A Generic Bayesian Network for Identification and Assessment of Objects in Maritime Surveillance

Max Krüger
Hochschule Furtwangen University (HFU)
Robert-Gerwig-Platz 1, D-78120 Furtwangen, Germany
E-mail: max.krueger@hs-furtwangen.de

Jürgen Ziegler and Kathrin Heller
Industrieanlagen-Betriebsgesellschaft mbH (IABG)
Einsteinstraße 20, D-85521 Ottobrunn, Germany
E-mail: jziegler@iabg.de, kathrin-heller@mytum.de

Abstract—Identification and assessment of objects are key capabilities of surveillance and information systems for maritime environments. Bayesian methodology provides established instruments for fusion of uncertain identification and assessment indications from various information sources. Particularly, Bayesian Networks are well qualified for modeling and inference in this application context. In order to standardize and simplify generation of Bayesian Identification Networks for new operational scenarios, a generic Bayesian Network for identification is proposed. This generic model defines adequate and necessary node types, well suited for modeling of identification and assessment tasks. In addition, the model provides a dependency structure by subgraphs, which simplifies provision of more complex cause-effect relations in Bayesian Identification Networks. Nevertheless, the generic model is flexible enough to cover various application scenarios with manifold operational demands. Closing, generation of a Bayesian smuggler detection Network for maritime surveillance in an exemplary littoral application scenario is presented.

Keywords: Identification, Affiliation & Threat Assessment, Bayesian Network, Generic Model, Uncertainty Modeling, Maritime Surveillance Systems

I. INTRODUCTION

Identification of a tracked object and assessment of its affiliation and threat potential are essential capabilities in civil and military surveillance systems, e.g., in maritime or air environment. Assignment of an identity and affiliation & threat assessment of an object are related tasks, see [1], [2], [3]. This holds in problem formulation and solution techniques, so we subsequently subsume both by the term identification (ID). In real-life scenarios, there is a large number of objects to be judged simultaneously, and consequently a strong need for automated assistance.

Bayesian techniques, and in particular Bayesian Networks provide a capable framework for an ID process ([1, ch. 5-7], [2, ch. 8,12], [3, ch. 7-9]). Existing Bayesian ID approaches tend toward a modeling that is driven by individual technical sensor capabilities and application specific structure, e.g., see [4], [5]. This makes approaches application-dependent and inflexible with respect to technical changes and enhancements, for instance new sensor technologies. More generically designed approaches, such as the standardized Identification Data Combining Process (IDCP, see [6], [7]) are constricted by certain independence assumptions of source measurements and preassigned source types, resulting from its initial context of air defense.

This paper proposes a generic Bayesian Identification Network (Bayesian ID Network) with extended application spectra in various environments, fulfilling extended operational demands. These extensions include readiness for integrating a variety of new technical sources as well as application in changing and new scenarios in asymmetric warfare.

Outline of this work: In section II we describe the use of Bayesian techniques and Networks for identification of objects. A generic Bayesian ID Network is introduced and its details are discussed in section III. The following section IV considers selected aspects of generation and configuration of Bayesian ID networks, and benefits of a source type taxonomy of contributing information sources. Section V presents a detailed example of maritime surveillance. Conclusions and future work are outlined in section VI.

II. BAYESIAN IDENTIFICATION

Classical identification by Bayesian inference uses the Theorem of Bayes

\[ p(id_i|d_1, \ldots, d_N) = \frac{p(d_1, \ldots, d_N|id_i) \cdot p(id_i)}{\sum_{j=1}^{N} p(d_1, \ldots, d_N|id_j) \cdot p(id_j)} \]  (1)

\[ p(id_i|d_1, \ldots, d_N) = \frac{p(d_1, \ldots, d_N|id_i) \cdot p(id_i)}{\sum_{j=1}^{N} p(d_1, \ldots, d_N|id_j) \cdot p(id_j)} \]  (1)

to assess the posterior probabilities of possible identities \(id_1, \ldots, id_K\), given discrete measurements \(d_1, \ldots, d_N\) of \(N\) ID sources ([2, pp. 496-497]). As a more sophisticated process, the IDCP combines several of these Naïve-Bayes assessment steps into one process ([6], [7]).

A Bayesian Network is a graphical probabilistic model. Following [8, pp. 33-34], it is defined as Directed Acyclic Graph (DAG) with each node representing a discrete random variable \(A_1, \ldots, A_N\), and directed edges representing dependencies between these variables. While modeling with Bayesian Networks, careful attention must be paid to direction of dependencies: Causes are modeled as parent nodes, effects as child nodes. Each variable \(A_i\) is in one out of a finite number of mutually exclusive, node-dependent states \(a_{i,1}, \ldots, a_{i,N}\), i.e., \(A_i = a_{i,j}\). Additionally, each node \(A_i\) is associated with a Conditional Probability Table (CPT), which describes the conditional probabilities

\[ p(A_i = a_{i,j}|A_{p_1} = b_{1}, \ldots, A_{p_K} = b_K) \]  (2)
for all (given) state combinations \( b_1, \ldots, b_K \) of all parent nodes \( A_p_1, \ldots, A_p_K \) of \( A_i \) in the DAG, \( \text{pa}(A_i) \) denotes the parent node set of \( A_i \). Bayesian Networks represent the joint probability distributions \( p(A_1, \ldots, A_N) \) of their variables. By the **Chain Rule for Bayesian Networks**

\[
p(A_1, \ldots, A_N) = \prod_{i=1}^{N} p(A_i | \text{pa}(A_i))
\]

the joint probabilities can be calculated ([8, pp. 36-37]). Generally, the state of a node variable is not known. Source measurements (evidences) in Bayesian ID Networks unveil states of some node variables. Due to dependencies between nodes, state probabilities of other nodes must be updated. This provides an inference mechanism in Bayesian Networks between source nodes and ID nodes.

Naïve-Bayes ID approaches and its IDCP extension can be expressed as Bayesian Network ([1, pp. 283-285]). Because of their modeling-inherent (conditional) independence assumptions, both DAGs have tree-structure. But modeling with Bayesian Networks allows more complex structures, capturing application-specific dependencies within an operational scenario. Figure 1 shows a Bayesian ID Network without tree-structure, taken from [4]. Finally, ID results and other higher-level information on tracked objects can be used to further improve tracking ([9]).

### III. Generic Bayesian ID Network

#### A. Generic Model

Bayesian Networks for identification with a more complex structure (see e.g. [4], [5]) have additional nodes next to the necessary *cause* and *effect* nodes, reflecting source measurements and ID results. Abstraction reveals five basic node types that occur in Bayesian ID Networks:

- **Identities&Assessments** (IDA-node type): These nodes describe ID-characteristics such as Friendly/Hos tile or Civil/Military in classical settings, or Smuggler, Pirate, Terrorist and Renegade in more recent scenarios. Generally, IDA-nodes are used to specify the possible identification results from an operational perspective. Selection of relevant possible ID results is based upon the operational application demands. For instance, allegiance is a typical characteristic to be described as IDA-node.

- **Affiliations&Intentions&Purposes** (AIP-node type): Affiliations, intentions, and purposes form the major intrinsic personality of an object, which impacts almost all facets of an object directly or indirectly. Their aggregation can be interpreted as operational personality of the object. Therefore, AIP-nodes describe the initial operational motivation and characterization, which determine appearance, behavior and activities of the object. For instance, consider hostile attitude of a terrorist towards a nation, or friendly affiliation of an own air force fighter plane.

- **Behavior&Attributes&Capabilities** (BAC-node type): Behavior, attributes, and capabilities are consequences of AIP-characteristics. Their aggregation can be interpreted as operational and technical behavior and properties of an object. BAC-nodes manifest intrinsic facets of AIP-nodes in behavior and properties, which are (by adequate measures under certain circumstances directly) observable from the objects outside. For example, BAC-nodes describe availability or use of technical properties and features, e.g., presence or utilization of anIFF mode IV device or the draft of a vessel, determining its ability to approach coastal waters.

- **Sources** (S-node type): Technical and non-technical sources provide measurements and information of BAC-aspects. Sources are modeled as S-nodes, accounting in particular for uncertainties and inaccuracies related with measurements. Possible results of source measurements are described as states of S-nodes. Therefore, assignment of conditional probabilities for these states takes account of related uncertainties and inaccuracies of their measurement process. Consider frequency types of radar devices or adherence to sealanes as example.

- **Environment&Conditions&Settings** (ECS-node type): Environment, conditions, and settings cover all object-external aspects that influence objects appearance, behavior and activities as well as corresponding measurements by sources. Being not object-inherent, ECS-nodes are interpreted as causal factors, that are located outside the considered object. Typical examples for ECS-aspects are environmental conditions, such as weather or terrain.

The DAG of the proposed generic Bayesian ID Network consists of five subgraphs, one for each node type, as shown in figure 2. Note that each subgraph contains only nodes of the dedicated type. The large arrows in figure 2 depict all possible directed dependencies between nodes of different subgraphs. Therefore, inter-subgraph dependencies are only allowed as follows:

- IDA-nodes depend only on AIP- and BAC-nodes.
- AIP- and ECS-nodes have only subgraph-internal parent nodes.
- BAC-nodes depend only on AIP- and ECS-nodes.
- S-nodes depend only on AIP-, BAC-, and ECS-nodes.

Besides these depicted ones, there are no other dependencies between nodes from different node types. Within subgraphs,
arbitrary dependencies are admitted, as long as the DAG-property is preserved within each subgraph. Obviously, the DAG-property then holds for the entire directed graph, if it satisfies the structure given by the generic Bayesian ID Network in figure 2. An example of a Bayesian ID Network which complies with the generic Bayesian ID Network is given in figure 3.

B. Structural Properties

Selected structural and content properties of the proposed generic Bayesian ID Network are discussed in this subsection. They make the network appear appropriate for a variety of ID tasks in different environments under extended operational demands:

The five basic node types, IDA-, AIP-, BAC-, S-, and ECS-nodes describe and distinguish the relevant aspects of ID-modeling on a sufficient level of abstraction. Besides the DAG-property, there are no other restrictions in modeling possible dependencies of nodes within each node-type specific subgraph. In Naïve-Bayes modeling, these inner-type dependencies are ignored, because their description is not possible. In Bayesian ID Networks, carful and frugal use of setting dependencies is recommended in order to keep the models manageable and applicable.

Identity and assessment results, modeled as IDA-nodes, are always consequences of deliberate intentions and activities: ‘No source measures identity directly’. Consequently, in the generic Bayesian ID Network, IDA-nodes only depend on AIP- and BAC-aspects and not directly on technical measurements, given by S-nodes. Differing from most classical approaches, identity aspects are expected to be modeled in several IDP-nodes. This is due to their multifaceted meaning and structure, and facilitates the understanding and configuration of the underlying model. For example, an object can be identified with respect to its Civil/Military, Friendly/Neutral/Hostile, Combatant/Noncombatant, and Private/Commercial/Governmental characteristics simultaneously. Classical approaches sometimes address this issue by using parallel assessment processes for different ID aspects based on different models.

Operational personality is modeled by AIP-nodes. These characteristics depend only on inherent intentions and existence purposes of an object. Therefore, AIP-nodes can only have AIP-subgraph internal dependencies. With some exceptions, AIP-nodes characteristics are not measured directly, but induce technical properties that can be measured. Operational expectations on the frequency of different object types determine the a priori parameters in the CPT of AIP-nodes.

Operational and technical behavior and properties are modeled by BAC-nodes. They describe operational and technical characteristics, for instance presence or use of technical devices. Besides dependencies on other operational and technical behavior and properties, BAC-nodes depend only on operational personality (AIP-nodes) of the object, and additionally on environmental factors (ECS-nodes). For example, the BAC-aspect Performing Smuggling Activities depends on the AIP-aspect Intention to Smuggle and the ECS-aspect Poor sight conditions.

Characteristics of sources, modeled by S-nodes describe the technical and non-technical sources that provide measurements and information on objects. This description includes the technical properties of sources, in particular uncertainties and inaccuracies of measurements and its interpretation. With some exceptions, source properties depend only on operational and technical behavior and properties (BAC-nodes), which are measured by the considered source. For instance, a source sudden maneuver may indicate a measurement sudden change of course. While the BAC-node state represents an actual activity, the S-node state represents the corresponding measurement. In some cases not an operational or technical behavior or property but operational personality (AIP-node) is measured directly. Consider intelligence information on Smuggling Intention of the object as example. In such cases measurements can be interpreted as update of the AIP-node a priori distribution. Concluding, S-nodes can depend on BAC-, ECS-, and AIP-nodes.
nodes, and as usual, on other S-nodes.

Environmental aspects model external factors by ECS-nodes. Therefore, they do not depend on any object aspect, but are causal to S- and BAC-nodes.

To our observation, other properties and dependencies seem to be subsidiary for sufficient identification. Therefore, they should be omitted in support of reduced complexity of modeling and algorithms. The generic Bayesian ID Network provides a modeling structure that preserves the causal structure of a given ID problem, compare [10]. Due to its generic characteristics, it is flexible enough to cover various identification tasks for manifold operational demands.

IV. ASPECTS OF PRACTICAL OPERATION
A. Generation and Configuration
The generic Bayesian ID Network is basis for generation of a Bayesian ID Network for a particular application scenario. A proceeding of generation is described in [10]: Operational experts perform a tool-based definition of the application network by defining relevant nodes, their states and their dependency structure in compliance with an underlying generic model. The proceeding in [10] takes account of the fact, that knowledge of Bayesian modeling cannot be expected from operational experts. Nevertheless the output of this first step is a qualitative model for the application scenario, covering relevant entities and dependencies.

Quantitative parameters of the application model, i.e., configuration data of the Bayesian ID Network, can be gained by User-oriented Configuration ([11]): This approach provides a process and techniques of Bayesian configuration-data acquisition. Problems related to appropriate handling of statistical information in Bayesian Networks are avoided. Particularly, this includes the known problems of misinterpreting conditional probabilities [11].

B. Source Data Exchange and Taxonomy
In order to improve overall identification quality of an object, all available source information should be used by an ID process. Particularly, this includes information generated by other dislocated, cooperating identification instances, compare [6]. Exchange of source information that is independent of the underlying ID assessment methodology provides the advantage of being able to use many additional sources. Standardized coding of (source) information is necessary precondition of Source Data Exchange. In figure 4 minimal content of Source Data Exchange is sketched. Generic fields can be adapted to formats used by data transmission systems, e.g., Tactical Data Link. The fields ID Source Number and Source Declaration are non-generic fields and to be standardized.

Development of a Source Type Taxonomy is in progress, which allows coding of source information, for instance ID Source Number, using an appropriate format. Each source instance, e.g., technical devices or human observations, is assigned to a combination of Source Type, Source Subtype, and Source Device Class indices according to a predefined taxonomy. Source Types have to be designed in a such way, that all information can be encoded. For air defense and surveillance, a taxonomy of source types has been defined in [7]. For environments other than air, definition of an adequate taxonomy and corresponding assignment of source type indices is work in progress. A selection of possible source types in maritime context includes:

- Classifying Non-Imaging Systems, e.g., ESM,
- Movement Plans & Procedural Routing,
- Track Behavior,
- Identification By Origin,
- Protected Network Location and Identification,
- Visual Sightings,
- Platform Performance,
- Events,
- Self-Identification, e.g., AIS, and
- Imaging Classification Systems.

Note that these source types are not complete and belong to the most abstract taxonomy level. Expandability of ID processes and adaptability to new application scenarios are major guidelines within the design process. The Source Type Taxonomy is intended as foundation of Source Data Exchange and cooperation in networks of heterogeneous ID systems.

V. MARITIME APPLICATION EXAMPLE

The Evaluation of Techniques for Uncertainty Representation Working Group (ETUR-WG) prepared a Ship Locating and Tracking scenario (see [12]) based upon illegal immigration detection in a maritime environment. We use this scenario as context for our subsequent Bayesian Network application. This exemplary application can be transferred to other surveillance tasks and domains, e.g., air and ground, as long as stable tracking service is available. A similar scenario assessing arms smuggling with speed boats is analyzed in [13]. By use of the IDCP ([6], [7]) a Bayesian ID process was implemented for demonstration.

A. Scenario

The scenario ([12]) in located in littoral waters, exemplarily located at Scott Islands, Canadian West Coast near Vancouver, see figure 5. A sealane from/to Asia runs in West-East direction and a major Tanker route passes Scott Islands in North-South direction. Both routes cross in large fishing grounds. Besides cargo and oil tanker traffic, there is a lot of fishing and leisure activity in the area. Military and governmental vessels supervise the area.

From intelligence sources it is known, that people smugglers intent to transport illegal immigrants on cargo ships and offload them by several trips with Zodiacs from ship
to coast. All vessels and boats involved in smuggling try to hide their activities and spoof identities by imitating fishery or leisure behavior and use of other measures. Identification task is to find the objects involved in smuggling and to discriminate them from regular commercial, fishery, private and military/governmental traffic.

B. Modeling of the Bayesian ID Network

Relevant components to be modeled in this scenario are identities according to the operational demands, maritime information sources contributing to ID processes, intentions and behavior of vessels, and environmental factors, that influence the ID processing. A dependency modeling for these components should take uncertainties and inaccuracies into account. Modeling an ID process for this scenario resulted in the Bayesian ID Network for smuggler detection in littoral waters, given in figure 6. This network consists of 40 nodes with a total of 97 states, 46 direct dependencies, and 399 parameters. Behind each node name in figure 6 its node type is denoted in brackets.

In more details, the Bayesian Network in figure 6 resulted from application of the generic Bayesian ID Network. According to scenario description ([12]), the Identities&Assessments subgraph contains a node Smuggler (IDA), which provides major discrimination between people smugglers and others. Civil/Military Discrimination (IDA) and vessel Category (IDA) node cover secondary identification demands in this scenario. Together, these three ID results provide an appropriate operational description of a vessel.

Within the Affiliations&Intentions&Purposes subgraph, the Type Affiliation (AIP) node depends on Smuggling Intention (AIP) and Military Affiliation (AIP) node. Type Affiliation (AIP) discriminates between Transport Ship, Passenger Vessel, Fishing Vessel, Leisure Boat, and Patrol Vessel. Additionally, each AIP-node is causal to its corresponding Identities&Assessments-node.

Seven behavioral facets, i.e., Military, Passenger Transport, Cargo&Tanker Transport, Fishing, Costal Cruising, Transporting Illegals, and Offloading Illegals, are given in the Behavior&Attributes&Capabilities subgraph. These facets each depend on one AIP-node. The additional dependency of Fishing Behavior (BAC) on Transporting Illegals Behavior (BAC) is due to the fact, that smugglers transport vessels imitate fishing behavior. For the same reason, Costal Cruising (BAC), which manifests leisure affiliation, depends on Offloading Illegals Behavior (BAC).

The Sources subgraph contains all sources, that can provide evidences resulting from human observations and technical devices. In order to keep the model simple, each source node gives evidence for (or against) only one behavioral facet. Therefore, each source node has few states, mostly only two, and depends only on one (behavioral) BAC parent node. Exceptions are the nodes Civil Rendezvous Report (S) and AIS (S). The former models the observation of a rendezvous between smuggler cargo vessel and zodiac. This node gives evidence for Transporting Illegals as well as for Offloading Illegals behavior, and consequently has two BAC parents. Same holds for AIS (S). The source nodes Electromagnetic Emissions (S) and Visual&EO/IR Classification (S) provide measurements that rather give evidence on affiliation then on a certain behavior of a vessel. Consequently, these two sources depend directly on the affiliation (AIP) node and not on a (behavioral) BAC node.

Only few environment modeling is provided. The Environments&Conditions&Settings subgraph contains three nodes. Nodes Visibility (ECS) and Sea State (ECS) depend on the common cause-node Weather (ECS) and influence measurements by S-nodes.

Configuration of the Bayesian ID Network has been performed with data available in or in compliance with the scenario description ([12]). Application results of this quantitative modeling part essentially depend on an appropriate qualitative modeling of the Bayesian Network graph. For options of tool-based configuration support, we refer to [11].

C. Experience

Sound modeling with a graph structure not too complex, i.e., not too many dependencies, allows easier configuration of the Bayesian ID Network. Consequently, a major part of generating a Bayesian ID Network involves definition of an adequate DAG. We judge the generic Bayesian ID Network as helpful in defining Bayesian Networks for application, because the approach reduces definition of the needed DAG in large parts into defining appropriate nodes and corresponding states. Construction is further supported by semantics of nodes, given by the subgraph-specific node types.

Looking at dependencies between nodes from different subgraphs, the cause-effect direction is instantly provided by the generic Bayesian ID Network. Considering the remaining ‘free-style’ part of modeling dependencies, we found the following hints helpful, while using the generic network:

- Normally, nodes do not need more than one parent node from each other subgraph. Otherwise, configuration can be difficult, given conflicting states of parents. If possible, source nodes should be modeled as depending only on its strongest BAC-type parent.
Dependencies within each subgraphs have to be modeled carefully and economically, i.e., only direct and strong cause-effect relationships are relevant.

Many simple nodes with only few states are preferable compared to fewer complex nodes with many states. In particular, this holds for S- and BAC-type nodes if different evidences indicate more than two different types of behavior or intentions.

For nodes with more than two states, splitting should be considered, in particular if nodes have several parents from same or other subgraphs. If not possible, try to identify a common property of all same-type parents and create a new property node.

These hints are (obviously) not obligatory. They are related to particular structure of Bayesian ID Networks complying with the generic Bayesian ID Network, and might not be applicable in other Bayesian Networks. Recommendations for modeling of general-type Bayesian Networks can be found in introductory literature, e.g., [8, ch. 3], [14, ch. 5].

D. Application to Example Cases

The Bayesian ID Network given in figure 6 is implemented using GeNLe&SMILE ([15]) software package. In the present subsection we apply our generated Bayesian ID Network for smuggler detection to several exemplary cases:

**Military Vessel**: A frigate leaves its home base and moves to a gunnery range. Available source evidences on this object are:

- **Apparent Origin Naval Base (S)** $\rightarrow$ Match.
- **Mission Plan (S)** $\rightarrow$ Match.

Identification results in figure 7 clearly indicate a military ship and exclude any smuggling activity.

**Private Yacht**: A private yacht moves at medium speed in coastal waters. Available source evidences on this object are:

- **Littoral area (S)** $\rightarrow$ Match.

Smuggling affinity is weak, but in this case there is few evidence overall.

---

**Figure 6. Bayesian ID Network for smuggler detection in littoral waters**

**Figure 7. Assessed ID military vessel**

**Figure 8. Assessed ID private yacht**
Cargo Ship: Coming from Asia, a freighter transports goods to Canada. It shows normal behavior without any anomaly. Available source evidences on this object are:

- **Sealanes (S) → Match.**
- **AIS (S) → Match.**
- **Apparent Origin Asia (S) → Match.**

Identification results in figure 9 indicate a commercial civil ship with no smuggling affinity.

![Figure 9. Assessed ID cargo ship](image)

Fishery Vessel: False evidence is given on this fishing vessel. By technical misassignment, a match on unexpected sealane leaving is given. Besides that, the vessel shows typical fishing behavior. Available source evidences on this object are:

- **Unexpected Sealane Leaving (S) → Match.**
- **Low Speed&Unsteady Course (S) → Match.**
- **Fishing Grounds (S) → Match.**

Despite false evidence, identification results in figure 10 indicate a fishing vessel. The slightly increased smuggling affinity is due to the false evidence given.

![Figure 10. Assessed ID fishery vessel](image)

Freighter Transporting Illegals: Transporting illegals, a freighter coming from Asia shows normal behavior, but starts heading towards its rendezvous point. Available source evidences on this object are:

- **Sealanes (S) → Match.**
- **AIS (S) → Match.**
- **Apparent Origin Asia (S) → Match.**
- **Unexpected Sealane Leaving (S) → Match.**

Identification results in figure 11 indicate a commercial ship. There is a suspicion towards smuggling, but so far no clear smuggling indication by any source. Contact seems to be worth of further observations. Compare to case ‘Cargo Ship’.

![Figure 11. Assessed ID freighter transporting illegals](image)

Smuggler Zodiac Offloading Illegals: A zodiac meets a cargo ship and afterwards moves towards coastal waters offloading illegals. The rendezvous is observed and reported by a fishing vessel. Available source evidences on this object are:

- **Civil Rendezvous Report (S) → Match.**
- **Littoral Area (S) → Match.**

Identification results in figure 12 indicate a small civil boat, probably involved in smuggling activities.

![Figure 12. Assessed ID smuggler zodiac offloading illegals](image)

Summing up application results of these exemplary ID cases, the generated Bayesian ID Network for detection of smuggling activities yields plausible and comprehensible results. By means of Bayesian Network learning techniques (see e.g. [16, ch. 16-17,19]) and manual fine tuning (see [17, ch. 2,5]) by operational subject matter experts, slight improvements appear possible.

VI. CONCLUSIONS

In this paper a generic model for Bayesian ID Networks has been proposed. Our intention is to standardize and simplify generation of Bayesian Networks for identification and assessment of affiliation and threat. Provision of appropriate node types and a dependency structure reflecting the cause-effect directions simplify the generation of application networks and lead towards adequate and uniform structures of Bayesian Networks for identification. Exemplarily, a Bayesian Network for smuggler detection in a maritime, littoral context has been constructed and gives encouraging application results.

Future work will need to address the question, if further detailing of node types and dependency relations can improve usability of the generic model. Next, other measures for improvement of generation and configuration of Bayesian ID models for surveillance applications are to be considered. Additionally, occurrence of type I and type II errors has to be studied. In context of the Bayesian ID Network for smuggler detection, discrimination capabilities, the set of contributing sources and their possible declarations will be detailed and completed. This might lead into an implementation for further evaluation.

REFERENCES


