Fusing Social Network Data with Hard Data

T. Abirami, Ehsan Taghavi, R. Tharmarasa and T. Kirubarajan
McMaster University
Hamilton, Ontario, Canada
{thirua2, taghave, tharman, kiruba}@mcmaster.ca

Anne-Claire Boury-Brisset
Defence Research and Development Canada
Valcartier, Quebec, Canada
anne-claire.boury-brisset@drdc-rddc.gc.ca

Abstract—Social networking sites such as Twitter, Facebook and Flickr play an important role in disseminating breaking news about natural disasters, terrorist attacks and other events. They serve as sources of first-hand information to deliver instantaneous news to the masses since millions of users visit these sites to post and read news items regularly. Hence, by exploring efficient mathematical techniques like Dempster–Shafer theory and Modified Dempster’s rule of combination, we can process large amounts of data from these sites to extract useful information in a timely manner. In surveillance related applications, the objective of processing voluminous social network data is to predict events like revolutions and terrorist attacks before they unfold. By fusing the soft and often unreliable data from these sites with hard and more reliable data from sensors like radar and the Automatic Identification System (AIS), we can improve our event prediction capability. In this paper, we present a class of algorithms to fuse hard sensor data with soft social network data (tweets) in an effective manner. Preliminary results using real AIS data are also presented.

Index terms: Dempster–Shafer belief theory, Random finite set theory, Modified Dempster’s rule of combination, soft and hard data fusion, airborne surveillance of surface targets, event prediction, social data analysis

I. INTRODUCTION

In defence, military or homeland security systems in order to track and predict events, and to track mobile target states, the decision makers need accurate data. Due to limited fields-of-view and obstruction, conventional prediction and tracking methods [2], [3] that rely exclusively on hard sensors (e.g., radar, sonar, video) can make erroneous decisions. On the other hand, algorithms that use only soft data (e.g., human input, social network data) can be ineffective due to conflicting unreliable information. In some cases, the unreliability of soft data might be intentional. Social Network (SN) data is one form of soft data that has many advantages: it is voluntary, voluminous, instantaneous and evolving. As a result, it is a rich source of data that is contributed over time by a large number of identifiable users, who are often close to unfolding events of interest, at virtually no cost to us. This has spurred great interest in mining social data for information extraction and exploitation. Specifically, the fusion of soft and hard data is of significant interest in many surveillance systems. This indeed provides the motivation for the proposed work.

However, there are many challenges in the fusion of soft data with hard data since they are often incompatible with each other and the computational load of processing large amounts of social network data for fusion can be prohibitive. The incompatibility stems from the fact that soft data is qualitative while hard data is quantitative [19]. We need both qualitative and quantitative information to predict events or to estimate target states precisely and with real-time capability. Such fusion is of interest in asymmetric military operations where human-generated data are shown to be of crucial importance [1]. Recent developments in the literature on human-centered information fusion [9], [23] as well as several preliminary works on soft/hard fusion are part of a trend towards more general data fusion frameworks [10] where both human (soft) and non–human (hard) data can be processed efficiently to yield better results. To develop an effective soft and hard data fusion system, one has to deploy an effective mathematical framework to fuse data and infer information while appropriately factoring in uncertainties. Commonly used frameworks for fusion are probabilistic, Dempster-Shafer, fuzzy set [25], possibilistic [5] and rough set theory [14]. This paper presents a novel approach for fusing soft social network data with hard data. Specifically, Twitter feeds are used as the source of soft data while Automatic Identification System (AIS) [12], [20] reports are used as hard data. The context of the motivating problem is the prediction of events like revolutions and terrorist attacks using social network data along with airborne surveillance data. The proposed work relies on the Modified Dempster’s Rule of Combination (MDRC) [16] because of its simplicity and its ability to resolve conflicts during fusion.

Automatic Identification System provides a way for ships to electronically send and receive data, which includes vessel identification, position, speed and coarse with vessel traffic service stations as well as with other ships. AIS uses the Global Positioning System (GPS) [18] data over digital Very High Frequency (VHF) radio communication equipment to electronically exchange location as well as other information. AIS is generally used by marine vessels along with the Vessel Traffic Service (VTS) to monitor vessel location and movement, which is primarily needed for vessel traffic control, collision avoidance and other safety applications. AIS has previously been used in many applications including fusion with radar data, anomaly detection (see Figure 1) and traffic pattern analysis. We chose AIS as the hard data source because of our focus on airborne surveillance of surface targets as well
as its ubiquity and versatility. A typical AIS functionality as shown in Figure 2 uses an array of data collection aircraft and satellites as well as coastal stations to collect information about the movement of vessels.

In the following sections, the proposed framework for soft and hard fusion with examples and implementation details is discussed. Section II presents the basic fusion framework using Dempster–Shafer Theory. Section III presents experimental results and discussions. Conclusions are presented in Section IV.

II. SOFT/HARD DATA FUSION USING DEMPSTER–SHAFER THEORY

A. Proposed approach

The proposed approach follows a hierarchy in which the data from social networking sites such as Twitter is initially processed with a set of keywords as shown in Figure 3. The output of such a processing block is the refined information according to the list of keywords. The pre-filtered data is then sent to another block to be fused with AIS data. As a fundamental step, it is necessary to address the uncertainty in the soft data in order to convert it into a quantitative value. This step is crucial as the soft data is going to be compared and fused with the output of hard sensors. In order to process large amounts of soft/hard data efficiently, an efficient method must be utilized. Here we proposed an efficient method to fuse the social network data with AIS data/hard data. The method that we follow in this paper starts with processing the SN data with a set of keywords assuming that the keywords are defined based on some evidence (see Figure 3). After extraction, there will be uncertainties and conflicts in the collected data. To remove the conflicts and uncertainties we apply Fuzzy Dempster-Shafer Belief Mass Assignment to the data. Then, Modified Dempster’s Rule of Combination (MDRC) [11], [24] is used to address the issue of fusing large amount of SN/Soft data with AIS/Hard data.

B. Dempster–Shafer theory

Here we consider a system with a finite set of possible states. These states are called the frame of discernment (also called state space) [4] in which the event under the observation can take place [1], [21]. A set of all possible outcomes of an event is formed by the Frame of Discernment (FoD). A single element of the newly formed set by FoD is called the proposition. If $\Phi$ be a set of disjoint states which forms the FoD, then the power set can be defined as $2^\Phi$. This is the set of all subsets of $\Phi$ including the null set $\{\}$.

Furthermore, the theory of evidence assigns a belief mass [7] to each element of the power set. The Belief Mass Assignment (BMA) assigns values $m(\xi)$ for all subsets $\xi \in 2^\Phi$ such that

$$m(\xi) \geq 0$$

$$m(\emptyset) = 0$$

$$\sum_{\xi \in 2^\Phi} m(\xi) = 1$$

Fig. 2: Automatic identification system functionality

Fig. 3: Block diagram of data flow in soft/hard data fusion
The belief mass that has been assigned to the proposition \( \xi \) can be treated as the certainty of the observer in the correctness of \( \xi \). The actual state of the system is represented by the elements of the power set concerning its propositions, by containing all and only the states in which the proposition is true. Dempster–Shafer theory belief function is then the total belief that the proposition is true [17]. The belief function \( b(\cdot) \) of a particular proposition \( \xi \) is given by

\[
b(\xi) = \sum_{\theta \subseteq \xi} m(\theta), \quad \xi, \theta \in 2^\Phi
\]  

(4)

C. Uncertain measurements

Handling the raw data from social network sites comes with a lot of uncertainties and conflicts in the data. In order to deal with the uncertain measurements we need to use fuzzy belief mass assignment to assign values to the measurements. Assuming that we are giving BMA based on subsets \( \omega \) with associated values \( m(\omega) \) on the set of all the subsets \( \mathcal{L} \), that is

1) \( m(\omega) \geq 0 \) is a function defined on all closed subsets \( \omega \subseteq \mathcal{L} \)
2) \( m(\omega) \geq 0 \) for all \( \omega \)
3) \( m(\omega) \neq 0 \) for finite number of \( \omega \) (which are focal subsets of \( m \))

then following is true

\[
\sum_{\omega \subseteq \mathcal{L}} m(\omega) = 1
\]

(5)

where the summation is well defined because of the third property. The function \( m(\omega) \) is known as the Dempster–Shafer measurement. Each \( \omega \) is a hypothesis of the observed measurement \( z \). Let \( \{\omega_1, \omega_2, \ldots, \omega_k\} \) be the focal subsets of \( m \), where \( k \) is the last focal subset. One of the hypotheses constrains \( z \) to be in \( \omega_1 \), i.e., \( z \in \omega_1 \) with the weight associated it as \( m(\omega_1) \). The other hypothesis can be constraining \( z \) to be in \( \omega_2 \), i.e., \( z \in \omega_2 \) with the weight \( \omega_2 \) and so on. If we know nothing about the measurement \( z \), then the weight of the hypothesis associated with that is the total value of \( m(\mathcal{L}) \)(the null hypothesis).

A fuzzy/vague measurement is thus an uncertain measurement whose focal subsets are linearly ordered under set theoretic inclusion (nested). A Fuzzy Dempster–Shafer Belief Mass Assignment (FBMA) \( m(\psi) \) is defined by the same properties as normal BMA [17]. As such the following is true

\[
\sum_{\psi} m(\psi) = 1
\]

(6)

The logical meaning of \( m(\psi) \) can be given by the fact that each \( \psi \) is a fuzzy hypothesis about the identity of \( z \) [17]. Let \( \{\psi_1, \psi_2, \ldots, \psi_k\} \) be the focal fuzzy subsets of \( m(\cdot) \) and assume that they are finite-level. It is unclear that \( z \) is or is not constrained by a particular subset \( \psi_1, \psi_1 \), therefore we must treat \( \psi_1, \psi_1 \) as initial guess about the meaning of the first fuzzy hypothesis \( \psi_1 \), where \( \psi_{1,j} \) is \( j^\text{th} \) subset of \( i^\text{th} \) focal fuzzy subset \( \psi_i \). By sequencing these into nested sequence \( \{\psi_{1,1} \subseteq ... \subseteq \psi_{1,k}\} \), we can further elaborate the nature of the uncertainty involved in the hypothesis \( \psi_1 \). This defines the finite–level fuzzy membership function \( \psi_1 \). However \( \psi_1 \) need not to be finite–level. Therefore we can interpret the remaining focal set \( \{\psi_2, \ldots, \psi_k\} \) in the same manner, where \( k \) is the last subset of \( m \).

Consider we have FDS measurements \( m, m' \). Then the FDS combination of \( m \) and \( m' \) is given by [16, pp. 144, Eq. (4.129)]

\[
(m \ast m')(\psi'') = 0 \text{ if } \psi'' = 0
\]

(7)

and if \( \psi'' \neq 0 \), then

\[
(m \ast m')(\psi'') = \alpha_{\text{FDS}}(m \ast m')^{-1} \times \sum_{\psi' = \psi''} m(\psi) \cdot m'(\psi'')
\]

(8)

where \( \alpha_{\text{FDS}}(m, m') \neq 0 \) and the FDS agreement of \( m, m' \) is

\[
\alpha_{\text{FDS}}(m \ast m') = \sum_{\psi' \neq 0} m(\psi) \cdot m'(\psi')
\]

(9)

Here, \( (\psi \cdot \psi') \triangleq \psi(z) \cdot \psi'(z) \) and the event \( \psi \neq 0 \) means \( \psi(z) \neq 0 \) for at least one \( z \).

D. Modified Dempster’s rule of combination

In this subsection we explain the data fusion using Modified Dempster’s Rule of Combination (MDRC). When actual subsets are the same as the focal subsets, then FDS combination reduces to Dempster’s rule of combination [16] as

\[
(m \ast m')(\omega'') = \alpha_{\text{FDS}}(m \ast m')^{-1} \times \sum_{\omega' = \omega''} m(\omega) \cdot m'(\omega')
\]

(10)

where Dempster–Shafer agreement is

\[
\alpha_{\text{DS}}(m \ast m') = \sum_{\omega' \neq \omega''} m(\omega) \cdot m'(\omega')
\]

(11)

The quantity \( 1 - \alpha_{\text{DS}}(m \ast m') \) is the conflict between \( m \) and \( m' \). If in addition the focal subsets of \( m \) are singletons [13], then

\[
(m \ast m')(\omega) \propto m(\omega) \cdot m'(\omega)
\]

(12)

If \( m \) and \( m' \) are interpreted as posterior probability distributions, then this is a special case of Bayes parallel combination [8]. As result we have

\[
(m \ast m')(\omega) \propto m(\omega) \cdot m'(\omega) \cdot q(\omega)^{-1}
\]

(13)

In (13) we assume that the two posterior distributions \( p_1(\omega) \) and \( p_2(\omega) \) are independent, they are conditioned on independent information and share common prior uniform distribution \( q(\omega) \). Consequently, (8) can be rewritten as

\[
(m \ast m')(\psi'' = \psi''') = \alpha_{\text{FDS}}(m \ast m')^{-1} \times \sum_{\psi' = \psi''} m(\psi) \cdot m'(\psi') \alpha_{\text{DS}}(\omega, \omega')
\]

(14)
Social network data analysis (location, content and network based analysis)

Text information (list of hash tags, places and number of repeats, etc.)

Placing disk centers (important subjects are selected)

Apply Dempster-Shafer (receives the sets, their associated probabilities from disks and creates the weights for all possible subsets)

Assign weight to the subjects (belief mass assignment)

MDRC (to remove the conflicts)

Anomaly detector (position of threat, probability)

AIS data (name, latitude, longitude, other details of vessels)

Fig. 4: Proposed hard/soft data fusion algorithm block diagram

providing that the modified agreement is non–zero and defined as

\[ \alpha = \alpha_q(m, m') \triangleq \sum_{m,m'} m(\omega) \cdot m'(\omega') \times \left[ \frac{q(\omega \cap \omega')}{q(\omega) \cdot q(\omega')} \right] \]  \hspace{1cm} (15)

where \( q(\omega) \triangleq \sum_{\nu \in \omega} q(\nu) \). If \( m \) and \( m' \) are BMA\\'s [15] whose only focal sets are singletons, then

\[ (m * m')(\nu) \propto m(\nu) \cdot m'(\nu) \cdot q(\nu)^{-1} \]  \hspace{1cm} (16)

The advantage of using MDRC over Dempster\\’s Rule of Combination(DRC) is its ability to resolve conflicts. For example, assume that a marine vessel potentially containing terrorists is approaching a coastline that has three cities, namely, A, B and C. AIS data predicts that the vessel has 99% chance of attacking city A and 1% chance of attacking city B but Social Network data such as Twitter trends suggest that there is 99% chance of an attack in city C and 1% in B. This situation is called a conflict, as it has conflicting information. A simple DRC fusion for this situation can be counter-intuitive whereas MDRC can provide a reasonable prediction. The numerical quantification of this situation is presented in Table I.

<table>
<thead>
<tr>
<th>City</th>
<th>AIS data</th>
<th>SN data</th>
<th>DRC fusion data</th>
<th>MDRC fusion data</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.9900</td>
<td>0</td>
<td>0.0000</td>
<td>0.4135</td>
</tr>
<tr>
<td>B</td>
<td>0.0100</td>
<td>0.0100</td>
<td>1.0000</td>
<td>0.1730</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0.9900</td>
<td>0.0000</td>
<td>0.4135</td>
</tr>
</tbody>
</table>

E. Hard/soft data fusion algorithm

Figure 4 illustrates the flow of the proposed approach for hard/soft data fusion. First, the raw data from social network is analyzed based on their location, content and network. This step gives the opportunity to have access to the refined data from social network for further analysis. Next, important hashtags, name of places and number of the repeats are extracted from the refined data and stored as a list.

It is of special interest to combine the list from social network data with hard data. Here we assume that we have access to AIS data, which consist of all the details about the vessels (name, latitude, longitude, speed, coarse, etc.). This AIS data needs to be processed using the anomaly detection algorithms to get the required information to be fused. By doing so a similar refined data list similar to social network data can be created based on AIS data.

At this stage we created similar materials from two different data sources. To combine all the information together and get the best decision out of it, we propose to, for each of the entities in the final combined list, put a disk center on the related coordinates of the problem. This way we can assign weights to those centers by using a belief mass assignment function. It is only after using BMA that we can send the sets, their associated probabilities and disk information to a Dempster–Shafer function to create all possible subsets and their associated probabilities. Finally, by applying MDRC to the output of the Dempster–Shafer function we can remove the conflicts between the information carried by the subsets and form the final list of subsets and probabilities to make our final decision (figure 4).

III. SIMULATIONS AND DISCUSSIONS

Marine security is a growing concern [6]. There are various types of threats that can enter a country through its waterways. For instance, a small water craft can be turned into a weapon and destroy the navy or to pirate a ship. Increased surveillance of sea is needed to protect countries from these types of threats. Presently, AIS signal and anomaly detection algorithms are used to filter the unusual behavior in maritime security systems. There are various types of sensors that are engaged in maritime security such as high frequency radar, active and passive sonar, and synthetic aperture radar. For
example, Canada’s CP-140 Aurora platform consists of many sensors that are used to collect data for the surveillance of surface targets [22]. In airborne surveillance of surface targets, sensor performance and data fusion are two major research areas. In this paper we proposed a novel approach of using the social network data (soft data) along with AIS or other airborne surveillance data sensors data (hard data) by fusing them to get a better estimation for tracking surface targets and also to increase the maritime security. In order to understand how the proposed algorithm works under different circumstances, we investigate two different scenarios in the following subsections.

A. Scenario 1

In this scenario we assume that data is collected from a social networking website (Twitter). Figure 5 shows the tweets in an area with green and red dots. Also, we consider that the red dots are the data is filtered. The threats have been identified and sorted in a list. Overall, 1 the total data collected about a particular threat $\Psi$ for our specific example is listed as follows:

- Data from sensors covering Mumbai region
- Attack on Mumbai
- Firing in Navi Mumbai
- Could be a blast in Pune

The data that we collected is the combination of both hard data from sensors and uncertain vague reports from social networking sites. This is why we first need to form the hypotheses. To form the first hypothesis, we consider a probabilistic area as a circular disk equal to $\omega_1$ centered at Mumbai. The second hypothesis $\omega_2$ is a closed disk centered at Mumbai. Third hypothesis $\omega_3$ is a closed disk centered at Navi Mumbai. The fourth hypothesis $\omega_4$ is a closed disk centered at Pune and we model it as the null hypothesis. If we have more data about some other threats going to happen in other places, we can place the disks as $\{\omega_5, \omega_6, \omega_7\}$ where $T$ is the total number of propositions.

Now we can model the uncertain hard and soft data using these hypotheses by assigning weights $\varrho_T \geq \varrho_3 \geq \varrho_2 \geq \varrho_1 \geq \varrho_0$ with these four hypotheses such that

$$\sum_{i=0}^{T} \varrho_i = 1$$  \hspace{1cm} (17)

Due to the vagueness in data, we cannot capture the place or situation correctly. Hence, we can replace each $\omega_i$ with the function of $\psi_i(z)$, that is the model for $i^{th}$ hypothesis, with probability $\varrho_i$ which represents the correct hypothesis. Then the weights $\varrho_1, \ldots, \varrho_T$ along with the set $\{\psi_1, \ldots, \psi_T\}$ give the measurement that has been collected, where $T$ is the last subset. By using this, we can define a random subset

$$\Xi_R = z|S \leq \psi_T(z)$$  \hspace{1cm} (18)

where $1 \leq I \leq T$ is the random integer defined by $P_r(I = i) = \varrho_i$ assuming $S$ and $I$ are independent. This is the random set representation of the threat $\Psi$. By having the set representation, we can apply the MDRC fusion rule to fuse the data and get the accurate position.

B. Scenario 2

Consider anomalous vessel movements in a maritime environment. The AIS data provides all details such as the name, latitude, longitude, Speed Over Ground (SOG), Course Over Ground (COG), base station and destination of all the vessels in a particular maritime region. By applying the anomaly detection algorithms to AIS data we can obtain the details of the anomalous vessels. We propose to use Twitter for getting our SN data to fuse with AIS data and find the anomaly of vessels by fusing them.

Consider country “A” receiving an alert regarding a possible terrorist attack. In this scenario we again consider taking SN data from Twitter. Tweets from a particular area of country “A” are collected through Twitter Application Program Interface (API) and processed using the JAVA programming language. According to the weights given to the propositions $(m_1, \ldots, m_n)$ of keywords, we can form the subsets in order to apply the Dempster–Shafer theory. After that, the MDRC theory is applied to reject the conflicts between the propositions and also to combine them together.

On the other hand, we can take the latitude and longitude data of vessels from AIS platform that are then converted into $X$ and $Y$ coordinate to be fused with the probabilistic measures that we get from SN data. Now that we have both SN and AIS data of a particular area over time, we can further analyze and fuse hard and soft collected data by our proposed fusion algorithm as shown in Figure 4.

Table II shows the probability of finding the threat for a city by adding SN data to AIS data. For the purpose of this simulation, AIS data and SN data for 6 cities are randomly sampled and fused using (14).

<table>
<thead>
<tr>
<th>Cities</th>
<th>AIS data</th>
<th>SN data</th>
<th>Fused data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.2096</td>
<td>0.2340</td>
<td>0.0749</td>
</tr>
<tr>
<td>2</td>
<td>0.3116</td>
<td>0.1737</td>
<td>0.0869</td>
</tr>
<tr>
<td>3</td>
<td>0.4093</td>
<td>0.5033</td>
<td>0.4125</td>
</tr>
<tr>
<td>4</td>
<td>0.6365</td>
<td>0.4069</td>
<td>0.5458</td>
</tr>
<tr>
<td>5</td>
<td>0.6582</td>
<td>0.9553</td>
<td>0.9763</td>
</tr>
<tr>
<td>6</td>
<td>0.8853</td>
<td>0.9548</td>
<td>0.9939</td>
</tr>
</tbody>
</table>

Table II shows probability of threat to a particular city with AIS data, SN data, and fused data. It shows that probability of finding the city associated with threat more effectively after adding SN data to AIS data. Figure 6 is the fusion simulation for 1000 sample cities using random probability values of hard and soft data (discrete data). In this figure we can see that when both AIS and SN prediction of threat is low (less than 0.45) the fusion predicts the threat to be lower than its parent data. On the other hand, if both AIS and SN predicts higher threat (greater than 0.7) then the fusion predicts even higher threats. These predictions are consistent with the analysis in [17]. We also performed a sample fusion of hard and soft data.
that varies with time (continuous data). For this study, the AIS and SN data are arbitrarily assumed to be a sinusoidal function and they are fed into the fusion algorithm. The resulting fusion data along with the assumed AIS and SN data are presented in Figure 7.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, a novel approach for predicting events and tracking vessels by fusing soft (e.g., Twitter) data with hard (e.g., AIS) data to improve the prediction capability was proposed. This framework was demonstrated on a representative airborne surface surveillance environment and the proposed framework can be used for other surveillance applications as well. The novelty of the work was in the use of Modified Dempster’s Rule of Combination to efficiently process large amounts of social network data along with large-scale AIS.
data and the preliminary results were presented. We plan to extend the work to consider more realistic scenarios with even larger data sets. In addition, theoretical performance quantification and computational complexity analysis are needed to be performed for assessing its efficiency.

REFERENCES


