JAMMER AND INTERFERENCE LOCATION SYSTEM – DESIGN AND INITIAL TEST RESULTS

Alison Brown, Dale Reynolds; *NAVSYS Corporation*.
Capt. Darren Roberts, Major Steve Serie; *Air Force Space Battlelab*

ABSTRACT

Conventional jammer location equipment consists of dedicated electronic intelligence (ELINT) equipment installed in an aircraft pod. This is effective against small numbers of high power jammers but is less effective when the threat is large numbers of low power, low cost jammers. The low power of GPS satellite signals makes it particularly susceptible to jamming or interference. NAVSYS has solved this more difficult jammer detection and location problem through a network centric approach where data is collected from both specialized GPS receiver equipment and conventional GPS user equipment acting as jammer sensors. The data from these sensors is relayed over a data link or network to a JLOC Master Station that can use the data to derive the various jammer locations.

To determine the accuracy that this technique can achieve, NAVSYS is building three types of sensors. The first uses the diagnostic data generated from conventional GPS user equipment to allow it to act as a jammer sensor. With this data from multiple sensors, jammer or interference locations can be derived. The second sensor identifies the Angle-of Arrival (AOA) of the jammer signals at the sensor. This unit is not based on an ELINT equipment design, so it is less expensive than existing jammer location hardware. With the data from one moving AOA sensor collected over a period of time, the jammer or interference positions can be found. The third sensor collects data snapshots of the jammer's RF spectrum at multiple locations. By correlating this data at the Master Station, the jammer or interference sources can be located. The design of this system will be presented.

To demonstrate the capability of a network centric jammer location system, the Air Force Space Battlelab has developed the GPS Availability To Overcome Resistance (GATOR) initiative. Under this effort, the applicability of a network based jammer location system to battlefield conditions will be evaluated and its data timeliness will be measured. In addition, alternative navigation technologies (ANT) will be evaluated for use when GPS is not available on the battlefield. A description of this effort as well as initial test results will be presented.

BACKGROUND

The U.S. military is becoming dependent on GPS not only for navigation, but also for other uses such as targeting and communications synchronization. Civilian users are also increasingly dependent on GPS for navigation (including aircraft landing), power grid synchronization, and communications synchronization (including the cellular phone system). Given our increasing dependence on GPS in our infrastructure and as a military force multiplier, it is critical that receivers be developed that are less susceptible to jamming, and that methods be developed for promptly identifying, and locating GPS jammers.

The current generation of commercial and military digital GPS receivers include the capability to monitor the received signals and are able to detect when signal anomalies occur. By adding the capability to these receivers to record or report data on the observed signal anomaly, a network-centric approach to locating jammer or other interfering signal sources (intentional or otherwise) can be developed.

Figure 1 shows the variety of different types of GPS jammers that could be experienced in a NAVWAR

scenario. These range from large, expensive, high power ECM assets to small, low cost jamming threats. Conventional ELINT methods are very effective against small numbers of high power jammers (>100W). These become easy to counter by designating guided weapons or HARM type missiles against these threats. A more significant threat is the likelihood that large numbers of low power, low cost jammers could be deployed to deny access to GPS over a region of interest (ROI). These are very difficult to locate using conventional ELINT methods and designating a HARM against each jammer would prove extremely costly.

GPS jammer (4 watts) is already being marketed as a commercial item. Terrorists and high-tech vandals may even use GPS jammers during peacetime to disrupt air navigation, which is a threat of great concern to the Federal Aviation Administration (FAA). Unintentional jamming can also occur from weak harmonics of other radio transmitters. Part of the FAA's standard operating procedure for installation of a GPS dependent landing system at an airport is to attempt to identify and locate any sources of interference that may affect GPS operation. To date, there is no cost effective method for the FAA to locate GPS interference sources.

Jammers can transmit different types of waveforms. The most difficult waveforms for an advanced GPS receiver to overcome using signal processing are wide band noise jammers. Narrow band jamming signals can be removed with adaptive filters. (Because the GPS signal is a spread spectrum signal, a narrow band filter that removes a jammer will remove only a small portion of the GPS signal and have no noticeable impact on GPS reception.) The jamming waveforms that must be focused on are therefore wide band signals rather than narrow band signals. Since they are harder to counter in the receiver but are not difficult to build, they are the most likely type of threat to be deployed.

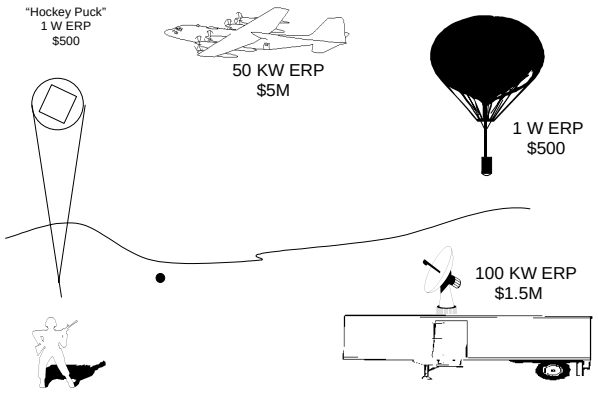

Figure 1 Jammer threats

Because the GPS signals are very weak, they can be jammed over significant distances by even low power, low cost transmitters. Figure 2 shows the jammer/signal (J/S) power levels as a function of distance and jammer transmit power (assumes a line of sight path and a received P(Y) code power of -163 dBw). Analysis under the Phase I effort has shown that C/A code acquisition can be denied with as little as 22 dB J/S. If precise time is known then P(Y) code signal acquisition can continue until the J/S exceeds 34 dB. With advanced signal processing techniques, such as are employed in NAVSYS GPS Acquisition Engine (GPS-ACE) described in section 4.3, acquisition can be achieved under J/S as high as 44 dB. However, as shown in Figure 2, even a relatively low power jammer can have drastic effect on GPS receivers at quite significant distances from the jammer source.

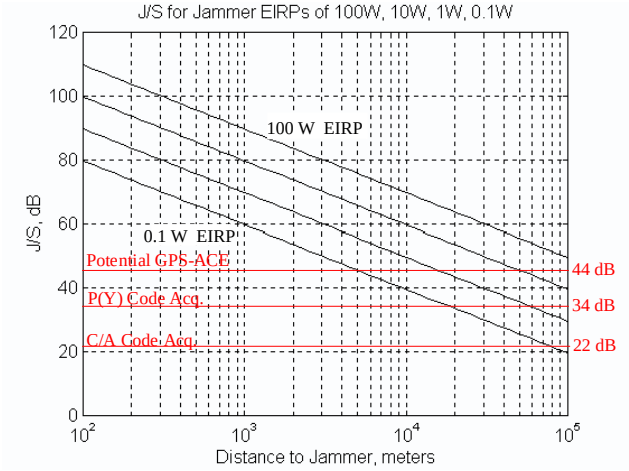

Figure 2 Jammer effects versus distance

The effect of a single 4-watt jammer on the battlefield is illustrated in Figure 3. When close in to the jammer, GPS receivers are unable to track the satellite signals. As the

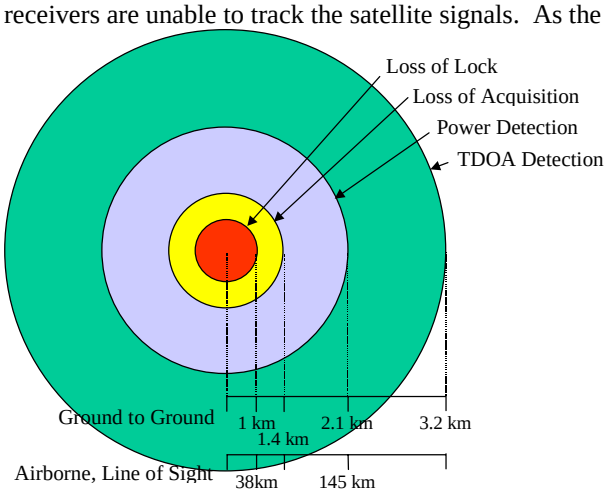

Figure 3 Received J/S as a Function of Distance from the Jammer

distance from the jammer increases receivers are able to track, but not acquire the GPS signals. Airborne users are more affected by a ground-based jammer than ground-based GPS users as they have a direct line-of-sight to the jammer for significant distances. As shown in Figure 3, an airborne GPS receiver would experience degraded operation out to distanced of 145 km from the jammer.

EXISTING GPS JAMMER DETECTION TECHNIQUES

The conventional method of identifying and locating jammers is to employ a suite of dedicated signal recognition and direction finding equipment. Such equipment is often located on specialized aircraft, such as the jammer location pod developed for the US Navy by FALON. While this technique can be effective against a small number of high value jammers, it is not practical against a "mine field" of low cost GPS jammers (such as the "hockey pucks" shown in Figure 1) that could be present on future battlefields.

Because of the high cost of dedicated electronic intelligence (ELINT) platforms, there is often only one platform present in an area. A single platform can have several problems in locating multiple jammers in a "mine field" scenario. The first is that a single platform can only make angle of arrival (AOA) and Doppler measurements. Time difference of arrival (TDOA) measurements can not be made by a single platform. TDOA techniques have many advantages when trying to find a large number of jammers. The second problem is the time required to establish an accurate fix. The single ELINT platform must move to a new location in order to triangulate. If the jammer is a significant distance away then it will take a long time for the platform to move far enough to make a good triangulating measurement. With a large number of jammers, measurements from many different positions will be required to get good measurements on all the jammers. Another problem occurs if the jammer is moving. A single dedicated platform will not be able to establish a target track because both platforms move between measurements. Doppler measurements can be used to gain information about the direction of travel, but Doppler measurements can be fooled if the carrier drifts or is intentionally dithered. A further problem involves the number of jammers that can be located with direction finding techniques. Direction finding techniques using antenna arrays are limited in the number of separate jammers that can be located. With more elements, more jammers can be located, but the physical size of an array is limited on most platforms so that only a small number of elements are practical. The number of GPS jammers may often exceed the number of jammers that can be isolated by an array. Finally, the accuracy of measurements is limited by the pointing resolution and the number of elements.

Under this effort, a cooperative Jammer Location system architecture is proposed that uses data from multiple GPS receivers as jammer "sensors" to provide a large number of observations from which the jammer location can be deduced. With a large number of jammers, a large number of measurements are necessary. To put it mathematically, to solve for N unknowns you need N equations. The bottom line is that many simultaneous measurements are necessary for quickly and accurately locating a large number of jammers and spoofers. Multiple dedicated ELINT platforms are not a good option because of the cost involved. A more cost effective option is to use conventional military GPS users equipment as jammer "sensors" in a networked systems architecture to enable detection of multiple jammers.

The network centric approach proposed will enable a variety of different types of JLOC sensors and anomaly reports to be combined in an integrated solution. Our plan is to leverage data already available from GPS user equipment, rather than requiring special purpose jamming detection equipment to be developed. The alternative types of JLOC sensors using information available from commercial and military user equipment are described below.

C/N0 Jammer Location Sensor

This is the simplest type of sensor that relies on logging GPS C/N0 data from a conventional GPS receiver to deduce where the jammer location is. All that is required is to record the output satellite signal strength data and time and location of the receiver. No special purpose GPS user equipment is required, as this information is available from the standard outputs from most GPS receivers.

The C/N0 jammer location technique relies on observing large variations in C/N0 as a function of distance from the jammer. This method is effective when large variations of C/N0 are observed. However, it is less effective in estimating the location of lower power interfering signals.

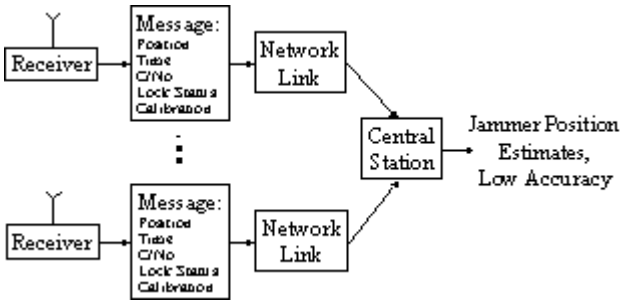

Figure 4 C/No Sensor Architecture

AOA Jammer Location Sensor

The angle of arrival of the jammer signal is observed by military GPS user equipment (UE) that are integrated with Controlled Radiation Pattern Antenna (CRPA) as shown in Figure 5. The CRPA is designed to detect jammer signals and place a null in the antenna pattern in the location of the jammer. This angle-of-arrival (AOA) information can be used to estimate the location of the jammer when the attitude (pitch, roll and yaw) of the aircraft is also known. This location method relies on a triangulation approach shown in Figure 6, using multiple AOA data from a moving aircraft or from multiple observation platforms. This method has the advantage that jammer location can be achieved using only a single aircraft. The location accuracy is primarily a function of the precision of the null-pointing and the inertial heading.

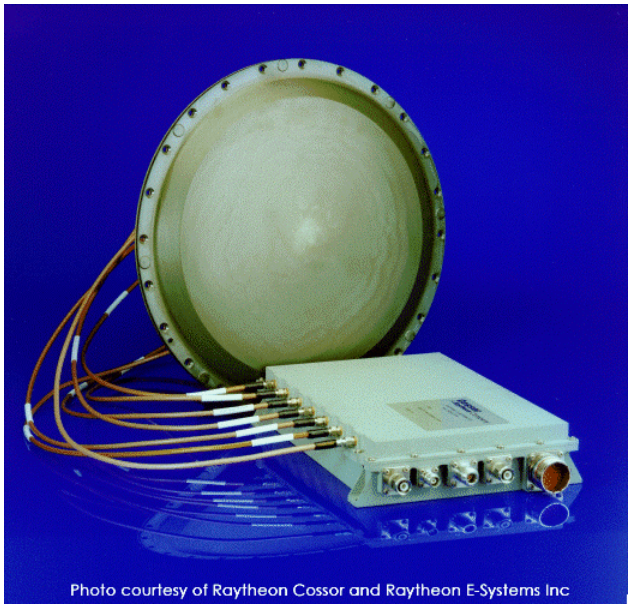

Figure 5 Military User Equipment with CRPA antenna

TDOA Jammer Location Sensor

The TDOA jammer location sensor requires two or more aircraft to be operating in the vicinity of the jammer. This method provides high accuracy jammer location data but requires a GPS sensor that is capable of recording a snapshot of GPS data when in the presence of a jammer signal. Next generation military user equipment include this capability to enable frequency domain processing techniques and digital filtering methods to be applied to aid signal acquisition in the presence of a jammer. The multiple aircraft each collect snapshots of GPS data at synchronized GPS time intervals. The data in the snapshots is cross-correlated to compute a time offset or TDOA observable (Time-difference-of arrival), and a relative doppler offset, or FDOA observable (Frequency-difference-of-arrival). The combination of these observables allows the location of the jammer to be computed and also to separate out signals from different interfering sources. This technique is highly effective when multiple jammers are present in the same area.

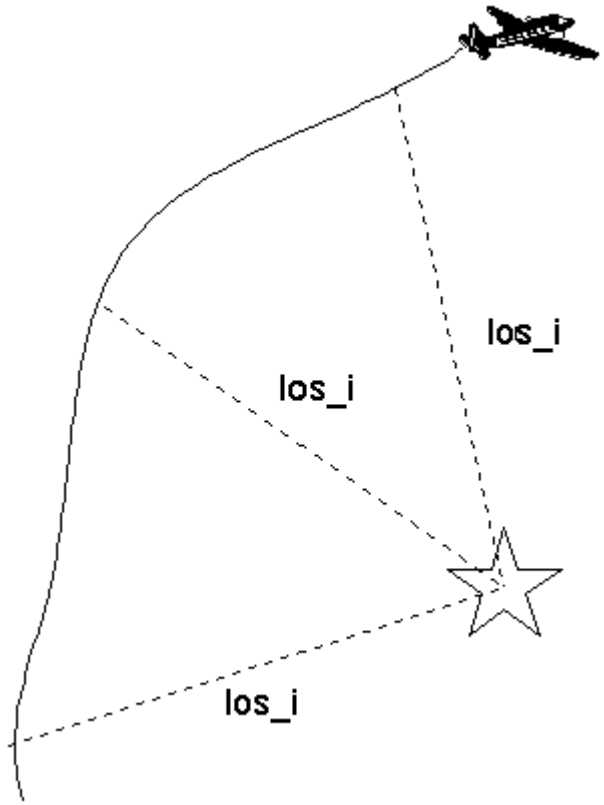

Figure 6 Triangulation approach needed for AOA jammer location sensor

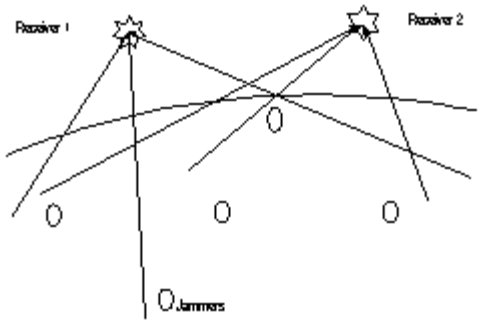

Figure 7 Triangulation approach needed for TDOA jammer location sensor

TECHNIQUE EVALUATION

To evaluate these various techniques, the Air Force Research Laboratory (AFRL) at Wright Patterson Air Force Base has directed NAVSYS to put together a evaluation suite that can be used to evaluate each of the three techniques. This has been combined with efforts from the Air Force Space Battlelab to arrange for live

jamming testing of these techniques under the GATOR initiative.

Evaluation Suite

To minimize costs, COTS/GOTS hardware was selected whereever it was cost effective. As shown in ,the C/No sensor has been selected to use a PLGR GPS receiver in combination with a palmtop or laptop computer to act as a data logger.

Figure 8 Demonstration C/No jammer location Sensor

For the AOA sensor, using an existing CRPA with GPS user equipment would be too difficult to analize. Therefore, a modified version of the NAVSYS High-gain Advanced GPS (HAGR) receiver has been selected. The architecture for this interference direction finder in shown below in Figure 9 and Figure 10.

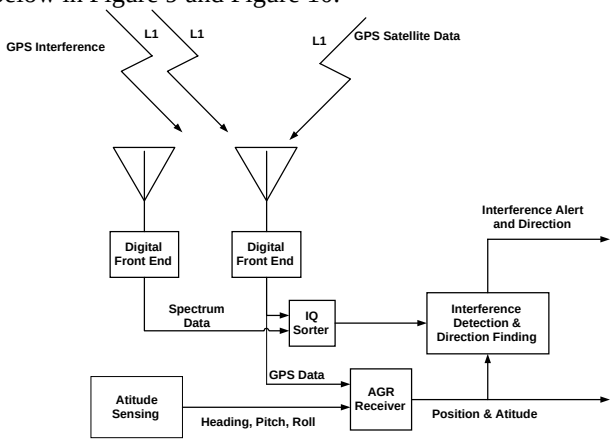

Figure 9 Block diagram for Interference Direction Finder

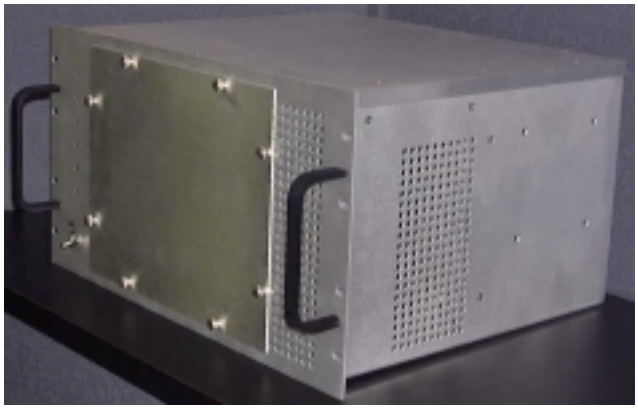

Figure 10 Photo of Interference Direction Finder

For the TDOA sensors, flexability is needed to evaluate the impact of recever time accuracy upon the sensor positional accuracy. To overcome this, a precise continuous GPS spectrum recording is needed at each TDOA jammer location sensor. Therefore, the NAVSYS GPS data logger shown in Figure 11 has been selected as the TDOA sensor. By analizing the GPS time before jamming is activated and having an atomic clock being used for sampling, accurate logging of the GPS spectrum can be achieved for long periods of time.

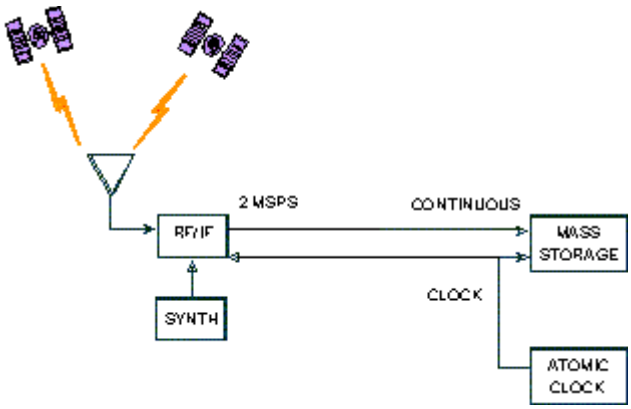

Figure 11 Block diagram of TDOA jammer location sensor

GATOR Initiative

The purpose of the GPS Availability To Overcome Resistance (GATOR) project under the Kenney Battlelab Initiative (KBI) is to determine the operational capability of using existing GPS COTS/GOTS equipment (installed in surface and airborne assets) to ensure accurate navigation within an Electronic Warfare (EW) environment.

To accomplish the stated purpose, this initiative will demonstrate the capability to conduct the following tactics: 1) locating GPS interference/jamming via the Jammer Location (JLOC) approach while continually operating within the EW environment using the GPS Receiver and 2) selecting alternate navigation techniques (ANT) as a backup if the severity of the EW environment warrants (e.g., TACAN, LORAN, Other satellites, etc.)

This initiative will also deliver a validated GATOR concept of operations (CONOPS) for employing this capability to the warfighters (e.g., an AEF, JFC, JFACC, or CINCs).

Objectives and Measures of Merit:

The objectives and measures of merit are organized around the two related parts of the initiative.

1) Jammer Location (JLOC)

a) Objective: Demonstrate that COTS and GOTS GPS user equipment technology can provide accurate and useful jammer location (JLOC) sensor data. Show a GPS jammer location and source can be determined by using centralized processing.

b) Measure of merit:

1) Determine ability of central processing system to isolate and locate GPS jamming sources by comparing jammer actual location vs. computed location.

2) Determine time required to process GPS jammer locations.

(a) Processing time.
(b) Time from detection to isolation solution.

2) Alternative Navigation Techniques (ANT).

a) Objectives:

1) Identify alternative navigation tools to employ if GPS were not available due to jamming, spoofing, or terrain limitations.

2) Demonstrate the effective use of alternative navigation systems.

b) Measures of Merit:

1) Identify critical navigation system characteristics, such as accuracy and coverage/availability.

2) Compare the characteristics of several systems. Determine which systems(s) would best serve as an alternative to GPS based on the above-mentioned characteristics specified in paragraph 3)b) 1).

3) Determine if these actual system capabilities are sufficient for current navigation requirements.

CONCLUSION

The following technical objectives will be achieved.

- Develop GPS integrated Jammer Location (JLOC) System Architecture and sensors. The system requirements and architecture for the JLOC system have been defined and are illustrated in Figure 4 and consists of the following elements: JLOC sensors which are GPS user equipment modified to provide anomaly reports in the presence of a jammer; JLOC data link to provide network connectivity from the sensors; and a JLOC master station which archives and analyzes the JLOC sensor data. Three different types of JLOC sensors are described: a C/N0 JLOC sensor, based on a conventional GPS UE, which provides reports of GPS signal strength; an Angle-of-Arrival (AOA) JLOC sensor, based on a GPS UE integrated with a CRPA, which provides directional data to the jammer; and a TDOA JLOC sensor, based on next generation GPS UE with adaptive A/J filtering, which provides raw jammer spectral data for TDOA/FDOA analysis.

- Develop jammer location algorithms. The jammer location algorithms, required to process the C/N0, AOA and TDOA data, were derived analytically and provide for optimal fusion of the data from the different JLOC sensor sources.

- Demonstrate performance using live jamming signals. Simulation data has been generated to demonstrate the performance of the C/N0 and TDOA jammer location algorithms. Using actual jamming environment data collected in the field, the performance of the various sensors can be evaluated and the location algorithms refined.

ACKNOWLEDGEMENT

This work was sponsored under the Air Force Research Laboratory SBIR contract F33615-99-C-1433, "Jammer Detection, Direction Finding, and Location."

REFERENCES

[1] Critical Item Development Specification for the Controlled Reception Pattern Antenna (CRPA) Line Replaceable Unit (LRU) of the NAVSTAR Global Positioning System Antenna System-1 (GAS-1), CI-GAS1/CRPA-300A, Appendix II to SS-GAS1-300A, 24 Apr 1998.

[2] 'Test Results of a High Gain Advanced GPS Receiver,' Alison Brown and Gengsheng Zhang, ION 55th Annual Meeting.