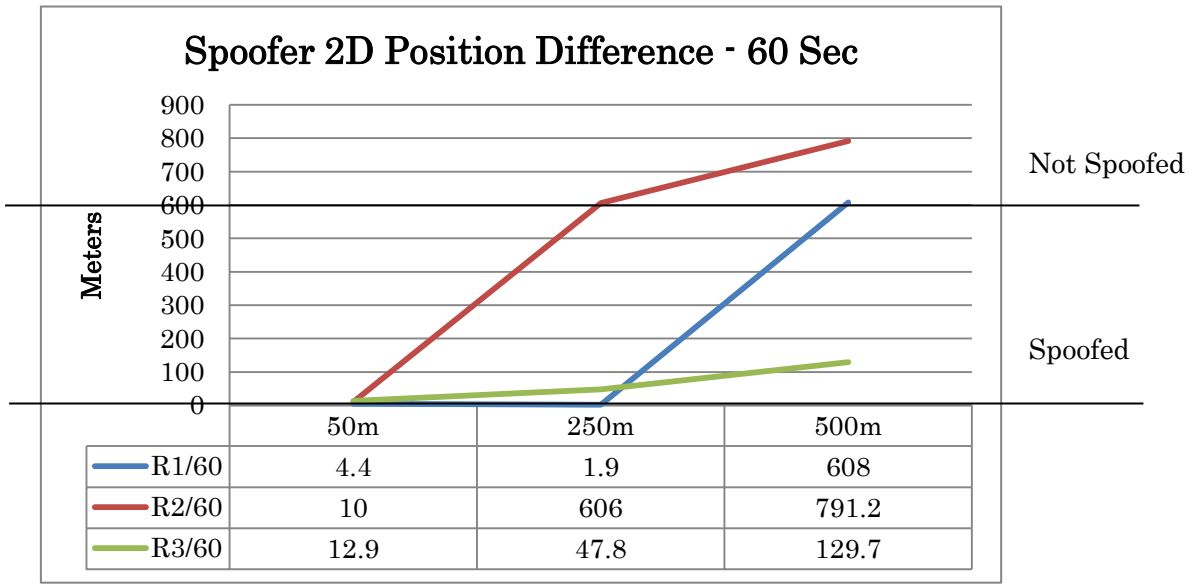
	50m	250m	500m
R1/30	302.1	393.4	425
R2/30	302	309.5	6.5
R3/30	263	344.6	309.1



	50m	250m	500m
R1/60	599.5	648.7	177.7
R2/60	602	725.7	146
R3/60	588.7	661.2	683.2

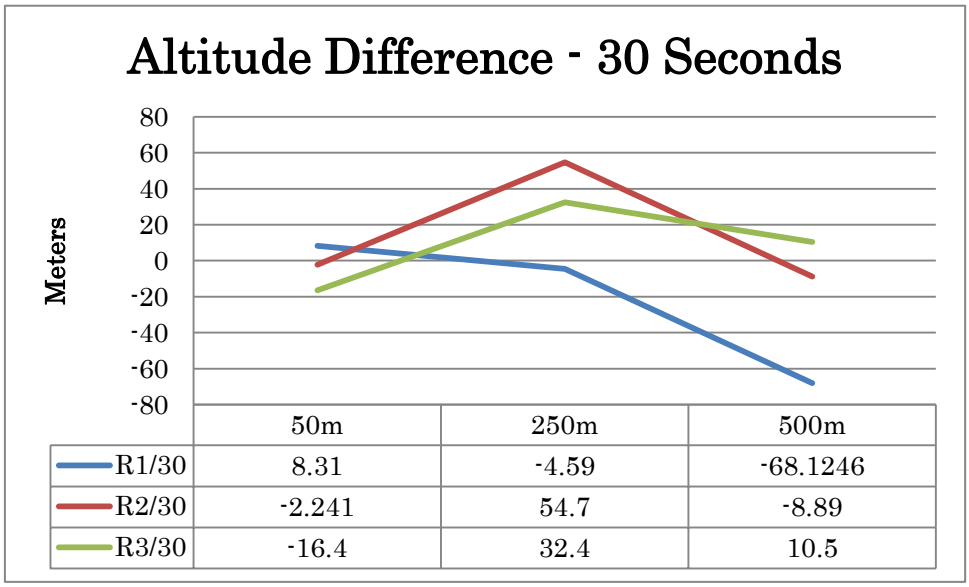


	50m	250m	500m
R1/30	7	8	180
R2/30	20.4	677	589.7
R3/30	42.5	63.2	32.3

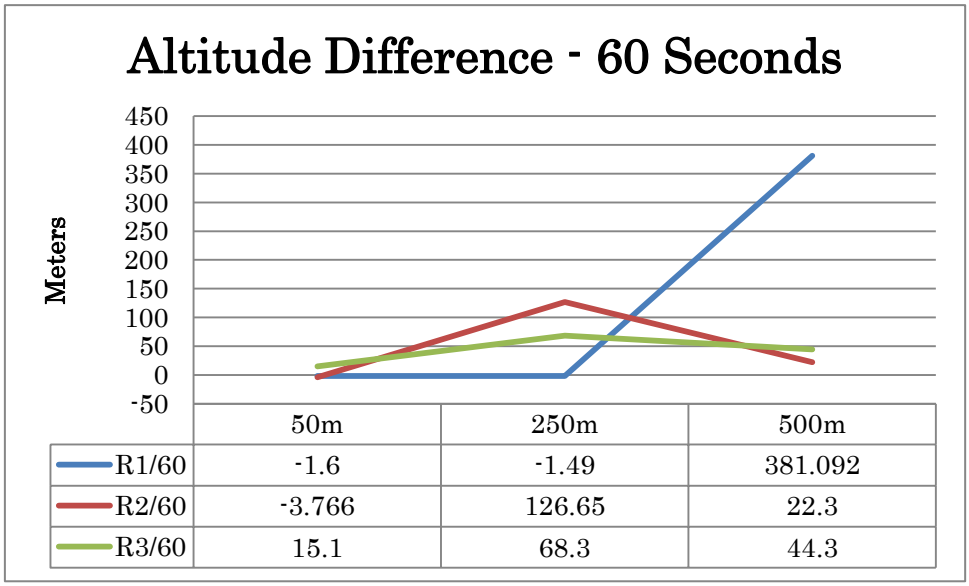


	50m	250m	500m
R1/60	4.4	1.9	608
R2/60	10	606	791.2
R3/60	12.9	47.8	129.7

DATT Summit
National Harbor, MD
April 25-28, 2016.



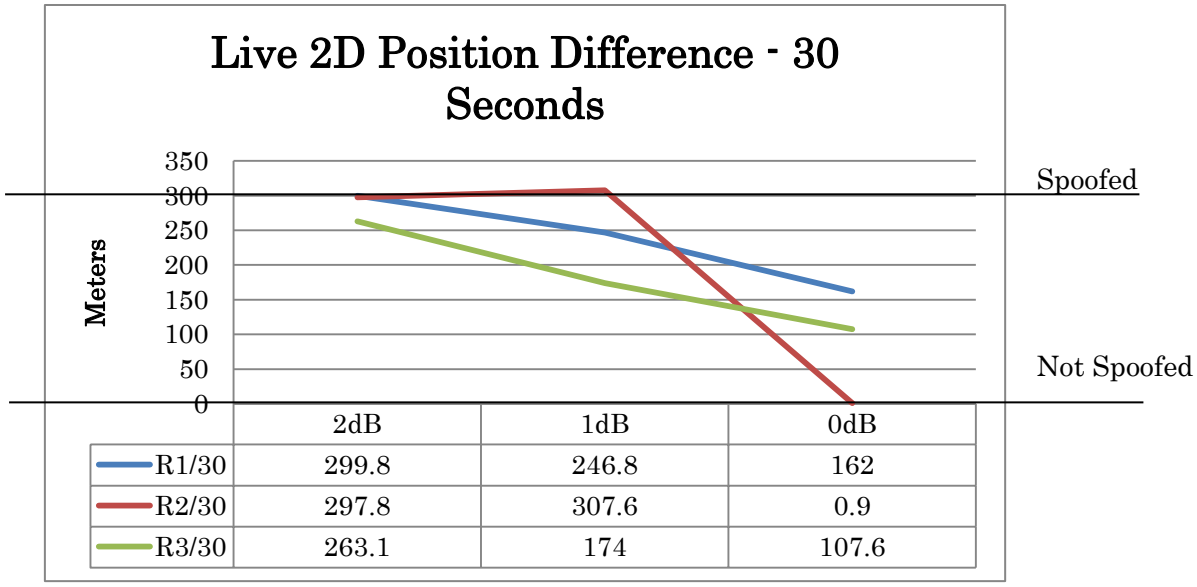
	50m	250m	500m
R1/30	8.31	-4.59	-68.1246
R2/30	-2.241	54.7	-8.89
R3/30	-16.4	32.4	10.5



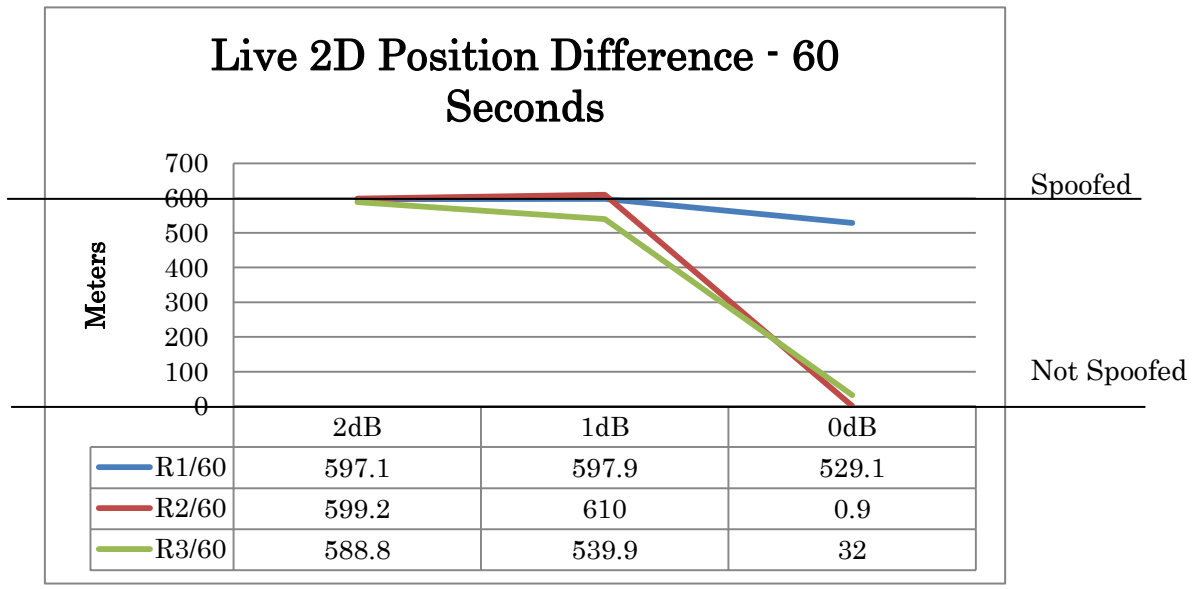
	50m	250m	500m
R1/60	-1.6	-1.49	381.092
R2/60	-3.766	126.65	22.3
R3/60	15.1	68.3	44.3

DATT Summit
National Harbor, MD
April 25-28, 2016.

Power Offset Results

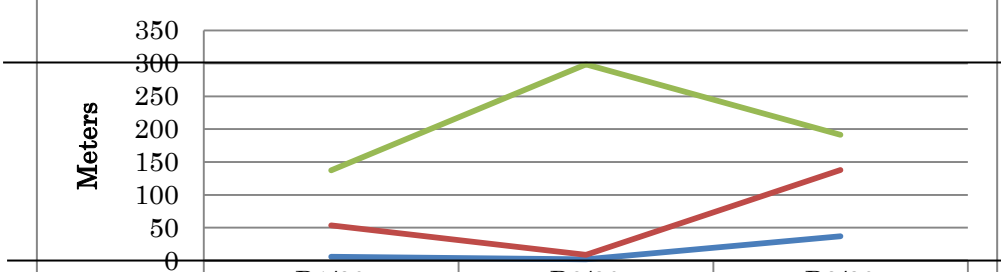


	2dB	1dB	0dB
R1/30	299.8	246.8	162
R2/30	297.8	307.6	0.9
R3/30	263.1	174	107.6



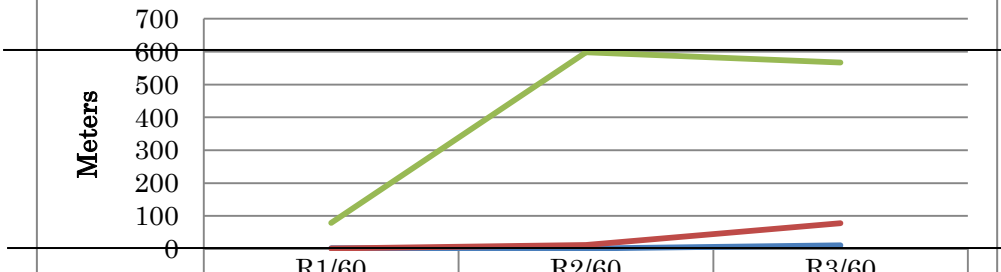
	2dB	1dB	0dB
R1/60	597.1	597.9	529.1
R2/60	599.2	610	0.9
R3/60	588.8	539.9	32

Spoofer 2D Position Difference - 30 Seconds



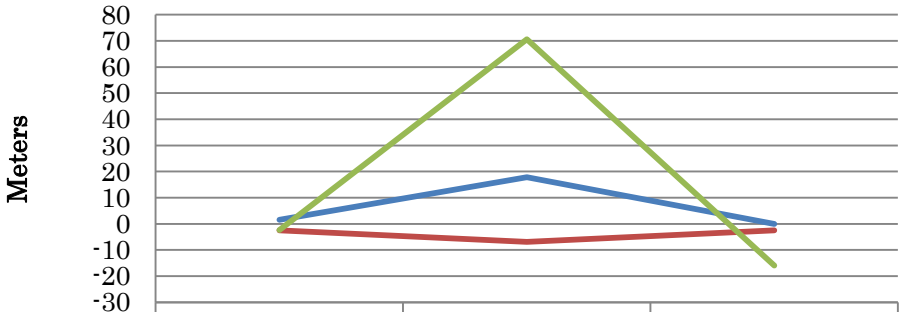
	R1/30	R2/30	R3/30
2dB	5.7	1.9	37.1
1dB	53.4	8.6	137.6
0dB	137.1	298.5	191.5

Spoofer 2D Position Difference - 60 Seconds



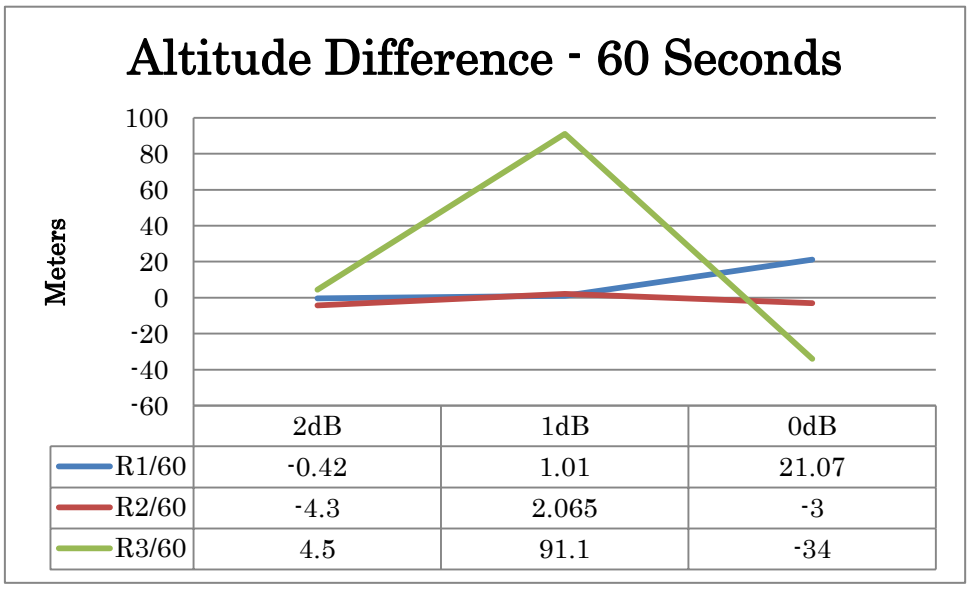
	R1/60	R2/60	R3/60
2dB	1.6	1	11.1
1dB	0.7	12	78.1
0dB	78.7	597.8	567

Altitude Difference - 30 Seconds



	2dB	1dB	0dB
R1/30	1.57	17.85	-0.02
R2/30	-2.5	-6.927	-2.433
R3/30	-2.4	70.6	-15.9

DATT Summit
National Harbor, MD
April 25-28, 2016.



	2dB	1dB	0dB
R1/60	-0.42	1.01	21.07
R2/60	-4.3	2.065	-3
R3/60	4.5	91.1	-34