Implementation and testing of a sensor-netting algorithm for early warning and high confidence C/B threat detection

Thomas Gruber\textsuperscript{a}, Ryan Fauth\textsuperscript{a}, Brian Tercha\textsuperscript{a}, Chris Powell\textsuperscript{a}, Kristin Steinhardt\textsuperscript{a}
\textsuperscript{a}MESH, Inc., 114 Barnsley Road, Oxford, PA USA 19363

ABSTRACT

Large networks of disparate chemical/biological (C/B) sensors, MET sensors, and intelligence, surveillance, and reconnaissance (ISR) sensors reporting to various command/display locations can lead to conflicting threat information, questions of alarm confidence, and a confused situational awareness. Sensor netting algorithms (SNA) are being developed to resolve these conflicts and to report high confidence consensus threat map data products on a common operating picture (COP) display. A data fusion algorithm design was completed in a Phase I SBIR effort and development continues in the Phase II SBIR effort. The initial implementation and testing of the algorithm has produced some performance results. The algorithm accepts point and/or standoff sensor data, and event detection data (e.g., the location of an explosion) from various ISR sensors (e.g., acoustic, infrared cameras, etc.). These input data are preprocessed to assign estimated uncertainty to each incoming piece of data. The data are then sent to a weighted tomography process to obtain a consensus threat map, including estimated threat concentration level uncertainty. The threat map is then tested for consistency and the overall confidence for the map result is estimated. The map and confidence results are displayed on a COP. The benefits of a modular implementation of the algorithm and comparisons of fused/un-fused data results will be presented. The metrics for judging the sensor-netting algorithm performance are warning time, threat map accuracy (as compared to ground truth), false alarm rate, and false alarm rate v. reported threat confidence level.

Keywords: sensor, netting, algorithm, fusion, tomography, map, uncertainty, consistency

1. INTRODUCTION

Large networks of disparate chemical/biological (C/B) sensors, MET sensors, and intelligence, surveillance, and reconnaissance (ISR) sensors reporting to various command/display locations can lead to conflicting threat information, questions of alarm confidence, and a confused situational awareness. A "sensor netting algorithm" (SNA) to do the following tasks was designed (i.e., process and mathematical approach) and initially developed during a phase I SBIR, as reported last year:\textsuperscript{1}

\begin{itemize}
  \item Ingest both standoff sensor (path integrated, line-of-sight measurements) data and point sensor (measurements at one location in space) data, as well as other non-traditional sensors (e.g., acoustic, terrain, MET, etc. type data), within one data fusion algorithm process in order to obtain high confidence threat detection results
  \item Resolve conflicting sensor data by detecting and rejecting erroneous (e.g., noisy, false alarming) sensor data
  \item Achieve higher confidence threat results than individual sensors (i.e., the un-fused data) within the network
  \item Provide a succinct and timely visualization of threat maps on a common operating picture (COP) display
\end{itemize}

Progress has been made in implementing and refining the SNA and in performing simulation based testing during phase II of the SBIR effort. This paper presents a comparison of "un-fused" and "fused" threat map results for a selected simulation scenario. An overview of the SNA design is provided in Section 2, followed by a description of the selected simulation scenario in Section 3, and then an explanation of the performance metrics used in evaluating the threat map results in section 4. The simulation results are then presented and discussed in Section 5.

2. SENSOR NETTING ALGORITHM DESIGN OVERVIEW

There are three key components to the SNA:
- Preprocessing Component - input data preprocessing to characterize noise and bias errors, assign uncertainty to all measurements, and detect/reject erroneous sensor data
- Tomography Component - threat map calculation via a tomography data fusion process which accepts both point and standoff data, adjusts sensor data for measurement age/MET conditions (i.e., a method of time correlation), and determines the threat level result, i.e., above or below immediate danger to life and health (IDLH) concentration levels
- Result Consistency Component - threat map post processing for checking sensor to threat consistency (with feedback to the input preprocessing), producing COP data products, and cueing of follow-on assets

These SNA components, related COP result displays, and threat / sensor models required for the simulation are shown in the system diagram of Figure 1. Simulated data are produced when sensor models report their position, and line-of-sight (LOS) direction for standoff sensors, to the threat model, which returns the calculated sensor response by reading a simulated cloud concentration data file (and integrating along the LOS as required for standoff sensors). The sensor models then add noise to the response via user chosen parameters for a Markov process. These signal + noise sensor results are then sent over a TCP/IP connection to the SNA "preprocessing component". Data then flows from the sensor data preprocessing to the map calculating "tomography component", and then to the "result consistency component" for confidence checks and sensor cueing. Fused and un-fused map results are generated by the SNA for display on COPs.

Each of these key components is described in more detail in the sub-sections that follow. Note that the standoff sensors and point sensors are assumed to be quantitative sensors with "raw signal taps" that allow for real time characterization and monitoring of the sensor noise.

Figure 1. Sensor netting algorithm design block diagram showing major components and data flows. The threat model and sensor models, which are external to SNA, are also shown.

2.1 Preprocessing of the Input Sensor Data Streams

The input data preprocessing GUI is shown in Figure 2. This display consists of a table of sensors and a raw signal graph for a selected sensor. The table lists the sensor IP address, connection status, sensor type, data rate, characterized noise
level, individual sensor noise to population noise ratio for that specific type of sensor, and sensor health status. The graph allows for a comparison of the signal with noise v. the noise only after a highpass filter has been applied.

The preprocessing component handles sensor connections by listening on user specified TCP/IP addresses and ports, which can be configured ahead of time or during runtime. Sensor data can come from either simulated sensor models or live sensor feeds. To emulate a real world environment, the preprocessing component is capable of handling sensors connecting and disconnecting from the system at any time. Sensor data buffers are maintained during short network drops to handle instances of network malfunctions.

Individual sensor alarms are sorted into events as they arrive in the preprocessing component. Alarms are sorted into different events by agent class of the alarm and the location of the sensor (for point sensor data). If a sensor is too far away to physically detect or "see" a current event that is already being tracked, then a new event is declared and tracked.

One of the jobs of the preprocessing component is to determine each sensor's noise estimate, and this requires a removal of any real signal trend (i.e., measured response to a real threat cloud). A sample standoff sensor response with noise is shown in Figure 3, and this same sensor noise is shown in Figure 4 after the Fourier transform based highpass filter has been applied. Note that the signal is clamped at zero (i.e., signal > 0), as shown in Figure 3, and this is why the noise only appears to be positive and negative wherever the signal is non-zero, as shown in various sections of the noise curve in Figure 4. Therefore, the best noise characterization occurs where the signal is non-zero.

A moving window that spans 120 seconds worth of the most recent data for each sensor is used to characterize the noise level every second. The noise levels of all sensors of given type are then averaged together to characterize each population of sensors. Whenever a sensor's noise is greater than some factor (e.g., 3 or 5) times the population noise, the sensor is rejected as defective. A sensor is also rejected whenever a health/status message reports a fault. All sensor data that passes noise and health/status checks is forwarded to the map calculating tomography component.

Figure 2. SNA sensor preprocessing component display showing a list of connected sensors.
2.2 Spatial and Temporal Correlation of Sensor Data with Tomography to Create Threat Maps

The tomography mapping component of SNA is a modified algebraic reconstruction technique (ART) tomography process\(^1\), called Sensor Amalgamation Mapping by MESH, Inc. (SAMMI). Tomography is the process of converting sets of path integrated measurements (e.g., path integrated concentration or "CL" vectors) into maps of some property as a function of location (e.g., concentration). The tomography is operated in a 2D mode and is used to spatially and temporally correlate the various input sensor data to produce the consensus threat maps depending on the number of unique events that are being tracked. SAMMI for SNA is operated at a low spatial resolution (e.g., 50m size voxels) due to an expected low spatial density of sensors.

SAMMI tomography is designed to work with both point and standoff sensor data. First the point sensor data is converted to a path integrated concentration. A point sensor measures the concentration for a strip of air during its measurement integration time. This strip of air has a direction (i.e., wind direction) and a length (i.e., wind velocity multiplied by the sensor integration time). This “strip” concentration multiplied by the length is a CL vector, which is the same type of measurement that standoff sensors make. By converting point sensor data to CL vectors, we have provided a means for correlating and fusing point and standoff data within the same process (i.e., tomography).

There are two different limitations to standoff and point sensor data that surprisingly can be mitigated with the same adjustment technique. Often standoff sensors cannot instantaneously measure their field of regard (FOR) due to a limited

---

**Figure 3.** Example standoff sensor input data stream comprised of signal and noise in path integrated units. The noise is created by the sensor model using a Markov process.

**Figure 4.** Example standoff sensor noise after high pass filtering to remove the signal. This noise data set can now be used to characterize the sensor noise using a standard deviation calculation.
FOV and the need to raster scan a wide FOR. This means that when maps are calculated, some portion of standoff sensor data may be relatively old (e.g., 30, 90, or 120 seconds old), which can lead to distorted threat map results since the air is moving during this time. Usually point sensors have a limited sampling domain of only their immediate location. SAMMI takes the recent collection (i.e., a chosen moving window through time) of point and standoff vector measurements and translates them to their approximately correct location at the time of the map calculation, based on each CL vector measurement age and the average wind velocity during that age time. The age is the map calculation time (e.g., now or a time value in the near future) minus the measurement time. This translation process reduces standoff distortion and it allows point sensors to influence a larger domain by translating the recent point sensor measurements downwind. The limits of how wide a window in time (e.g., how much translation is possible) are to be determined.

Several strategies are used to improve the quality of tomography results including:

- Requiring that at least 3 different sensors agree that a threat is present in each voxel - this reduces false alarms because a single false alarming sensor cannot produce a threat map result
- Use of terrain data to limit the sensor LOS (e.g., when LOS hits the ground or a mountain range) and to constrain the threat map solution to be above ground

The terrain data are obtained from a "global terrain elevation database" that was produced during the "NASA Shuttle Radar Topography Mission", which collected global elevation data at high spatial resolution. Terrain data for a particular region of interest are loaded into memory as a series of elevation readings at GPS coordinates on a grid. These data are then used in two ways. The first affects the measurements of all sensors equally and limits the map calculation result of each voxel to be above ground. The second use of terrain data is to limit an individual standoff sensor LOS, as shown in Figure 5, which effects the tomography projection matrix calculation (which controls which voxels are influenced by a particular CL vector measurement). The terrain feature function can also be used to load information about manmade objects (e.g., tall buildings) that block sensor line of sights. This information is also useful in making sensors cueing decisions.

![Figure 5](image-url)  
Figure 5. Terrain data from a NASA database are used to limit standoff sensor LOS and to constrain the tomography map solution to be above ground level. The concept of limiting a sensor’s LOS is shown. For this case, the sensor’s LOS is limited to only those voxels that are not grey.

### 2.3 Post Processing of the Threat Map and Sensor Data to Obtain Confidence Levels and to Cue Sensors

The result consistency component has several functions including:

- Determine map result confidence - provide a measure of confidence with all SNA results (SNA results should have higher confidence than the results from individual sensors)
- Check for covariance consistency between each sensor input data streams and the resulting threat map
- Cue sensors based on ISR sensor information or the need for an "orthogonal technology" confirmation of the threat map

A qualitative check list approach, as shown in the display of Figure 6, was developed to provide the user with an easy to understand confidence metric:

- Covariance consistency - the covariance between the majority of reporting sensors data streams and the current threat map result indicates consistency. Covariance consistency is the same as the "Pearson's r" correlation test.
• Threat persistence - the existence of the threat persisted long enough to be significant (e.g. beyond a time threshold)
• ISR event at threat location - an Intelligence, Surveillance, or Reconnaissance (ISR) sensor has alarmed in the same region
• Orthogonal technologies - C/B alarms are occurring from different types of sensing technologies
• Multi-location, multi-sensor alarms - more than one C/B sensor is alarming in multiple locations
• Sensor Alarms - at least one C/B sensor is currently alarming

![Figure 6. Threat confidence display. Highlighted rows indicate that a particular confidence condition is met for the current threat map result.](image)

2.4 Fused and Un-fused COP Result Displays

SNA produces a fused and un-fused COP display by writing out KML files that can be viewed using Google Earth. The un-fused COP display shows the raw sensor data alarms as they arrive. The color of the C/B point sensor icons indicate whether the sensor is in alarm. Alarm areas for C/B standoff sensors are indicated using the azimuth and elevation alarm extents to shade a sector of the map where the sensor has alarmed within its FOR.

The SNA result COP display indicates the area on the map where the threat level is above immediate IDLH levels, as shown in results section Figure 11. This fused COP display is the combination of the most recent data from all sensors.

2.5 Modular Design Implementation to Facilitate Integration with other Data Fusion and Network Systems

The SNA uses a modular design with each component residing as a separate application. Communication between the SNA components is performed via TCP connections, making the system capable of running on separate machines to distribute system load across multiple processors. This approach allows the SNA to be integrated into other testbeds or run alongside other fusion engines with minimal modification.

3. SIMULATION TEST SCENARIOS

Even though the SNA is not fully developed, three basic simulation tests were performed using some or all of the SNA components / features to show some preliminary results. These simulations were:

• Test rejection of a sensor from its population based on detection of excessive noise - an operator connected 6 standoff sensor models to the preprocessing component, and turned up the sensor model noise level on one of the sensors at a selected time
• Test initial warning time with and without sensor cueing - a simulated ISR event (i.e., acoustic sensor detection) was either ignored or used to cue nearby standoff sensors to turn towards the event. The ISR event corresponded to the formation of a simulated nerve cloud.
• Compare un-fused v. fused map results over a period of time - a simulated nerve cloud was created and monitored by the network of sensors. An ISR event was used to initially cue standoff sensors for this scenario.

The scenario for "compare un-fused v. fused map results over a period of time" includes the specifications shown in Table 1 and the following sequential events:
1. A network of simulated sensors is brought on-line and connected to the SNA system. The standoff sensor data is passed to the tomography component.
2. A simulated nerve agent cloud originates at 2km off of a base starting with an explosion. The wind is blowing 5 m/s to the east.
3. A simulated ISR acoustic sensor detects this explosion location.
4. SNA cues standoff sensors to look towards the ISR event location.
5. Standoff sensors start alarming and point sensors alarm when the cloud comes in contact with them.
6. SNA produces map results with a confidence metric. The un-fused maps are also produced for comparison.
7. SNA fused results indicate accurate threat size and location.

A sample of simulated standoff sensor data for this scenario is shown in Figure 7. This data was taken from the tomography log file for one of the map calculations created during the simulation, as discussed in Section 5.

Table 1. Simulation scenario specifications for the sensor network and threat cloud for un-fused v. fused data test.

<table>
<thead>
<tr>
<th>Number of Sensors in the Network</th>
<th>Chemical Standoff Sensors: 4</th>
<th>Chemical Point Sensors: 4</th>
<th>ISR Acoustic Sensors: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standoff Sensor Specifications</td>
<td>Data Rate: 20 Hz</td>
<td>iFOV: 0.50°</td>
<td>Field of Regard (azimuth x elevation): 90° x 4°</td>
</tr>
<tr>
<td></td>
<td>Noise level: 0 mg/m²</td>
<td>Point Sensor Specifications</td>
<td>Data Rate: 0.5 Hz</td>
</tr>
<tr>
<td>Threat Cloud Specifications</td>
<td>Chemical Class: Nerve</td>
<td>Threat Origin: 2000 m west of base at ground level</td>
<td>Radius: 200 m</td>
</tr>
<tr>
<td></td>
<td>Concentration Profile (from center): Cosine (northing, easting), Constant (altitude)</td>
<td>MET Specifications</td>
<td>Wind Speed: 5 m/s</td>
</tr>
</tbody>
</table>

Figure 7. Sample standoff sensor input data v. time for raster scans across the simulated threat cloud. The time is the "sensor measurement age" relative to the map calculation time (i.e., map time minus sensor measurement time).
4. PERFORMANCE METRICS

Prior to data fusion algorithms such as the SNA described here, sensor alarms (or NBC reports created from these alarms) were simply plotted on a map without an algorithm to combine the data from the various sensors. In order to compare un-fused and fused results, several metrics were developed as described below. For some of these metrics, the un-fused and fused results cannot be compared, and instead the metrics are used to judge SNA performance relative to SNA parameter choices.

4.1 Early Warning Time

Time of first warning relative to the event starting time with and without cueing can be compared. The use of ISR information to cue standoff sensors is expected to result in earlier warning time.

4.2 Result Confidence v. Time

As data arrives and is analyzed by the data fusion SNA, the measure of confidence in the fusion result can increase over time. The level of confidence in the fusion result will be compared to the un-fused data as seen without the SNA process. The confidence level cannot be judged for the un-fused map.

4.3 Threat Location and Size v. Ground Truth

The centroid error and cloud overall size error will be compared to the correct answer as a function of time. The un-fused map cannot provide a centroid and will probably always over report the threat size since the passive standoff sensors cannot report range (e.g., only an angular section of the FOR can be identified as having alarms).

4.4 IDLH Levels of Fusion Result vs Ground Truth

The percentage of threat cloud area that is correctly identified as "above IDLH" will be determined as a function of time. This metric can only be determined for the SNA fused map result.

5. RESULTS

The SNA test results for each of the scenarios discussed in Section 3 are evaluated using the metrics from section 4.

5.1 Rejection of a Noisy Sensor

When a sensor exceeds the preset sensor noise to population noise ratio threshold, the sensor is rejected from further SNA processing. Sensor data from the rejected sensor is still received and processed by the preprocessing component; however, the data is not forwarded on to the tomography component if the sensor is considered too noisy. This is because the sensor’s noise may distort the threat map if other sensors have real alarms. Figure 9 shows a noisy sensor being rejected by the preprocessing component within ~1min of the operator setting the sensor model to higher noise level.
5.2 Warning Time with and without Sensor Cueing

The SNA result consistency component provides earlier detection of events by cueing the sensors to scan areas that may not normally be covered (or covered at a particular moment in time). The example in Figure 10 shows SNA redirecting standoff chemical sensors to scan the area where an acoustic sensor has just detected an explosion event. This cueing enables the standoff sensors to detect a cloud and alarm earlier than if not cued. Tables 2 and 3 show the results with and without cueing for the simulated scenario. The event timelines show that the difference in initial alarm time is over 1 minute earlier than when cueing is not used.
Table 2. Event timeline when using SNA sensor cueing based on ISR data.

<table>
<thead>
<tr>
<th>Time (min:sec)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:00</td>
<td>Acoustic Sensor Detects Explosion Event 2km from FOB perimeter</td>
</tr>
<tr>
<td>0:01</td>
<td>Standoff Chemical Sensors Cued to scan area of Explosion Event</td>
</tr>
<tr>
<td>0:03</td>
<td>1st Standoff Sensor Detects Nerve Agent</td>
</tr>
<tr>
<td>3:08</td>
<td>Leading Edge of Nerve Agent cloud crosses FOB perimeter</td>
</tr>
</tbody>
</table>

Table 3. Event timeline without SNA cueing. First sensor alarm does not occur until elapsed time 1:46.

<table>
<thead>
<tr>
<th>Time (min:sec)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:00</td>
<td>Acoustic Sensor Detects Explosion Event 2km from FOB perimeter</td>
</tr>
<tr>
<td>1:46</td>
<td>1st Standoff Sensor Detects Nerve Agent</td>
</tr>
<tr>
<td>3:08</td>
<td>Leading Edge of Nerve Agent cloud crosses FOB perimeter</td>
</tr>
</tbody>
</table>

5.3 Un-Fused v. Fused Map Sequence Performance

The un-fused and SNA fused Google Earth based map COP displays for the scenario described in Table 1 are shown in Figure 11. The series of maps shows the cloud as it moves across a military base area of interest.

The un-fused data maps show the point sensors (square icons) alarming as the cloud moves over them (as indicated the square icon changing from green to red). The alarm area of each standoff sensor (circle icons) is seen over the min and max azimuth extents (as indicated by a red wedge). When alarms from multiple sensors are occurring, many overlapping areas of alarm are observed, making it difficult to discern by eye where the real threat is located, as seen in results section Figure 11. The exact size and shape of threat cannot be determined in the un-fused maps.

The fused data maps show the result of the SNA as a set of 50 meter square voxels. Red indicates areas where the chemical concentration is above IDLH. The fused maps clearly show the location of the cloud as it moves across the base. The fused data confidence v. time is shown in Tables 4 and 5. The confidence increases with time as more conditions are met. Table 6 provides a comparison of the SNA map results v. the true answer for this preliminary simulated scenario, including:

- Centroid location error (lower number is better) - the centroid is usually within 1 voxel off the correct location
- Size error (lower number is better) - the first map has large error but then the error drops
- IDLH area correctly identified (higher number is better) - typically 80% of the IDLH area is correctly identified
- Concentration errors (lower numbers are better) - two different methods of reporting concentration error as a percentage are given. Typically the concentration error is ~20% for this scenario.

The threat cloud size is also visualized for a selected map in Figures 12 (un-fused) and Figure 13 (fused). Note that the size and shape of the SNA result cloud are within ~1 or 2 voxels of being correct (i.e., 50 to 100m in error) as compared to the un-fused map, where an area much larger than the true cloud is indicated.

The covariance consistency test (also called "Pearson's r") is used to check the consistency of each sensor's input data stream (i.e., CL data) against the consensus threat map answer (i.e., back projected "output" CL data). The covariance consistency values for the map results are shown in Table 7, and all values above 0.5 are shaded gray. We are still working to understand reasons for occasional bad values, and we need to determine if the covariance test will still work with noisy sensor data. The goal is to produce a histogram of covariance consistency for all sensors and then determine if most sensors are or are not consistent with each threat map result.
Table 4. SNA confidence level major changes during the simulation timeline.

<table>
<thead>
<tr>
<th>Event Timeline</th>
<th>00:00</th>
<th>00:01</th>
<th>00:03</th>
<th>00:20</th>
<th>03:08</th>
<th>05:28</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR Event</td>
<td>Sensors Cued</td>
<td>First Standoff Sensor Alarm</td>
<td>Multiple Standoff Sensors Alarm</td>
<td>Cloud Reaches FOB perimeter</td>
<td>Point Sensor Alarms</td>
<td></td>
</tr>
<tr>
<td>Confidence Level</td>
<td>Orthogonal Technologies</td>
<td>Persistence of Threat</td>
<td>Multi-Location Alarms</td>
<td>Sensor Alarms</td>
<td>ISR Event</td>
<td></td>
</tr>
</tbody>
</table>

Table 5. Confidence level reported and corresponding simulation event.

<table>
<thead>
<tr>
<th>SNA Confidence Measurement</th>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR event detected</td>
<td>0:00</td>
<td>Acoustic sensor detects explosion event 2km from base perimeter</td>
</tr>
<tr>
<td>Sensor alarms</td>
<td>0:03</td>
<td>The first standoff chemical sensor alarm is received</td>
</tr>
<tr>
<td>Multi-Location Alarms</td>
<td>0:20</td>
<td>Chemical alarms are received from sensors in other locations</td>
</tr>
<tr>
<td>Persistence of Threat</td>
<td>2:03</td>
<td>Chemical alarms have been received for the past 120 seconds</td>
</tr>
<tr>
<td>Orthogonal Technologies</td>
<td>5:28</td>
<td>First chemical point sensor alarm</td>
</tr>
</tbody>
</table>

Table 6. SNA fused map results v. threat cloud "ground truth" as a function of time.

<table>
<thead>
<tr>
<th>Threat Cloud &quot;Ground Truth&quot;</th>
<th>SNA Fused Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centroid</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Northing [m]</td>
<td>Easting [m]</td>
</tr>
<tr>
<td>Map #</td>
<td>Elapsed Time [mm:ss]</td>
</tr>
<tr>
<td>2</td>
<td>04:28</td>
</tr>
<tr>
<td>5</td>
<td>04:58</td>
</tr>
<tr>
<td>8</td>
<td>05:28</td>
</tr>
<tr>
<td>11</td>
<td>05:59</td>
</tr>
<tr>
<td>14</td>
<td>06:29</td>
</tr>
</tbody>
</table>
Figure 11. Un-fused (left) and fused (right) Google Earth based COP map sequence results comparison.
Figure 12. Un-fused map result display and truth cloud location comparison at elapsed time 5:28.

Figure 13. SNA fused map result display and truth cloud location comparison at elapsed time 5:08.
6. CONCLUSIONS

Preliminary simulation testing results for a partially completed SNA have been presented. The SNA fused threat map results show promising performance as compared to un-fused maps:

- Result confidence v. time – in the limited simulation work done so far, the checklist based confidence does increase as expected over the duration of an event.
- Fused map v. un-fused map - the fused map results are clearly more specific in identifying the threat location. The un-fused maps cannot identify the IDLH area.
- Threat size, location, and IDLH indication – the preliminary results indicate that it is possible for the low resolution tomography based data fusion to make accurate maps (~80% correct identification of IDLH). The next steps will be to determine if this performance can be maintained with noisy sensors and more realistic cloud shapes / concentration profiles.

Simulation based testing/refinement of the SNA and processing of some real data sets will occur during the remaining 16 months of our phase II SBIR effort.

ACKNOWLEDGEMENTS

This work was supported under the SBIR topic “CBD09-110 CNRN Sensor and Sensor Netting Algorithms” via phase II contract #W911SR-10-C-0034. The authors wish to acknowledge the helpful technical discussions with Christopher Keiser and William Ginley of the U.S. Army ECBC, and Steve Waugh of DTRA.

REFERENCES