Modeling a Probabilistic Ontology for Maritime Domain Awareness

Rommel N. Carvalho, Richard Haberlin, Paulo Cesar G. Costa, Kathryn B. Laskey, KC Chang
Center of Excellence in C4I / The Sensor Fusion Lab
George Mason University, MS 4B5
Fairfax, VA 22030-4444 U.S.A.
Email: rommel.carvalho@gmail.com, [rhaberli,pcosta,klaskey,kchang]@gmu.edu

***Abstract*—Situational awareness and prediction are essential elements of information fusion. Both involve various types of uncertainty and require a sound automated inferential process. Probabilistic ontologies support uncertainty management in semantically aware systems, and facilitate modular, interoperable systems. This paper describes the process of developing a probabilistic ontology for a Maritime Domain Awareness application. The ontology was created to support identification of ships behaving suspiciously enough to be declared ships of interest. The original model was expanded in two ways: to provide reasons for declaring a ship as being of interest, and to include individual crew member associations. The latter is achieved by supporting inferences about a person's close relations, group associations, communications, and background influences to assess his likelihood of having terrorist links.**

Keywords: modeling methodology, probabilistic ontology, uncertainty reasoning, predictive situational awareness, web services, Bayesian networks, MEBN, PR-OWL.

I. Introduction

Maritime Domain Awareness (MDA) involves the ability to automatically integrate information from multiple sources in a complex and evolving scenario to produce a dynamic, comprehensive, and accurate picture of the naval operations environment. The emphasis on net-centric operations and the shift to asymmetric warfare have added an additional level of complexity and technical challenge to automated information integration and predictive situation assessment. A probabilistic ontology (PO) [1] is a promising tool to address this challenge. A PO for Maritime Domain Awareness (MDA) was presented by Carvalho *et al.* [2]. This PO was designed for the PROGNOS project [3]. The current work leverages the original MDA PO by extending its feature set to provide improved support for automated reasoning.

PR-OWL [1] is an OWL upper ontology for representing uncertainty that relies on Multi-Entity Bayesian Networks (MEBN) [4]. MEBN semantics integrates the standard model-theoretic semantics of classical first-order logic with random variables as formalized in mathematical statistics. It represents the world as consisting of entities that have attributes and are related to other entities. Knowledge about the attributes of entities and their relationships to each other is represented as a collection of MEBN fragments (MFrags) organized into MEBN Theories (MTheories). An MFrag represents a conditional probability distribution for instances of its resident random variables given their parents in the fragment graph and the context nodes. An MTheory is a set of MFrags that collectively satisfies consistency constraints ensuring the existence of a unique joint probability distribution over instances of the random variables represented in each of the MFrags within the set. An MFrag can be instantiated as many times as needed to build a Situation-Specific Bayesian Network (SSBN) in response to a query. In a PR-OWL based system, domain knowledge is encoded as a set of MFrags. When a query is posed to the system, a MEBN reasoner builds a SSBN to answer the query.

PROGNOS [3], [5] (PRobabilistic OntoloGies for Net-centric Operation Systems) is a naval predictive situational awareness system devised to work within the context of U.S. Navy's FORCENet. The system uses the UnBBayes-MEBN framework [6], which implements a MEBN reasoner capable of saving MTheories in PR-OWL format. The next section presents the methodology used in PROGNOS for modeling a probabilistic ontology. Then, Section III provides an explanation on how the methodology was used to build the updated version of the original MDA ontology, as well as the two extensions that are the major contributions of this article.

II. The Uncertainty Modeling Process for the Semantic Web

Although there is now substantial literature about what PR-OWL is [1], [7], [8], how to implement it [9]–[11], and where it can be used [3], [5], [12]–[14] little has been written about how to model a probabilistic ontology. Carvalho *et al.* [15] addressed this by presenting an approach to modeling a probabilistic ontology and using it for plausible reasoning. This will be the methodology used to design and develop the probabilistic ontology for Maritime Domain Awareness.

The Uncertainty Modeling Process for the SW (UMP-SW) is divided into three steps: to model the domain, to populate its KB, and to use both to perform reasoning.

The modeling step consists of three major stages: Requirements, Analysis and Design, and Implementation. These terms are borrowed from the Unified Process (UP) [16] with some modifications to adapt to the domain of ontology modeling. The UMP-SW is also consistent with the Bayesian network modeling methodology described by [17] and [18]. Figure 1

Figure 1. Probabilistic Ontology Modeling Cycle (POMC) - Requirements in blue, Analysis and Design in green, and Implementation in red.

depicts these three stages of the Probabilistic Ontology Modeling Cycle (POMC). Like the UP, POMC is iterative and incremental. The basic idea is to model the domain incrementally, allowing the modeler to take advantage of lessons learned during the modeling of earlier versions of the model. Learning comes from discovering new rules, entities, and relations that were not obvious previously, which can give rise to new questions and evidence that might help us achieve our previously defined goal as well as give rise to new goals.

In the POMC (Figure 1) the Requirements stage (blue circle) defines the goals that must be achieved by reasoning with the semantics provided by our model. The Analysis and Design stage describes classes of entities, their attributes, how they relate, and what rules apply to them in our domain (green circles). This definition is independent of the language used to implement the model. Finally, the Implementation stage maps our design to a specific language that allows uncertainty in the SW, which in this case is PR-OWL (red circles).

III. Probabilistic Ontology for Maritime Domain Awareness

The PROGNOS MDA PO was created using the Uncertainty Model for the Semantic Web (UMP-SW) and the Probabilistic Ontology Modeling Cycle (POMC) presented in Section II, with the support of the stakeholders (MEBN and PR-OWL experts and subject matter experts from the Navy).The probabilistic ontology developed so far has passed through three iterations. The first iteration was detailed in Carvalho *et al.* [2] and consists of a simple model to identify whether a ship is of interest. The second iteration expanded the model to provide clarification of the reasons behind declaring a ship of interest. The third iteration focused on detecting an individual crew member's terrorist affiliation given his close relations, group associations, communications, and background influences.

A. Probabilistic Modeling - First Iteration

The original model consists of the following set of goal/query/evidence:

1) Identify if a ship is of interest, *i.e.*, it seems to be suspicious in any way.
   a) Does the ship have a terrorist crew member?
      i) Verify if a crew member is related to any terrorist;
      ii) Verify if a crew member is associated with any terrorist organization.
   b) Is the ship using an unusual route?
      i) Verify if there is a report that the ship is using an unusual route;
      ii) Verify if there is a report that the ship is meeting some other ship for no apparent reason.
   c) Does the ship seem to exhibit evasive behavior?
      i) Verify if an electronic countermeasure (ECM) was identified by a navy ship;
      ii) Verify if the ship has a responsive radio and automatic identification system (AIS).

The final result of this initial iteration is the PO depicted in Figure 2. There, the hypotheses related to the identification of a terrorist crew member are presented in the `Has Terrorist Crew`, `Terrorist Person`, and `Ship Characteristics` MFrags. The hypotheses related to the identification of unusual routes are presented on the `Unusual Route` and `Meeting` MFrags. Finally, the hypotheses related to identification of evasive behavior are shown in the `Evasive Behavior`, `Electronics Status`, and `Radar` MFrags. Further details can be found in [2], and the test and evaluation of this initial process are explained in an upcoming paper.

B. Probabilistic Modeling - Second Iteration

Once the initial model was built and tested, the second iteration shifted focus to understanding the reasons for classifying a ship's behavior as suspicious. The approach was to define possible terrorist plans that might result in specific behaviors. At this stage, two terrorist plans were taken into consideration: exchange illicit cargo (*e.g.*, explosives) and bomb a port using a suicide ship. Another distinction from the original model is that the behavior depends not only on the plan being executed, but also on the type of the ship. In addition, there are now two reasons why a ship might be executing a terrorist plan: it either has a terrorist crew member (the only option in the original model) or the ship was hijacked.

1) Requirements: With the new task of identifying the terrorist plans associated to a suspicious ship (*i.e.*, exchanging illicit cargo, bombing a port, or no terrorist plan), the second iteration's set of goal/query/evidence was also expanded:

Identify if a ship is a ship of interest, *i.e.*, if the ship has some terrorist plan associated with it.

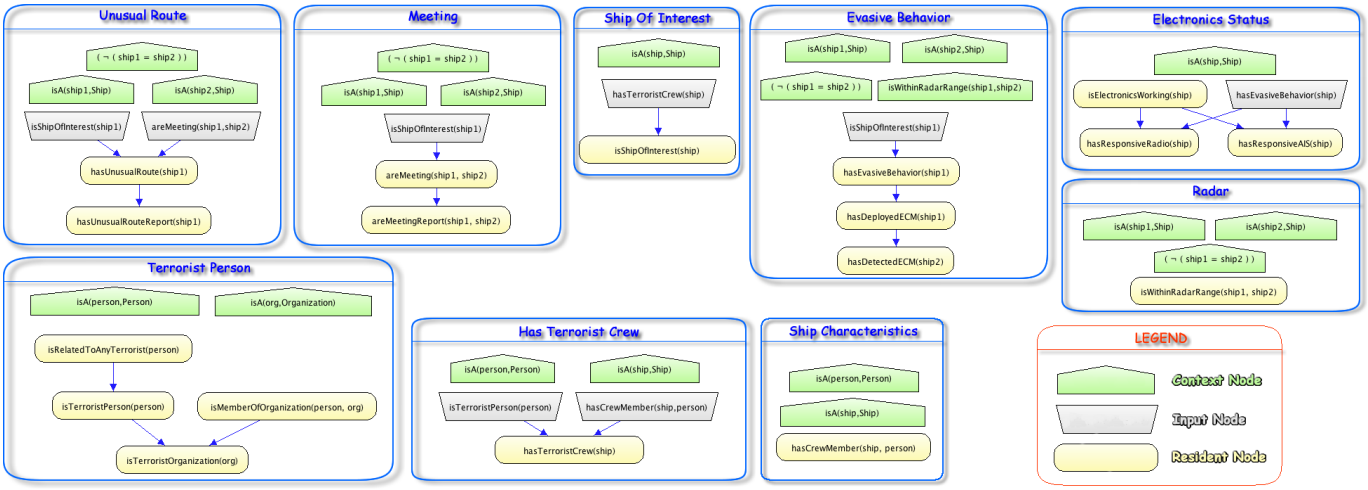

Figure 2. MTheory created in first iteration.

1) Is the ship being used to exchange illicit cargo?
   a) Was the ship hijacked?
   b) *Does the ship have a terrorist crew member?*
      i) *Verify if a crew member is related to any terrorist;*
      ii) *Verify if a crew member is associated with any terrorist organization.*
   c) *Is the ship using an unusual route?*
      i) *Verify if there is a report that the ship is using an unusual route;*
      ii) *Verify if there is a report that the ship is meeting some other ship for no apparent reason.*
      iii) Verify if the ship had a normal change in destination (*e.g.*, to sell the fish, which was just caught.)
   d) *Does the ship seem to exhibit evasive behavior?*
      i) ~~*Verify if an electronic countermeasure (ECM) was identified by a navy ship;*~~
      ii) *Verify if the ship has a responsive radio and automatic identification system (AIS).*
   e) Does the ship seem to exhibit erratic behavior?
      i) Verify if the crew of the ship is visible.
   f) Does the ship seem to exhibit aggressive behavior?
      i) Verify if the ship has weapons visible;
      ii) Verify if the ship is jettisoning cargo.
2) Is the ship being used as a suicide ship to bomb a port?
   a) Was the ship hijacked?
   b) *Does the ship have a terrorist crew member?**
   c) *Is the ship using an unusual route?**
   d) Does the ship seem to exhibit aggressive behavior?*

Requirements inherited from the first iteration are in italic. Items crossed out refer to evidence considered by the SMEs, but that pertain only to war ships. Since these are not included in the scenarios they were excluded from the model. Queries marked with '*' are also used for another subgoal. For instance, an unusual route is expected both from ships with plan to bombing a port and fron a plan to exchange illicit cargo. The associated evidence is shown only for the first subgoal using the query.

2) Analysis and Design: As the original requirements were expanded, the UML model was also expanded to identify new concepts needed for achieving the new goals. Figure 3 displays the resulting model, with some classes added (*e.g.*, `Plan`, `TerroristPlan`, `TypeOfShip`, etc) and others removed (*e.g.*, `ECM`). Major changes are the new types of behavior (`AggressiveBehavior` and `ErraticBehavior`), the classification of ships (`TypeOfShip` and its subclasses), and planning information (`Plan`, `TerroristPlan`, and its subclasses). In addition, class `Ship` was expanded to allow for situational awareness of its behavior and to predict future actions based on it.

The next step is to define rules associated with the new requirements. The probabilistic rules below complement the cardinality and uniqueness rules in Figure 3 (same typing convention for rules inherited or not used in the model apply).

1) *A ship is of interest if and only if it has a terrorist ~~crew member~~* plan;
2) A ship has a terrorist plan if and only if it has terrorist crew member or if it was hijacked;
3) *If a crew member is related to a terrorist, then it is more likely that he is also a terrorist*;
4) *If a crew member is a member of a terrorist organization, then it is more likely that he is a terrorist*;
5) *If an organization has a terrorist member, it is more likely that it is a terrorist organization*;
6) *A ship of interest is more likely to have an unusual route*, independent of its intention;
7) *A ship of interest*, with plans of exchanging illicit cargo, *is more likely to meet other ships*;
8) *A ship that meets other ships to trade illicit cargo is more likely to have an unusual route*;

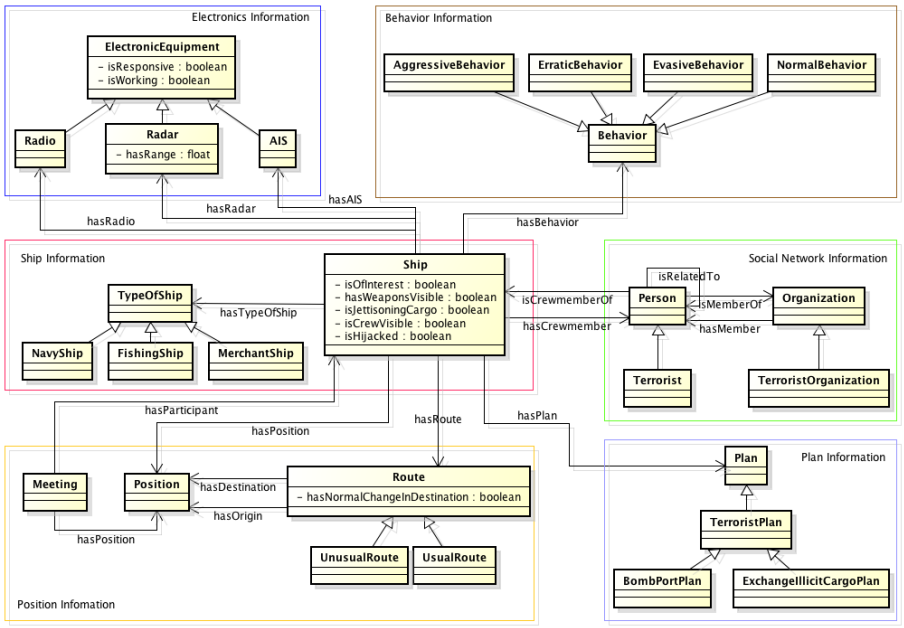

Figure 3. Entities, their attributes, and relations for the MDA model after the second iteration.

9) A fishing ship is more likely to have a normal change in its destination (e.g., to sell the fish caught) than merchant ships;
10) A normal change in destination will probably change the usual route of the ship;
11) *A ship of interest*, with plans of exchanging illicit cargo, *is more likely to have an evasive behavior*;
12) A ship with evasive behavior is more likely to have non responsive electronic equipment;
13) A ship might have non responsive electronic equipment due to maintenance problems;
14) ~~A ship with evasive behavior is more likely to deploy an ECM~~;
15) ~~A ship that is within radar range of a ship that deployed an ECM might be able to detect the ECM, but not who deployed it~~;
16) A ship of interest, with plans of exchanging illicit cargo, is more likely to have an erratic behavior;
17) A ship with normal behavior usually does not have the crew visible on the deck;
18) A ship with erratic behavior usually has the crew visible on the deck;
19) If the ship has some equipment failure, it is more likely to see the crew on the deck in order to fix the problem;
20) A ship of interest, independent of its intention, is more likely to have an aggressive behavior;
21) A ship with aggressive behavior is more likely to have weapons visible and to jettison cargo;
22) A ship with normal behavior is not likely to have weapons visible nor to jettison cargo.

3) Implementation: Once the Analysis and Design stage is finished, implementation in a specific language (PR-OWL in this case) begins. The initial step is to map entities, attributes, and relations to PR-OWL. There is no need to map all entities in the model to entities in PR-OWL. In fact, the MDA model contains many simplifications. One is to define the random variable `hasTypeOfShip` mapping to values `Fishing` or `Merchant`, instead of creating them as subclasses. This can be done by creating a class in OWL using *oneOf* to specify the individuals that represent the class `ShipType`. Also, the original assumption of every entity being uniquely identified by its name still holds. The entities implemented in the MDA PO were `Person`, `Organization`, and `Ship`. All other entities were simplified in a similar manner as *ShipType*. For details on defining entities in UnBBayes see [10].

After defining entities, the uncertain characteristics are identified. Uncertainty is represented in MEBN as random variables (RVs). In UnBBayes, a RV is first defined in its Home MFrag. Grouping RVs into MFrags closely follows the grouping observed in the Analysis and Design stage. Typically, a RV represents an attribute or a relation in the designed model. For instance, the RV `isHijacked(Ship)` maps to the attribute `isHijacked` of the class `Ship` and the RV `hasCrewMember(Ship, Person)` maps to the relation `hasCrewMember` (refer to Figure 3). As a predicate relation, `hasCrewMember` relates a `Ship` to one `Person` or more, the same way class `Ship` might have one `Person` or more as its crew members. Hence, the possible values (or states) of this RV are `True` or `False`. Subclasses were avoided by using Boolean RV like `isTerrorist(Person)`, which represents the subclass `Terrorist`. Each RV is represented as a resident node in its home MFrag.

Once all resident RVs are created, their relations are defined by analyzing dependencies. This is achieved by looking at the

rules defined in the model. For instance, the first rule indicates a dependence between `hasTerroristPlan(Ship)` and `isShipOfInterest(Ship)`. The structure of the relations added to the MDA PO can be seen in Figure 4.

After defining the relations, the local probability distributions are inserted for each resident node. For conciseness, these are not presented here but they must be consistent with the probabilistic rules defined in the Analysis and Design stage.

C. Probabilistic Modeling - Third Iteration

While the original model considered whether a person is related to a terrorist or is part of a terrorist organization, this iteration focuses on determining whether a person *is* a terrorist. Ethical aspects excluded, creating a profile of a terrorist from the available merchant population reduces the volume of individuals requiring further investigation by limited analytic resources. The idea is to infer an individual crew member's terrorist affiliation given his close relations, group associations, communications, and background influences. Literature on the subject reveals several models that sought to map the terrorist social network using social network analysis and some method of probabilistic inference. Using automation to identify interconnections between terrorists can reduce operator workload. Yang and Ng constructed a social network from weblog data gathered through topic-specific exploration [19]. Similarly, Coffman and Marcus performed social network analysis through pattern analysis to classify the roles of actors within a network using communication data [20]. Dombroski and Carley propose a hierarchical Bayesian inference model to produce a representation of a network's structure and the accuracy of informants [21]. Krebs has mapped a terrorist network topology from open-sources following the 9/11/2001 attacks and introduced a model representing the degrees of separation in Al Quaida leadership [22]. In a few cases, these network analyses were taken a step further and used to evaluate effects of friendly force courses of action, effects of removing particular individuals, and predicting attacks based on patterns of activity. Wagenhals and Levis used a timed influence net to add a temporal component to a model with terrorists embedded in a society that is supporting them to describe desired and undesired effects to both the adversary and local population caused by friendly forces [23]. Moon and Carley linked social and spatial relations to predict the evolution of a terrorist network over time, and posit the effect of "isolating" particular individuals within the network [24].

These models all concern groups, their members, and linkages. Our third iteration has the goal of applying high-level fusion by combining information about relations, group affiliations, communications, and ethno-religious or political background into a model describing the likelihood that a particular individual becomes a terrorist. This will extend the overall high-level fusion MDA PO developed so far.

1) Requirements: The main goal is to identify the likelihood of a particular crew member being a terrorist. Specific statistics were not available in open-source material so the model assumes 0.001 percent of the target demographic to be involved in terrorism, and expands the query "Does the ship have a terrorist crew member?" as follows (same typing convention applies):

1) *Does the ship have a terrorist crew member?*
   a) *Is the crew member associated with any terrorist organization.*
   b) Has the crew member been negatively influenced in some way by his/her personal history?
      i) Verify if the crew member has direct knowledge of someone either detained or killed by coalition forces during the conflict;
      ii) Verify if the crew member is married.
   c) Has the crew member been using communications media frequently used by terrorists?
      i) Verify if the crew members uses cellular communication;
      ii) Verify if the crew members uses chat room communication;
      iii) Verify if the crew members uses email communication;
      iv) Verify if the crew members uses weblog communication;
   d) Is the crew member a potential terrorist recruit?
      i) *Verify if the crew member is related to any terrorist;*
      ii) Verify if the crew member has friendship with any terrorist.
   e) Is the crew member associated with any of the four primary terrorist cliques introduced by Sageman who are operating in the Middle East, North Africa and Southeastern Asia [25]?
      i) Verify if the crew member is a professional, semiskilled, or unskilled laborer;
      ii) Verify the education level of the crew member;
      iii) Verify if the crew member is from the upper, middle, or lower class;
      iv) Verify the nationality of the crew member.

2) Analysis and Design: This stage formally defines the model semantics captured in the UML model. Table I presents a two step approach to identifying the major entities, their attributes, and relationships. Initially, the requirements are the main source for keywords representing concepts to be defined in the ontology (*e.g.*, highlighted text in Table I). Then, the chosen keywords are grouped in a logical manner, e.g., grouping attributes with the entities possessing them (see simple grouping on the second column). Although not shown here for brevity, this method was used for the analysis and design of all the requirements in this iteration. The resulting attributes, relationships and their grouping for the entities `Person` and `Organization` is shown in Table II.

These three iterations are meant to illustrate the probabilistic definitions of the ontology, and thus reflect just the initial steps in building a full model. Further analysis of this listing will show that other entities are necessary to encode its

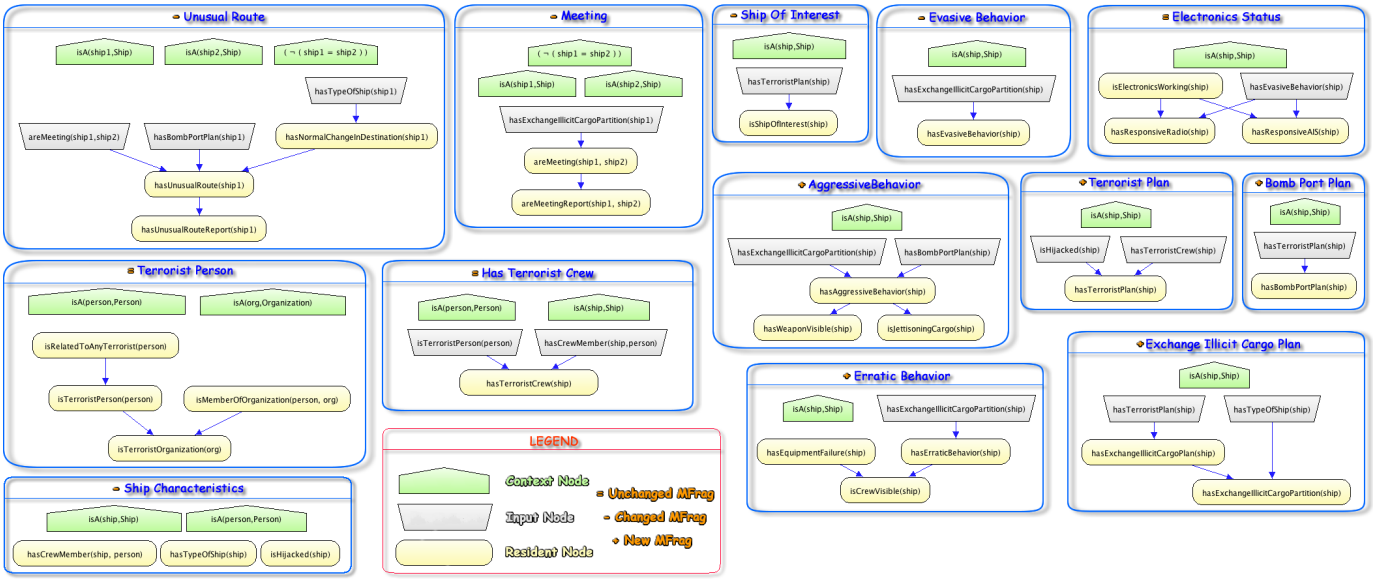

Figure 4. MTheory created in second iteration.

Table I
A SIMPLE METHOD FOR IDENTIFYING ENTITIES, ATTRIBUTES, AND RELATIONSHIPS.

...Does the ship have a terrorist crew member? ...Is the crew member associated with any terrorist organization. ...Verify if the crew member is married. ...Verify if the crew members uses cellular communication; ...	Ship -hasCrewMember Person -isMemberOfOrganization -isMarried -usesCellularCommunication

Table II
GROUPING FOR ENTITIES, ATTRIBUTES, AND RELATIONS IN THIRD ITERATION.

Terrorist grouping -Person -isTerrorist -Organization -isMemberOfOrganization -isTerroristOrganization Communication grouping -Person -usesWeblog -usesEmail -usesCellular -usesChatroom Relationship grouping -Person -hasTerroristBeliefs -hasKinshipToTerrorist	-hasFriendshipWithTerrorist Background influence grouping -Person -hasInfluencePartition -hasFamilyStatus -hasOIForOEFInfluence -knowsPersonKilledInOIForOEF -knowsPersonImprisionedInOIForOEF Cluster grouping -Person -hasClusterPartition -hasNationality -hasEconomicStanding -hasEducationLevel -hasOccupation

whole semantics. For instance, the `Country` entity is needed to express the relationship that `Person hasNationaly some Country`. The next step is to understand the domain rules, making use of the concepts identified so far to achieve the goals elicited during the requirements stage. The following rules, already grouped in fragments, were identified after a review of the open source literature available.

1) Terrorist organization grouping;
   a) *If a crew member is a member of a terrorist organization, then it is more likely that he is a terrorist;*
   b) *If an organization has a terrorist member, it is more likely that it is a terrorist organization.*
2) Background influence grouping;
   a) An individual who chooses to become a terrorist was negatively influenced in some way by his personal history. A terrorist crew member is assumed with certainty that his history affects his decision to get involved. Non-terrorists from the demographic of interest are assigned a 20% likelihood for past history affecting this decision;
   b) An individual is usually negatively affected (leads him/her in becoming a terrorist) by having direct knowledge of someone either detained or killed by coalition forces during the conflict;
   c) In the geographic area of interest, an estimated 2% of the population knows someone who was killed as a result of OEF/OIF [26];
   d) In the geographic area of interest, approximately 2% of the population knows someone detained as a result of coalition operations [26];
   e) Contrary to common perception, terrorists are predominantly married in keeping with the teachings of the Quran [25].

3) Communication grouping;
    a) It is possible that a crew member may communicate with a terrorist without being involved in terrorism due to non-terrorist affiliations or other relationships that have some normal expectation of interaction;
    b) For each of the internet communications paths there is also the background usage rate of 28.8% in the Middle East [27]. Because the data is not broken down for the three internet transmission paths, this probability was applied equally to chat room, email, and weblog methods of communication;
    c) Similarly, cellular telephone usage among the general population is assumed to be 31.6% based on Egyptian subscriber rates [28];
    d) Given the availability of cellular technology and subscribing to the prioritization, a probability of 90% is assigned to terrorists communicating using cellular telephones;
    e) The transient nature and unfettered availability of chat room communications makes it appealing to individuals who desire to remain nameless. A probability of 85% is assigned to terrorists communicating through chat rooms;
    f) Email is the least desirable form of communication because it requires some form of subscriber account. Even in the event that fictitious information is used in creating such an account, an auditable trail may lead determined forces to the originator. Still, it is a versatile means of communication and is assigned a probability of 65% for terrorists;
    g) The anonymity associated with weblog interaction is very appealing to terrorists. This path is similar to chat room communications, but is less transient in content and can reach more subscribers simultaneously. For these reasons, a probability of 80% is assigned to weblog communications.
4) Relationship grouping;
    a) Research shows that if a crew member has a relationship with terrorists, there is a 68% chance that he has a friend who is a terrorist;
    b) Research shows that if a crew member has a relationship with terrorists, there is a 14% chance that he is related to a terrorist.
5) Cluster grouping;
    a) It is assumed that all active terrorists fall into one of the terrorist cliques or their subsidiaries described by Sageman [25];
    b) Contrary to popular thought, terrorists tend to not be unskilled drifters with no options other than martyrdom;
    c) Many believe terrorist recruits to be uneducated simpletons who are easily persuaded by eloquent muftis who appeal to their sense of honor and perception of persecution. In fact, the data indicate that the typical terrorist is more educated than the average global citizen and is by far more educated than those in the Middle East, North Africa, and Southeastern Asia regions [25];
    d) Terrorist from the clusters described by Sageman [25] are less likely to be of lower class than other people from that demographic area.

This time, it was possible to assert some probability values when elaborating these rules, given the extensive research previously done. Usually, only fuzzy statements are used in these conditional rules (*e.g.*, more likely, less likely, rare, etc).

3) Implementation: Appropriate assumptions are needed to accommodate available data without compromising the utility of the model. First, a terrorist will communicate with other terrorists with certainty, but there is variability on the communication path used. Also, an individual might communicate with terrorists inadvertently. Next, there is 0.1% chance that any random person in the target demographic is a terrorist, which drives the coincidental interaction between a honest crew member and someone who may happen to be a terrorist without his knowledge. Further, the target area (Middle East, North Africa and Southeast Asia) enables using the cluster organizations introduced by Sageman [25] as basis for the groups in the association partition. Other attributes within this partition are compiled given the individual's participation in one of those groups. Additionally, a crew member could be involved with a terrorist organization other than the four identified, and that would negatively affect the outcome since he would be grouped with non-terrorists. However, it is likely that smaller groups are splinters from one of these major clusters and could therefore be included in the analysis under their super-group. Finally, in its current form, the model only captures the influence of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) and marital status in the crew member's background.

IV. Conclusions

This paper illustrates use of the UMP-SW methodology defined in [15] to create a MDA PO. The modularity provided by the MEBN fragments allows new probabilistic rules to be added, sometimes with no change to existing MEBN fragments, as for most probabilistic rules added in the third iteration. Future work involves the mapping between this PO and a maritime deterministic ontology to better understand how they can be integrated in information fusion applications.

Acknowledgment

Research on PROGNOS has been partially supported by the Office of Naval Research (ONR), under Contract♯: N00173-09-C-4008.

References

[1] P. C. G. Costa, "Bayesian semantics for the semantic web," PhD, George Mason University, Jul. 2005, brazilian Air Force. [Online]. Available: http://digilib.gmu.edu:8080/xmlui/handle/1920/455

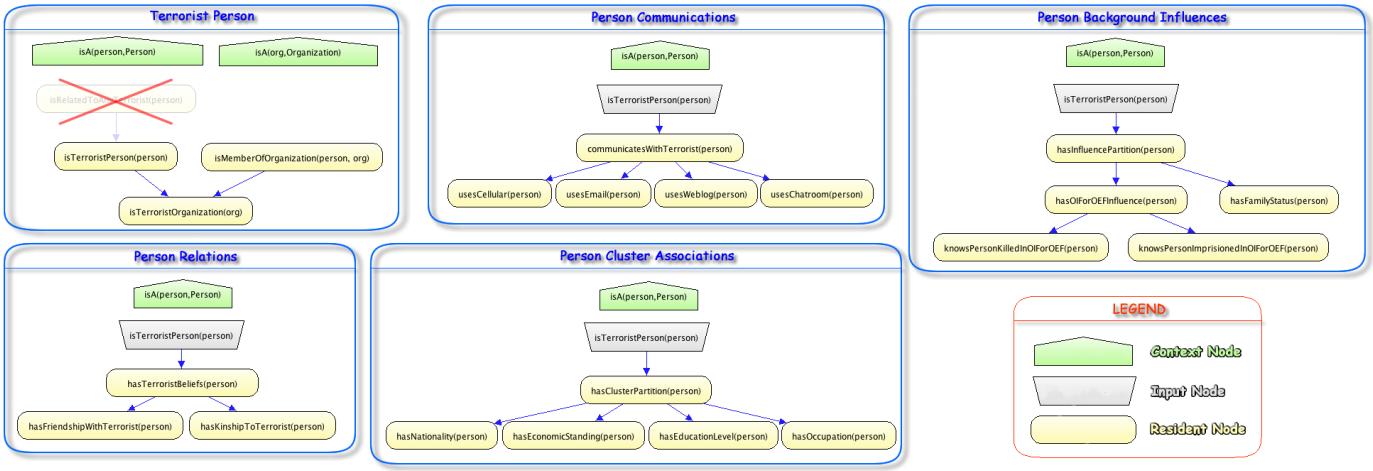

Figure 5. MFrags changed/added in third iteration.

[2] R. N. Carvalho, P. C. G. Costa, K. B. Laskey, and K. Chang, "PROGNOS: predictive situational awareness with probabilistic ontologies," in *Proceedings of the 13th International Conference on Information Fusion*, Edinburgh, UK, Jul. 2010.

[3] P. C. G. Costa, K. B. Laskey, and K. Chang, "PROGNOS: applying probabilistic ontologies to distributed predictive situation assessment in naval operations," in *Proceedings of the Fourteenth International Command and Control Research and Technology Conference (ICCRTS 2009)*, Washington, D.C., USA, Jun. 2009. [Online]. Available: http://c4i.gmu.edu/~pcosta/pc_publications.html#2009iccrts

[4] K. B. Laskey, "MEBN: a language for first-order bayesian knowledge bases," *Artif. Intell.*, vol. 172, no. 2-3, pp. 140–178, 2008. [Online]. Available: http://portal.acm.org/citation.cfm?id=1327646

[5] P. Costa, K. Chang, K. Laskey, and R. N. Carvalho, "A multi-disciplinary approach to high level fusion in predictive situational awareness," in *Proceedings of the 12th International Conference on Information Fusion*, Seattle, Washington, USA, Jul. 2009, pp. 248–255.

[6] R. N. Carvalho, "Plausible reasoning in the semantic web using Multi-Entity bayesian networks - MEBN," M.Sc., University of Brasilia, Feb. 2008. [Online]. Available: http://hdl.handle.net/123456789/159

[7] P. C. G. Costa, K. B. Laskey, and K. J. Laskey, "PR-OWL: a bayesian framework for the semantic web," in *Proceedings of the first workshop on Uncertainty Reasoning for the Semantic Web (URSW 2005)*, Galway, Ireland, Nov. 2005. [Online]. Available: http://digilib.gmu.edu:8080/xmlui/handle/1920/454

[8] P. C. Costa, K. B. Laskey, and K. J. Laskey, "PR-OWL: a bayesian ontology language for the semantic web," in *Uncertainty Reasoning for the Semantic Web I: ISWC International Workshops, URSW 2005-2007, Revised Selected and Invited Papers*. Springer-Verlag, 2008, pp. 88–107. [Online]. Available: http://portal.acm.org/citation.cfm?id=1485733

[9] R. N. Carvalho, L. L. Santos, M. Ladeira, and P. C. G. Costa, "A GUI tool for plausible reasoning in the semantic web using MEBN," in *Intelligent Systems Design and Applications, International Conference on*. Los Alamitos, CA, USA: IEEE Computer Society, Oct. 2007, pp. 381–386.

[10] R. N. Carvalho, M. Ladeira, L. L. Santos, S. Matsumoto, and P. C. G. Costa, "A GUI tool for plausible reasoning in the semantic web using MEBN," in *Innovative Applications in Data Mining*, ser. Studies in Computational Intelligence. Nadia Nedjah, Luiza de Macedo Mourelle, Janusz Kacprzyk, 2009, vol. 169, pp. 17–45.

[11] P. Costa, M. Ladeira, R. N. Carvalho, K. Laskey, L. Santos, and S. Matsumoto, "A First-Order bayesian tool for probabilistic ontologies," in *Proceedings of the 21st International Florida Artificial Intelligence Research Society Conference*, May 2008, pp. 631–636.

[12] P. C. G. Costa, K. B. Laskey, and K. J. Laskey, "Probabilistic ontologies for efficient resource sharing in semantic web services," in *Proceedings of the Second Workshop on Uncertainty Reasoning for the Semantic Web (URSW 2006)*, Athens, GA, USA, Nov. 2006. [Online]. Available: http://digilib.gmu.edu:8080/xmlui/handle/1920/1735

[13] K. Laskey, P. da Costa, E. Wright, and K. Laskey, "Probabilistic ontology for net-centric fusion," in *Information Fusion, 2007 10th International Conference on*, 2007, pp. 1–8.

[14] K. Laskey, P. Costa, and T. Janssen, "Probabilistic ontologies for knowledge fusion," in *Information Fusion, 2008 11th International Conference on*, 2008, pp. 1–8.

[15] R. N. Carvalho, K. B. Laskey, P. C. G. da Costa, M. Ladeira, L. L. Santos, and S. Matsumoto, "UnBBayes: modeling uncertainty for plausible reasoning in the semantic web," in *Semantic Web*, gang wu ed. INTECH, Jan. 2010, pp. 1–28. [Online]. Available: http://www.intechopen.com/books/show/title/semantic-web

[16] I. Jacobson, G. Booch, and J. Rumbaugh, *The Unified Software Development Process*. Addison-Wesley Professional, Feb. 1999.

[17] K. B. Laskey and S. M. Mahoney, "Network engineering for agile belief network models," *IEEE Trans. on Knowl. and Data Eng.*, vol. 12, no. 4, pp. 487–498, 2000. [Online]. Available: http://portal.acm.org/citation.cfm?id=628073

[18] K. B. Korb and A. E. Nicholson, *Bayesian Artificial Intelligence*, 1st ed. Chapman & Hall/CRC, Sep. 2003.

[19] C. Yang and T. Ng, "Terrorism and crime related weblog social network: Link, content analysis and information visualization," in *Intelligence and Security Informatics, 2007 IEEE*, 2007, pp. 55–58.

[20] T. Coffman and S. Marcus, "Pattern classification in social network analysis: a case study," in *Aerospace Conference, 2004. Proceedings. 2004 IEEE*, vol. 5, 2004, pp. 3162–3175 Vol.5.

[21] M. J. Dombroski and K. M. Carley, "NETEST: estimating a terrorist network's structure - graduate student best paper award, CASOS 2002 conference," *Springer Netherlands*, vol. 8, no. 3, pp. 235–241, 2002. [Online]. Available: http://dx.doi.org/10.1023/A:1020723730930

[22] V. Krebs, "Mapping networks of terrorist cells," 2001. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.16.2612

[23] L. Wagenhals and A. Levis, "Course of action analysis in a cultural landscape using influence nets," in *Computational Intelligence in Security and Defense Applications, 2007. CISDA 2007. IEEE Symposium on*, 2007, pp. 116–123.

[24] I. Moon and K. M. Carley, "Modeling and simulating terrorist networks in social and geospatial dimensions," *IEEE Intelligent Systems*, vol. 22, pp. 40–49, Sep. 2007, ACM ID: 1304517. [Online]. Available: http://dx.doi.org/10.1109/MIS.2007.91

[25] M. Sageman, *Understanding Terror Networks*. University of Pennsylvania Press, Apr. 2004.

[26] J. Moody, "Fighting a hydra: A note on the network embeddedness of the war on terror," *Structure and Dynamics*, vol. 1, no. 2, Jan. 2005. [Online]. Available: http://www.escholarship.org/uc/item/7x3881bs

[27] "World internet usage statistics news and world population stats," http://www.internetworldstats.com/stats.htm, 2010. [Online]. Available: http://www.internetworldstats.com/stats.htm

[28] "Wireless/Mobile statistics," http://www.mobileisgood.com/statistics.php, 2010. [Online]. Available: http://www.mobileisgood.com/statistics.php