Data Association and Graph Analytical Processing of Hard and Soft Intelligence Data

Ketan Date, Geoff A. Gross, Sushant Khopkar, Rakesh Nagi, Kedar Sambhoos
Center for Multisource Information Fusion
State University of New York at Buffalo
Buffalo, New York, U.S.A.
ketandat@buffalo.edu, gagross@buffalo.edu, skhopkar@buffalo.edu, nagi@buffalo.edu, sambhoos@cubrc.org

Abstract—In traditional data fusion hard physical sensor data has been the main source of information. This has changed during the past decade, under the backdrop of counter insurgency (COIN). In the COIN environment the majority of information comes from human sources (soft data). The source of this information can be human informants or soldiers conducting reconnaissance in the field. This human sourced soft data is filled with vast amounts of valuable information. Recently a large number of Natural Language Processing techniques have been developed to process this soft data into the form of relational graphs. In this paper we have described various graph analytical techniques that can be applied towards fusion of hard and soft information and understanding the situations of interest by an analyst. The processing elements exhibited in this paper are association of entities and relations in observational hard and soft data graphs to form the cumulative data graph, situation assessment via graph matching of situations of interest against the cumulative data graph, and social network analysis to identify and extract high value individuals in the network. To illustrate these graph analytic tools we have used the Sunni message thread of SYNCOIN consisting of 114 soft messages and 4 hard data reports. The value of this work has been demonstrated with detailed analysis and examples from the aforementioned dataset.

Keywords — hard and soft data fusion, information fusion, fusion architecture

I. INTRODUCTION

Insurgencies and the methods of Counter-Insurgency (“COIN”) [1] operations are extraordinarily complex environments to deal with and even to define. The Research Problem Domain [2] is considered to be the problem of Small-scale COIN insurgency. In Small-scale insurgencies, belligerent groups have established some size, are developing tactics, techniques and procedures, and are causing hostile and possibly lethal events. These groups however are still quite covert and operate very carefully; their leadership and organizational structures and their insurgency-related goals and objectives are still not well understood. Considering the Small-scale COIN problem, the requirements for Information Fusion (IF) are to estimate and identify the “essential elements of information (EEIs)” for this sub-problem space of COIN, in support of corresponding military or other possible courses of action.

We have chosen a deductive or model-based and inductive or learning/discovery-based approach regarding the development of insights for a dynamic COIN problem. Modern literature shows that the ability to effectively model human group dynamics and relationships remains a very challenging problem and that only very limited capability exists. In particular for the Soft Data Fusion problem, we have chosen graph-based methods as an inferencing framework, wherein the soft data are associated and compiled into an evolving, accumulating “Cumulative Data Graph” representing accumulated situational evidence. Using this Cumulative Data Graph and analyst formed queries that can also be represented as graphs (“Target or Template Graphs”) and graph matching algorithms are applied to yield inferred assertions. Further, social network analysis tools supporting an adaptive analyst learning process are applied. The operational focus here is on human social network type inquiries.

This research paper focuses on the intelligence analysis domain of COIN [1]. The COIN domain spans multiple operations including defensive and stabilizing operations to provide services for economic and social development. In this domain data can come for multiple sources, hard data coming from physical sensors deployed in the field to track and ID targets (people, vehicles, etc.) and soft data from human sources such as soldiers. This information is collected in response to priority information requirements (PIRs). PIRs are generated by analysts to answer the Information requirements (IRs) provided to them by the commander. The analyst needs to understand the IRs and to fulfill them based on the current observed data. The data at hand is analyzed by the analyst and s/he makes a decision to fulfill the missing data. In the current data intensive environment the most challenging part is to separate relevant information from the noise. Due to cognitive and temporal limitations the analyst cannot consume all of this data. To extract the relevant information from this vast amount of data the intelligence analyst has to incorporate automated methodologies. The processing elements [3] of our graph analytic engine: graph association, graph matching and social network analysis comprise the automated methodologies that will aid an analyst in responding to IRs.

In the Fusion architecture [2] designed for this program we are fusing the hard sensor data with soft data at the data association level. This decision is made with the interest of
“early” fusion, and is premised on the availability of hard and soft graphical data. The soft textual data needs to be processed using Natural language processing tools like Tractor [4] to convert text into graphical data before association can be performed. The research contribution and merit of each of the fusion system processing elements of data/graph association, graph matching and social network analysis, have been demonstrated with the help of the Sunni criminal thread (SUN) of SYNCOIN developed by Graham et al. [5] which is described in Section III.

The remainder of this paper is organized as follows: Section II provides an overview of the fusion processing architecture, Section III discusses the example scenario used to demonstrate the graph analytic techniques, Section IV describes the data/graph association process, Section V illustrates the graph matching process, Section VI presents the social network analysis while Section VII presents conclusions and plans for future work. Each section utilizes examples from the Sunni criminal thread to demonstrate important concepts within that section’s processing elements.

II. FUSION ARCHITECTURE OVERVIEW

The architecture designed for the joint fusion of the hard and soft data is presented in Gross et al. [6]. The process starts with COIN data generated by Graham et al. [5]. This COIN data is described in Section III. The overall SYNCOIN dataset consists of 595 plain text reports from soft data sources. In addition to that there are raw sensor reports for the hard processing stream. The focus of this paper is on the soft processing stream although hard data is also integrated in our analysis. Details of the fusion algorithms utilized to produce the hard data tracks are omitted here. The soft plain text reports are processed using the natural language processing (NLP) tool, Tractor [4]. Tractor is responsible for parsing, recognizing and coreferencing entities within messages, mapping syntactic data to semantics information and contextual enhancement to produce an ontologically enhanced propositional graph. These propositional graphs are directed graphs where entities, relationships, locations and events are represented as nodes connected by edges as propositions.

These propositional graphs are then converted to attributed graphs. In attributed graphs, entities, locations and objects are represented as nodes while relationships between entities are represented as edges. Events are represented using a group of nodes (entities involved, objects used) and edges. Finer grained information like age, height, weight of a person are represented as attributes. Attributes are the finest grain level of observable information within the attributed graph. In addition to this information most of the nodes and edges have additional information to identify their type (person, location, group, etc.). This type information is derived from an ontology during the natural language processing step. The type information provides a computational advantage while processing these nodes during the graph analytics tasks of scoring, data association, social network analysis and graph matching.

After the graph conversion, these messages pass through the data association step where the entities are merged to form unique nodes that span (or are mentioned/described in) multiple messages. The result of the data association is a cumulative data graph which forms the input for graph matching and social network analysis.

The next step in the architecture is scoring for data association. The soft data which is represented as attributed graphs is merged by comparing the attributes of the nodes like entity type, age, weight, height, etc. Hard information is also included in the scoring process. The data association process merges the highly scored entities to form a cumulative data graph. This cumulative data graph would ideally have a single node for a person mentioned across messages with relationships from multiple messages. The common attributes of graph elements are fused during this process.

The cumulative data graph from data association is passed to further graph analytic processes of graph matching and social network analysis. The graph matching algorithm takes the situation of interest created by an analyst and matches it against the cumulative data graph. The graph matching algorithm follows an inexact approach towards graph matching. The graph matching algorithm generates completely or partially matched alerts. The social network analysis algorithm extracts the people network from the cumulative data graph and calculates centrality metrics to identify high value individuals. The extracted network along with centrality values is displayed to the analyst for interpretation and further analysis.

III. EXAMPLE SCENARIO

Under the MURI research program [2], a synthetic COIN inspired data set (SYNCOIN) [5] was developed to support the test and evaluation of emerging hard and soft data fusion algorithms and techniques. The data includes 595 messages (“soft data”) and synthetic complimentary simulated physical sensor data (“hard data”). The scenarios cover a four month period between 1st January, 2010 and 10th May, 2010; centered in Baghdad, Iraq. The central theme throughout the dataset involves Improvised Explosive Device (IED) operations and associated networks. There are several stories and sub-stories that have been interlaced throughout the message set. These stories are about people, their plans, and the timeline towards fulfilling their intended IED related activities.

The data set involves six threads of parallel activity including; a bio-weapons thread, a Bath’est resurgence thread, an Iranian Special Group thread, a sectarian conflict thread, a Sunni criminal thread (SUN) and a Rashid IED Cell thread. In this paper we are concentrating on the Sunni criminal thread. This thread contains 114 messages consisting of both soft and hard reports.

These SYNCOIN messages are front line reports from soldiers’ and information gathered by soldiers from informants in response to Priority Information Requests (PIRs). These messages are very short as exemplified by the message shown in the following:
54. 01/25/10 - Iraqi Domestic Counter-Intelligence

passed the names of six prominent Sunni criminal leaders operating in Rashid to Coalition Forces. This group controls most of the criminal activity across Rashid — little happens without their knowledge. They have been known to cross sectarian boundaries when they can turn a profit.

They have both Shi'a and Assyrians on the payroll.

In the SUN thread, Dhanun Mahmoud Ahmad Mahmoud (DAM) and Abdul Jabar Wahied are arrested at two different locations, East Dora and Abu T'Shir respectively. DAM is a Sunni Munitions trafficker working for Rashid Criminal Group, while Abdul Jabar Wahied is an Iranian Special Group (ISG) affiliate which he denies and expresses himself as an independent contractor. They both deny any associations with one another. Abdul Jabar Wahied provided information on his dealings between the Rashid Criminal Group and the Iranian Special Group during interrogation in exchange for his repatriation. Immediately after that DAM starts to cooperate as he fears the Shia dominated Iraqi National Police (INP). DAM is interrogated in an attempt to identify other members of the group’s leadership. At first he claims no connection but eventually relents and provides names of other leaders.

An un-coordinated raid by INP infuriates Brigade Combat Team (BCT) forces and there is some prevailing tension between them. In other intelligence gathering it has been found that DAM has been identified as the key link between the Sunni Criminal Group and the Iranian supported IED logistics network. In multiple movements of DAM, he ends up with INP in Karkh. Here he is freed after an early morning raid and gun battle. The raid indicated use of a Vehicle Borne Improvised Explosive Device (VBIED) which was detonated at the rear of the police building along with the use of hand grenades. DAM was injured during this attack and was treated by nearby doctor’s office assistant at gunpoint. The breakout is an attempt to provide DAM cover since he has been converted to an informant. DAM’s mission is to gather more information on the Rashid Criminal Group’s activities.

DAM is asked to re-create his network and do small transfer tasks to determine his loyalty. DAM sets out to the Iranian border with another unidentified individual to pick up IED components. The GPS device fitted to DAM's car eventually loses contact and it is unclear if he obtains these components. Upon returning DAM alerts his handlers his duties have been downgraded to low level purchasing duties as the leadership of the Rashid Criminal Group has become skeptical of his loyalty. DAM provides information on a mortar purchase which he will make. A raid is performed by INP officers at the location of the purchase, the day before DAM reported the purchase was supposed to take place. DAM is arrested in the raid but eventually transferred to a U.S. holding facility in Karkh. In the interrogation following arrest he reveals the name of Lufti Dilawar. DAM is released, provided a new car and told to claim he was hiding out with family as he tries to renew contact with Rashid Criminal Group leadership. The leaders are skeptical of his allegiance and take his car from him. Communication to

"replace a supplier" is intercepted from Lufti Dilawar cell phone. The next day Dhanun Ahmad who is ready to leave Rashid is attacked with VBIED where he and his family fail to survive. The VBIED was determined to contain both Iranian and U.S. components.

BCT forces that are monitoring a safe house in Dora, see new arrivals. From the updated intelligence information it is confirmed that INP and Iraqi National Guard (ING) have been infiltrated by terrorists. The public communicates concerns of Iraqi National Guard (ING) and Iraqi National Police (INP) officers returning at night in plainclothes in “Shi'a death squads”. Intelligence forces from BCT have started monitoring all calls originating from INP and ING. It is also confirmed that Lufti Dilawar is one of the persons who arrived at the safe house in Dora. In one of the raids by BCT forces Lufti Dilawar is arrested along with nineteen others. BCT forces capture a mix of 25-30 INP and ING members during the raid in Dora. Lufti Dilawar's biometric data found to match that of the VBIED biometric data and also chemical weapon biometric data.

IV. DATA ASSOCIATION

A. Introduction

The data obtained from the real world contain references to entities and their relationships and describe the various attributes of each. Many times these references are duplicated in that multiple references represent the same real world entity. There are many causes of duplicate mentions, such as additions to the data over time, typographical errors or multiple data entries. Presence of these duplicate references could limit the efficient use of the data and can cause several problems like incorrect information retrieval, wasted storage space etc. The goal of data association task is to identify the references which correspond to the same real world entity and merge them into fused (cumulative) evidence. This cumulative evidence will contain more information about the real world entities than offered by any single observation and it can be used to build hypotheses or draw conclusions on the current state of the real world.

To serve the needs of data association, each data set can be represented as a relational, attributed graph. By doing this, the data association problem can be modeled as a graph association problem, which in turn is closely related to a multi-dimensional assignment problem. Tauer et al. [7] studied various mathematical formulations for the data association problem and proved that it is in fact an NP-hard problem. The authors developed a Lagrangian heuristic for solving the data association problem for N graphs (GA\(N\)), which obtains the best solution in an iterative fashion until a provably optimal solution is found or a pre-determined optimality gap is achieved. In their later work, Tauer et al. [8] studied a relaxed version of the data association problem in which the edges between the nodes are not required to be associated. This problem is known as multi-dimensional assignment problem with decomposable costs (MDADC) and it is somewhat easier to solve than GA\(N\) due to the absence of the complicating edge association constraints. The authors developed a parallel version of the Lagrangian
heuristic and implemented it using the Map/Reduce programming architecture, so that large problems can be solved efficiently using the power of distributed computing. Since MDADC formulation does not have any edge association constraints, its accuracy for entity (node) association is suspected to be worse than the GA\textsuperscript{N} formulation.

B. Computational Experiments

We performed a computational comparison of the sequential Lagrangian heuristic for GA\textsuperscript{N} and the Map/Reduce Lagrangian heuristic for MDADC, in terms of their accuracy and computing time. Both the procedures are coded in Java and executed on Intel Core 2 Duo processor, with 3 GHz clock speed and 4GB RAM. The experiments were performed on the 115 messages from the Sunni criminal thread of the SYNCOIN dataset. The text messages are converted into relational, attributed graphs with the help of Tractor and the propositionalizer [4]. These graphs are used as an input to the data association engine. Initially, a pairwise comparison is conducted between the nodes and edges across different graphs (between messages) and a similarity score is calculated for each pair using various string similarity measures. Note that the nodes and edges present within the same graph (within message) are not scored, because the within message co-referencing is done by Tractor. After scoring the node and edge pairs, we execute the data association algorithms on the graphs. The output of the data association engine is a cumulative data graph, in which the pairs of associated entities are merged together, along with their relationships (only in the case of GA\textsuperscript{N}). This cumulative data graph can now be considered as fused evidence and it can be used in the various downstream analyses like graph matching or social network analysis.

The computational results of the data association are presented in the TABLE 1. The Precision, Recall and F-score in the table represent the accuracy of the association and higher values typically indicate greater accuracy. We provide a detailed description of these measures in Subsection C.

C. Evaluation

To evaluate the accuracy of data association, we count three types of entity pairs from the cumulative data graph: (a) correctly associated, (b) incorrectly associated, and (c) incorrectly not associated. These counts are obtained by comparing the cumulative data graph with a ground truth prepared by a human analyst. After getting these counts, we use the following three measures to estimate the accuracy of the data association:

1. Precision: This is the ratio of correctly associated entity pairs to the total number of associated entity pairs (i.e., \( \frac{a}{a+b} \)). This value lies between 0 and 1.
2. Recall: This is the ratio of correctly associated entity pairs to the total number of correctly associated and incorrectly not associated entity pairs (i.e., \( \frac{a}{a+c} \)). This value also lies between 0 and 1.
3. F-score: This is the harmonic mean between the Precision and Recall. This value lies between 0 and 1.

We would like to point out that the calculation of the above measures is not that straightforward. As we mentioned before, the within message co-referencing is performed by Tractor. Therefore the main assumption of data association is that there are no duplicate references within a particular message. If Tractor were to miss any of the within message co-references, then this imprecision is manifested in the data association results as well. To calculate the true precision and recall of the data association, we came up with a scheme in which we identify the incorrectly associated and incorrectly not associated entity pairs which stem from the imprecision caused by Tractor. To be fair we also disregard correct associations which overcame some imprecision from Tractor. We discounted these entity pairs from (a), (b) and (c), which can potentially improve the precision and recall of data association. This way we can judge the data association in an objective and impartial manner. The results presented in the TABLE 1 are obtained using this scheme.

<table>
<thead>
<tr>
<th>No.</th>
<th>Procedure</th>
<th>Precision</th>
<th>Recall</th>
<th>F-Score</th>
<th>Computing Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GA\textsuperscript{N} (Sequential)</td>
<td>0.92</td>
<td>0.87</td>
<td>0.89</td>
<td>107133</td>
</tr>
<tr>
<td>2</td>
<td>MDADC (MR)</td>
<td>0.82</td>
<td>0.90</td>
<td>0.86</td>
<td>60220</td>
</tr>
</tbody>
</table>

We can clearly see a tradeoff between the computing time and the accuracy of the results (the F-score). The GA\textsuperscript{N} formulation gives more accurate results but at the expense of the computing time. If the data size is large, the GA\textsuperscript{N} procedure will prove to be a bottleneck. On the other hand, MDADC formulation solved using Map/Reduce gives a quick and reasonably accurate solution and it can be easily applied to large sized problems given the necessary hardware.

V. Graph Matching

Graph matching is an analytical technique for identifying situations of interest (template graphs) within some accumulated graphical knowledge base (cumulative data graph). There are a number of complicating factors in identifying graph matches including: uncertainties present in observed data as well as situations of interest, necessity to maintain matching results in a streaming environment, identifying results in an efficient manner while considering very large data graphs and overseeing many (sometimes overlapping) situations of interest simultaneously. Techniques for addressing some of these challenges have been developed in the past [9]-[12]. A new method for handling multiple situations of interest concurrently is briefly introduced here and demonstrated on the SYNCOIN vignette discussed in Section III.

The method developed for concurrent consideration of multiple situations of interest is the matching of AND/OR template graphs. An AND/OR template graph conglomerates...
multiple situations into a single template. AND/OR templates are useful in circumstances where a situation of interest can be represented in a number of different ways or for different situations which contain some overlapping graph elements. The efficiency of the graph matching algorithm is improved by branching on common template nodes at earlier search tree levels, thereby eliminating the redundant branching which would exist in multiple graph matching executions.

An example AND/OR template graph is provided in Figure 1. In this template we are interested in identifying a trafficker who possesses IED materials. There are a number of ways the “possession” of these IED materials could be reflected in the accumulated evidence. The possession could be directly indicated (e.g., by the possession edge number 4), or the possession relationship may be an indirect relationship. In the subgraph of edges 5 and 6 and node 3 we represent the condition where IED materials are located in some possession of the matched trafficker. The fulfillment of this AND/OR template graph is satisfied by matching either of the template paths pictured in Figure 2.

Figure 1. Example AND/OR Template Graph

A hypothetical S2 analyst charged with investigating the activities of the Sunni Criminal Group would likely have some knowledge of their involvement in IED trafficking. To better understand the nature of the IED trafficking business the analyst could create the template pictured in Figure 1 to be matched in the SYNCOIN SUN cumulative data graph. The top result from a graph matching execution on the cumulative data graph produced in Section IV is pictured in Figure 3. In this top result we have identified a known trafficker (Dhanun Ahmad Mahmud Ahmad) who possesses a car in which IED trigger devices are located. This match allows the analyst to further investigate this IED trafficker who is eventually arrested and converted to a paid informant.

Figure 3. Top Graph Matching Result
Let, $w(i, j)$ be the weight of an edge between node $i$ and node $j$. 

$P_{ij}$ be a set of all paths between node $i$ and node $j$. 

$p_{ij}$ be a single path such that $p_{ij} \in P_{ij}$. 

$h(p_{ij})$ be the number of hops in path $p_{ij}$. 

$T$ be the hops threshold.

Then, 

$$w(i, j) = 1 \sum_{p_{ij} \in P_{ij}} \frac{1}{h(p_{ij})}, \text{ such that } h(p_{ij}) \leq T.$$  \hspace{1cm} (1)

2) Centrality Metrics Calculations: Three centrality metrics, viz., degree centrality, closeness centrality and betweenness centrality are computed for each node in the extracted social networks. To identify high value individuals, nodes are rank ordered by sorting them in a decreasing order of betweenness centrality, then by closeness centrality and degree centrality thereafter to identify the high value individuals.

In an undirected graph, the degree centrality is defined as the number of connections of a node, which is nothing but the number edges attached to a node.

Closeness centrality is calculated as the inverse of the sum of the shortest path distances between a node $i$ and the remaining $n-1$ nodes in a network of size $n$. Thus, the node $i$’s closeness centrality, $C_c(i)$ is given by:

$$C_c(i) = \frac{1}{\sum_{j \neq i} d_{ij}}, \forall i.$$  \hspace{1cm} (2)

Where, $d_{ij}$ is the distance between nodes $i$ and $j$ taken along a shortest path. The division by zero is mathematically undefined. Thus, closeness centrality cannot be calculated for graphs containing isolated nodes. This is applicable only to those nodes that form a connected graph. Our CDG is a disconnected graph. Hence, Opsahl’s closeness centrality [13], which is defined for disconnected graphs, is used. It is defined as,

$$C_c(i) = \sum_{j \neq i} \frac{1}{d_{ij}}, \forall i.$$  \hspace{1cm} (3)

According to the original definition, the betweenness centrality value for a fixed node $i$ in a given network is found as follows [14].

Consider every pair of nodes, $j$ and $k$, in the network. Let $\sigma_{jk}$ denote the number of shortest paths between nodes $j$ and $k$, and let $\sigma_{jk}(i)$ denote the number of shortest paths between nodes $j$ and $k$ that involve node $i$. Then, betweenness centrality of node $i$ is given by,

$$C_{B}(i) = \sum_{j,k \neq i} \frac{\sigma_{jk}(i)}{\sigma_{jk}}.$$  \hspace{1cm} (4)

The exact betweenness centrality values are computed using Brandes’ betweenness algorithm [15].

3) Visualization of the Generated Social Network: Figure 4 shows a visualization of the ground truth data, while Figure 5 represents the extracted social network with the hop threshold $T$, set to 5. These visualizations are performed in Gephi software [16] with ‘Force Atlas’ layout type. In these figures, the larger the node size, the higher its betweenness centrality value is. Also, the darker the blue color of a node, the higher its degree centrality value is. The thicker the edge width, the farther apart is the relationship. Visualization, apart from actual centrality metric values helps an analyst identify high value individuals in a network. It can be observed that the extracted social network is bigger and denser than the ground truth network. There are two reasons for these deviations from the ground truth. First, some of the nodes in the extracted network are not actual person nodes (they are wrongly tagged as person nodes), and some nodes have not been successfully associated in CDG. That is, two or more nodes represent the same person. However, when the top 5 high value individuals in the ground truth network are compared against the top 5 individuals in the extracted social network, it is found that top 3 out of 5 individuals are common between the two networks. Their ranks are also the same (see TABLE 2).
TABLE 2. COMPARISON OF HIGH VALUE INDIVIDUALS.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Extracted Network</th>
<th>Ground Truth Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dhanun Ahmad</td>
<td>Dhanun Ahmad</td>
</tr>
<tr>
<td>2</td>
<td>Abdul Jabar Wahied</td>
<td>Abdul Jabar Wahied</td>
</tr>
<tr>
<td>3</td>
<td>Lufti Dilawar</td>
<td>Lufti Dilawar</td>
</tr>
<tr>
<td>4</td>
<td>Mu’adh Nuri Khalid Jihad</td>
<td>BCT</td>
</tr>
<tr>
<td>5</td>
<td>node-text: She</td>
<td>Ragib Madharia</td>
</tr>
</tbody>
</table>

VII. CONCLUSIONS AND FUTURE WORK

This paper has presented various graph analytical tools for the fusion of hard and soft information. The soft integration and analysis has advanced from single stream analysis to multi-stream parallel processing, allowing more data to be processed quickly and efficiently. The example SUN message thread illustrates the effect of hard+soft data integration at the elemental and relationship level in addition to the value added through graph analytic operations of graph matching and social network analysis. The future work for this approach includes the continuation of improving the precision and recall of the within message associated entities, development of an incremental data association methodology, increasing the flexibility of graph matching and tighter integration of the provided and
additional social network metrics within the analytical toolbox.

ACKNOWLEDGMENT

This work has been supported by a Multidisciplinary University Research Initiative (MURI) grant (Number W911NF-09-1-0392) for “Unified Research on Network-based Hard/Soft Information Fusion”, issued by the US Army Research Office (ARO) under the program management of Dr. John Lavery. We gratefully appreciate this support.

Some aspects of this work were supported by the National Science Foundation via grant number ICES-1216082. This support is gratefully acknowledged.

REFERENCES


[2] “Unified Research on Network-based Hard/Soft Information Fusion”, Multidisciplinary University Research Initiative (MURI) grant (Number W911NF-09-1-0392) by the US Army Research Office (ARO) to University at Buffalo (SUNY) and partner institutions.


