Abstract—The need for improving the capability to detect illegal or hazardous activities and yet reducing the workload of operators involved in various surveillance tasks calls for research on more capable automatic tools. To maximize their performance, these tools should be able to combine automatic capturing of normal behavior from data with domain knowledge in the form of human descriptions. In a proposed Joint Statistical and Symbolic Anomaly Detection System, statistical and symbolic methods are tightly integrated in order to detect the majority of critical events in the situation while minimizing unwanted alerts. We exemplify the proposed system in the domain of maritime surveillance.

Keywords—anomaly detection; situation assessment; data driven methods; knowledge driven methods; statistical methods; symbolic methods; maritime domain awareness; surveillance

I. INTRODUCTION

With an increasingly complex maritime situational picture, operators cannot rely simply on their eyes in order to detect anomalies or suspicious vessel behavior. Due to the sheer volume of incoming sensor data, it becomes both impractical to visualize and hard to manually detect the important aspects of the vessels on a nautical chart. Furthermore, several suspicious behaviors may not be practically detectable by human operators, or may need to be observed over long periods of time to be detected.

The need for improving the capability to detect illegal or hazardous activities and yet reducing the workload of operators involved in maritime surveillance calls for research on more capable automatic tools. Such tools must capture the majority of essential events in the situation without unnecessarily disturbing the operators with unwanted alerts. In addition, they must be adaptable to changes in the behavior of legal and harmless traffic as well as to the evolvement of methods applied by criminal actors. The tools used should also be very flexible with regards to available data sources in order to present conclusions to the operators based on all relevant information that is at hand.

To address such challenges, a number of approaches have previously been presented in the research community. These could more or less be divided into two main categories:

On the one hand there are statistical or data driven approaches focusing on detecting significant deviations from normal behavior as characterized by historical data. Stemming mainly from the machine learning community the data driven approaches are often denoted Anomaly Detection.

On the other hand there are knowledge driven approaches, where humans describe the situations that are to be detected, usually by some kinds of symbolic rules. The knowledge driven methods are closely related to ‘Situation Assessment’, indicating their roots from the Data Fusion community and the JDL model.

We argue that these two main avenues of approach should be more tightly integrated than has previously been the case. To maximize performance, the tools should be able to combine automatic capturing of normal behavior with human descriptions of interesting events in a number of ways:

- The statistical anomaly detectors and the symbolic situation reasoners have many similarities that can be used to design a coherent platform.
- Statistical methods may collect statistics regarding complex events as indicated by symbolic situation assessment.
- Symbolic situation assessment may involve indications of unusual behavior as indicated by a statistical anomaly detector.
- Finally, similar methods that are used for statistical anomaly detection can be used to evaluate the performance of the rules of a symbolic situation reasoner.

These synergies will be emphasized using a proposed anomaly detection system as an example. An overview of statistical and symbolic methods is provided in Section II. The context for the proposed anomaly detection system, its architecture, and its main building blocks are presented in Section III. Next, Section IV describes and discusses the exploited synergies as listed. Finally, these proposals are concluded in Section V.
II. BACKGROUND: ANOMALY DETECTION METHODS

A. Statistical Approaches

The essence of Statistical Anomaly Detection is that an observation is tagged as an anomaly whenever the observation has low probability given a statistical model; otherwise it is tagged as normal. There are three main stages in statistical anomaly detection: finding a suitable representation of the domain data, constructing a statistical model, and determining the conditional probability of an observation given the model. For finding a suitable representation of the domain data, the domain at hand is analyzed for determining both which types of anomalies are of interest and which characteristics of the data are significant for the chosen anomaly types. This step is of great importance, as the choice of statistical model depends on it. The choice of statistical model in turn greatly affects the success of the ensuing anomaly detection. The statistical model can be constructed by standard statistical methods, e.g. by fitting a data set to an existing parametric model. The data set used for finding the model is called the training data. The model obtained from the training data is assumed to characterize normal behavior. Determining whether an observation is an anomaly is made by statistical inference.

In the system described in this paper, we use Bayesian inference to compute the probability of an observation given the statistical model. If the probability is low, the observation is considered to point to suspicious behavior that should be meaningful to investigate further by the operators. The model for each feature is selected from a set of relatively simple parametric models. The anomaly detection algorithms are described in more detail in [1] and [2].

Another variant of the statistical approach uses clustering techniques for finding a model. Given a set of training data, a model of the training data is built by using a similarity measure to group similar data items together into clusters. For determining whether an observation is anomalous, one uses a decision procedure based on the similarity measure. For example, an observation may be tagged anomalous if it does not fall into a cluster, or it may be tagged anomalous whenever it is at some distance from the center of any cluster. Laxhammar describes in [3] a clustering approach using the Gaussian Mixture Model and the Greedy EM algorithm for anomaly detection for sea surveillance.

Recently, Laxhammar and Falkman proposed a general algorithm for on-line learning and anomaly detection known as Similarity-based Nearest Neighbor Conformal Anomaly Detector (SNN-CAD) [4]. SNN-CAD is based on the theory of Conformal Prediction [5], and has a number of key properties that makes it well-suited for anomaly detection applications. In particular it is possible to control the false alert rate directly via the anomaly threshold. It is parameter-light and does not make any structural assumptions regarding the probability distribution of normal data. The method has been applied for anomaly detection in trajectory data, such as vessel routes [4], [6].

B. Symbolic Approaches

As opposed to the statistical approaches, symbolic approaches depend on knowledge provided by humans. By using a symbolic language, humans may define either a model of normal behavior from which deviations could be detected, or a model of the actual behavior that is to be detected. In the following we will only address the latter principle, since it admits a direct and precise control over the characteristics of the behavior that is to be detected and thus provides a powerful complement to the statistical approaches described in the previous section.

Obviously, a substantial work effort is required to define the characteristics of the behavior to be detected. Thus the performance of the detection system will very much depend on how easy it is to use the language to describe situations of interest. One way of building a model is to abstract the important features of the system by forming an ontology, i.e. a set of concepts and their relations in a particular domain. In [7], Matheus et al. construct a core ontology for situation awareness. The core ontology can express temporal relations between objects and it is extendable so that domain specific knowledge can be incorporated into the model. In [8] Matheus et al. use OWL [9] and SWRL [10] for expressing an ontology. This approach has its advantages in terms of standardization and the ease with which OWL and SWRL can be used for describing the world.

A few examples of symbolic anomaly detection based on ontologies have been published. Roy [11] describes the development of knowledge based tools for supporting maritime domain awareness, based on an ontology of maritime anomalies. Edlund et al. [12] describe how an ontology-based model (building on the core ontology [7]) can be used for finding predefined patterns in sea-surveillance data. In the scenarios described in the paper, certain known and interesting multi vessel temporal patterns (hijacking, smuggling, and piloting) are described as rules. The paper illustrates how a rule based approach can detect long-term intentions and situations. The system proposed in Section III builds further on this approach, however the expressiveness of the rule language has been restricted in order to suppress computational complexity.

It should be noted that the term ‘relation’ is used to emphasize that a situation of interest consist of entities (such as vessels, areas, and other objects), and relations between these, in accordance with the definition of Level 2, ‘Situation Assessment’, in the JDL model [13]. Thus the behavior to be detected in the general case involves actions of several vessels together with other objects.

C. Mixed Approaches

Some approaches mixing statistical and symbolic methods for anomaly detection have been reported.

Wong et al. [14] use a rule based approach for considering the relation between several observations. The motivation here is that in some particular cases, statistical techniques may not find anomalies that depend on the relations between several observations when those observations either are rare or, taken individually, are tagged as normal.
A somewhat similar idea is given in [15], where the traces of moving objects are broken down into trajectory fragments (called motifs) on which statistics can be applied. The motifs may be associated with attributes such as time, position, or vessel type. The trace of a moving object can then be characterized in terms of a set of (adorned) motifs whose frequencies are measured and inter-dependencies are analyzed. The authors build a feature space from the analyzed sets of motifs, thus enabling the construction of a model of normalcy. A rule-based classifier is used for classifying moving objects according to the feature space.

One way of mixing symbolic and statistical approaches is the application of Bayesian networks (BN), where the topology of the network captures domain knowledge, whereas the conditional probabilities in each node constitute statistical features. The conditional probabilities could be defined by subjective assessments, in which case the specification of the Bayesian network is purely knowledge driven. However, an example of a truly mixed approach is when the probabilities are based on statistics collected from real examples. There are some examples of such approaches used for anomaly detection, see e.g. [16].

A known difficulty with BNs is to maintain the network structure when it is getting complex, and to instantiate efficient networks for specific situations. Ontologies, on the other hand, are good at keeping track of large complex structures but lack the ability to handle uncertainties. The combination of Multi-Entity Bayesian Networks (MEBN) [17] and PR-OWL [18] address these issues. MEBN provides a way to express BNs by first-order logic. In turn, PR-OWL is an add-on to OWL including MEBN constructs. Thus an ontology expressed in PR-OWL could be used to generate a BN in order to perform reasoning on a specific case. This does not provide a method for performing anomaly detection as such, but it should be possible to pursue this approach in combination with the methods presented in [16].

Seibert et al. presented and discussed a system for detecting anomalies in a port surveillance application [19]. The system has both a rule-based pattern recognition component and normalcy learning-based component. In the rule-based component, operators use GUIs to create patterns of interest based on an ontology. The normalcy learning component, which is based on a neural network algorithm, operates in an online and semi-supervised fashion, where a context-sensitive model of vessel behavior is incrementally updated based on historical track reports and occasional operator feedback.

In this paper we will go much further in joining methods for statistical and symbolic anomaly detection, such that the two approaches may coexist on an equal footing, be freely mixed, and may take advantage of each other in a hierarchical manner.

III. THE JOINT STATISTICAL AND SYMBOLIC ANOMALY DETECTION SYSTEM

A. System Requirements

We have within the project SADV (Statistical Anomaly Detection and Visualization for Maritime Domain Awareness) studied the requirements on a real world anomaly detection system for maritime domain awareness by interviewing maritime surveillance operators in Sweden.

Some general conclusions are that the system should be capable to handle large amounts of data while, at the same time, robust when data are too few or are missing attributes; it must be able to handle several different normal states, as the traffic patterns change with seasons or during weekdays/weekends, and are different for different vessel types; and it should not give too many false alerts since this overloads the operators and makes them lose trust in the system.

From the interviews it is also clear that there are many maritime activities of interest, as for example smuggling, hijacking, or environmental threats. Different hazardous situations are also vital to detect, including risk for grounding or collisions.

These activities are characterized by different features and are on different time scales. Some examples of feature types that are interesting to model are:

- Movement patterns, such as unusual turns or stops.
- Trajectories, to detect unusual paths.
- Relative motion of two vessels, to detect e.g. rendezvous at sea.
- Inconsistencies between data sources, such as between AIS and radar.

Some of these features may be more suitable to monitor statistically and some with rules, which in itself adds support to a hybrid approach. However, more important is that many of these features are interesting to monitor both statistically and symbolically, as we will show examples of in section V.

B. System Context

To address the requirements, different statistical and symbolic concepts for anomaly detection will be hosted in a prototype for a future Joint Statistical and Symbolic Anomaly Detection System.

The context in which this future system will operate is depicted in Figure 1. It is assumed that the anomaly detection system will be connected to a maritime surveillance system that has information of the vessels that are travelling in the surveillance area. This information may origin from primary source radars, GPS receivers, and other sensors, via different distribution channels (AIS, data links, etc.). The track information that is fed to the anomaly detection system is assumed to be correlated, i.e. there is only one target track for each real vessel. In addition, the surveillance system is assumed to provide spatial information, such as areas, lines, and points of interest, together with other items that are represented in sea charts. Finally, there should be context information available regarding the vessels including their names, owners, cargo, visited harbors, expected time of arrival, and other declarations made to authorities. Context information may also include lists of suspicious vessels, owners, harbors etc.
The anomaly detection system uses this information to detect suspicious behavior among the vessels. When the anomaly values supersede certain thresholds, the resulting indications will be fed to the surveillance system together with some explanations why the indications have been issued.

The anomaly indications may be presented to the operators in different manners. A very significant anomaly indication may show up in an alert list, signaling to the operators that they at least have to evaluate the indication before it is dismissed. A less significant anomaly indication may, instead, be presented to the operator in a less intrusive manner, e.g., by altering the track symbol that represents the suspicious vessel in the situation picture. To support further analysis of the suspicious behavior, the surveillance system should provide functionality for replaying the situation that is indicated by the anomaly.

The anomaly detection system is managed by the operators in terms of configuration of rules, and of monitoring the system’s performance. Thus, the system may be executed in two different modes: In the on-line mode, anomalies will be detected as the situation evolves and as new information regarding the vessels is being received in real time. By using the off-line mode, the operators may configure the system to perform e.g. forensic analysis of historical behavior. Equally important, the off-line mode will be used to develop and evaluate symbolic rules and statistical models before they are engaged for execution in the on-line mode. To this end the performance of the rule or model is being measured and compared to how much computer resources in terms of processor load and memory usage that it will require.

C. Similarities between the two approaches

Let us consider separately first a statistical approach and then a symbolical approach to anomaly detection, to see what they have in common.

In statistical anomaly detection the performance depends critically on the features that are modeled. For example, if only the speed and heading of vessels are modeled, only vessels with anomalous speed and heading will be detected. This is clearly inadequate for finding the more intricate movements and relations involved in various maritime activities of interest, as for example smuggling, hijacking, or environmental threats. Therefore a major task in designing an anomaly detection system for surveillance is to select a number of suitable features that are able to catch the kind of behaviors and activities we would like to detect. This has to be done in collaboration with domain experts. The resulting features may require rather elaborate computation to derive from the raw data. The calculation of these feature values are represented by the left box in Figure 2.

The next step is to select statistical models for the features (the middle box of the figure). Typically they must reflect that there are different categories of vessels, and possibly other circumstances that affect the traffic. The statistical models are trained on data from a selected period and subset of comparable vessels, and then used to evaluate how anomalous the vessels are in the current situation.

Finally, the anomalies found must be presented and visualized in a way suitable for the user. The basis for this presentation is put together in the rightmost box in the figure: explanations for the anomalies in terms of involved features and time spans, expected values versus actual values, statistically allowed ranges, additional information about the involved vessels, etc.

Now let us consider a purely symbolic system, as illustrated in Figure 3. The leftmost box represents the relation extractors, which compile a number of primitives interesting for maritime surveillance. These are the primitives that the rules may refer to, such as categories of vessels, changes of speed and course of the vessels, whether the water is shallow, whether vessels approach each other or ports or shallow waters, etc. These have been designed in collaboration with domain experts to cover relevant behaviors.

The middle box is the reasoner, which has a number of rules and tries to match them to the current maritime situation. The rules are typically formulated in terms of relations, but may also refer to other rules (in a non-circular way). Effectively, matched rules are fed back as new relations, to be used by other rules.
Finally, just as in the statistical case, the matched rules should be presented to the users, including explanations for what matched and why. This information is prepared in the rightmost box.

Although there is a huge conceptual difference between the methods behind statistical and symbolic anomaly detection, due to their stemming from different disciplines, it is clear from the picture that there are significant similarities in the process: Both require relevant relations/features of the domain, both generate matches/indications and both must deliver timely explanations and information to be presented to the users. This leads us to the joint system.

D. System Overview

An overview of the internal modules in the anomaly detection system is provided in Figure 4. The main characteristics of these modules are described in the following.

The anomaly detection system is managed by the operators using the Management User Interface. By this interface both
symbolical and statistical rules may be configured using a simple graphical language. Additionally, by using the management user interface, the overall performance of the system could be monitored.

The Relation and Feature Extractors are used to hide the specifics regarding different types of data from the symbolic situation reasoner and the statistical anomaly detector. Each detected relation may be used for triggering a symbolic rule or for providing data for the statistical anomaly detection. The relations thus constitute predefined building blocks, or primitives, by which it is possible to design symbolic or rules or statistical models. In the general case, a relation connects a subject with an object (e.g., the subject is an instance of an object, or the subject is approaching an object). In some cases, only a subject is needed (e.g., the subject is changing speed).

The Symbolic Reasoner detects when all conditions are fulfilled in order to satisfy a symbolic rule:

- All relations according to the rule must be present within a certain time frame.
- The conditions regarding which subjects and objects that are involved in the relations must be matched.
- The time constraints between the relations must be matched.

The number of potential situations to be tested grows very fast when there are more than one relation in a rule. In order to quickly dismiss hypotheses, the symbolic reasoner is optimized to find at least one condition that is not satisfied as fast as possible.

The Statistical Anomaly Detector maintains statistical models over the features selected for anomaly monitoring, and computes anomaly values when new samples arrive. An anomaly value above a threshold, corresponding to a desired significance level, generates an anomaly indication.

The Visualization Presentation module collects all necessary information regarding a symbolic or a statistical anomaly indication to be transmitted to the surveillance system. The message includes: the name of the rule and a short description of it; the anomaly value; lists of involved relations and entities; and, as specified in the rule, the means for how to present the indication together with a list of operators or groups of operators that should have access to it.

IV. **Synergies Between the Statistical and Symbolic Approaches**

A. **Exploited Similarities**

One obvious synergy between the two approaches is to take advantage of the similarities, according to the discussion in the previous section. The Joint Statistical and Symbolic Anomaly Detection System depicted in Figure 4 thus uses a number of relationships between the two approaches in order to present an integrated solution. By designing unified principles for the main information flows to and from the Symbolic Situation Reasoner and the Statistical Anomaly Detector respectively, the system architecture and the main modules for management, relation/feature extraction, and visualization preparation, could be shared between the two. By exploiting these possibilities the development and maintenance costs of the system will be significantly lower, but above all, it will be much easier to learn how to configure the symbolic and statistical rules and how to combine the two approaches. When trying out a new rule, the flexibility to select any of the two approaches together with the possibility to use them together may be invaluable.

**Figure 5. An example of an anomaly rule for detecting series of unusual changes in velocity**

B. **Symbolic Indications as a Basis for Statistical Reasoning**

As mentioned above, it is important that the features of the statistical models are appropriate for characterizing interesting properties of the domain. Since the relations used in the rules are also selected as relevant for the domain, it is straightforward to use these relations as features in the statistical models. Figure 5 shows an example of this, where a statistical model is created that counts the number of turns and speed changes of each vessel, and singles out those with a significantly different frequency of those events than the others. Note also that we in these figures use the same notation for symbolical rules and statistical models, such that the user need not bother about the difference: A symbolical rule would just have the expression "fixed thresholds" to the right of the bars, which indicates that there are fixed limits for what constitute a turn or a speed change, rather than the expression "unusually freq." which indicates that there is a statistical limit for how often they occur.

Even more interesting, though, is the observation that when the user has formulated a new rule, this too is supposed to indicate some interesting property of the domain, and thus also could be used as an input feature for statistical consideration. By just checking a box the user could say that in addition to (or instead of, if that is preferred) generating an alert for every match of the rule, the number of matches per vessel is counted and when some vessel shows an unusually high (or low) number of matches an alert is generated. Many times it is interesting both to get an alert every time something happens, and to have a long term follow-up to find out which vessels triggers it the most often. Everyone may have bad luck now and then and accidentally trigger an alert, but those that do so persistently can not blame bad luck alone. One example is a rule that monitors a speed limit in some area. The rule may easily catch every single speeding offender. If a statistical detector is put on top of the rule, it will instead detect those that...
repeatedly and systematically run to fast, ignoring those that only occasionally exceed the speed limit.

C. Statistical Indications as a Basis for Symbolic Reasoning

A symbolic rule in the proposed anomaly detection system requires that all conditions are satisfied before an indication is issued. To create a viable rule it is in some cases required to allow rather relaxed conditions for triggering a relation. To reduce the number of false alerts caused by a high frequency of these relations, it may be advisable to complement the rule with a requirement for unusual behavior.

Figure 6. An example of a symbolic rule for detection of a vessel that has run aground

One example of this is how to detect a vessel that has run aground. A symbolic rule determining a low velocity in shallow waters may not be sufficient since there may be routes where vessels travel or anchor despite the information provided in the sea chart. To reduce the number of false detections, the symbolic rule should thus be complemented by a condition that the vessel must follow an unusual route, as indicated by a statistical anomaly detector.

Figure 6 shows an example of such a symbolic rule requiring five relations: The first two relations from above are ontological relations used to define which kind of entities that are affected by the rule. The third relation states that the vessel must take a route that deviates from the trajectories of other vessels. The measure for this distance is the maximum distance to the most similar trajectory (for further explanation, see [6]). The remark ‘unusual value’ means that this distance must be unusual compared to what is normal. If, instead ‘fixed value’ were used, a threshold for the allowed distance would have been required. The fourth relation in the rule states that the vessel must be present in any area of the type ‘Shallow Water’. The remark ‘fixed value’ means in this case that there are some fixed parameters defining the threshold for what is meant by ‘in area’, in this case for how long time the entity must be present in the area. The fifth relation defines that the vessel must travel slowly.

In addition some other conditions apply to this rule: The time frame specifies that the complete situation must have occurred within 1 hour. Finally, the time constraints connecting the last three relations (denoted ‘intersects’), mean that at some point in time all three relations must exist concurrently.

D. Comparable Anomaly Values for Statistical and Symbolic Indications

Anomaly values for statistical methods are typically related to the significance level of rejecting the hypothesis that the situation is normal. This in turn is related to the false alarm rate, i.e., the probability that a normal situation would generate an alert by an unfortunate coincidence.

It should be possible to use an analogous approach to calculate anomaly values also for symbolic rules. As explained in Section III, a symbolic rule specifies a set of relations that are required and a set of further conditions regarding which entities that are involved in the relations and the timing between the relations. Assuming that a valid combination of such relations (i.e., for which all conditions are satisfied) has been detected, there are two possible hypotheses: either these relations have been generated by the type of behavior that we had in mind when the rule was created, or they have, by chance, been generated by some other behavior. As we do not know the characteristics of this other behavior we assume that the appearance of the different relations will be uncorrelated. Thus, by measuring the frequency of the different relations and by estimating the expected frequency of valid combinations caused by these, we have the basis for calculating anomaly values for symbolic detections as well.

If the anomaly values for the statistical and the symbolic detections could be unified, it will be possible to provide a graded output that has the same meaning for the operator regardless of which method that has generated the anomaly indication. This will be very useful for a joint approach as presented in Section III.

V. CONCLUDING DISCUSSION

We have shown that symbolic and statistical anomaly detection can be successfully combined. There are two basic ways of combining them. The first way is to use the rules as features in the statistical model, for example by counting the number of times a rule applies to each object. The second way is to use indications from a statistical detector as input to a rule, such that the rule triggers only for objects that have already turned out to be unusual in some way. Furthermore, there are additional advantages in the joint approach, in that the symbolic and statistical parts can use the same features and the same configuration interface.

From the user perspective, statistical and symbolic anomaly detection fit conceptually well together. The user can turn on or off either rules or statistical models for monitoring different aspects, often without actually knowing whether they are statistical or rule based or a combination. Both result in similar types of alerts or indications which can be visualized alongside each other in a similar way.

It may be argued that there is an important difference in that the statistical anomaly detection can give a graded output whereas a rule either applies or not. However, it is often
advisable to use a hard threshold for the statistical anomaly detection for when a situation is considered sufficiently unusual, where this threshold is used to control the number of false alerts. This means that in practice the output is binary also from the statistical anomaly detection. On the other hand, as we have argued above, a graded value can be calculated also for the significance of a symbolic rule.

A misconception with the statistical approach is that, since it uses probabilities, there is always a risk that important situations will be missed. However, there is no guarantee that all interesting situations match a symbolic rule either. Indeed, a symbolic rule should be tuned to balance the amount of missed and false alerts. Thus, the statistical and rule based approaches are, when correctly configured and used, comparable in this regard.

There is an opposite misconception that with statistical anomaly detection it is possible to detect completely new situations that nobody has conceived of beforehand and therefore not written any rules about. This is partially true, but, as discussed above, only unusual situations with regard to the statistically modeled features can be detected. Once a feature is recognized as important to monitor, it can be monitored either by a rule or a statistical model.

Still, there are some differences, both conceptual and practical. From the user's perspective, for example configuration is somewhat different. A rule may often contain parameters that must be set by the user, as for example a speed limit such that an alert is generated if that speed is exceeded. The statistical detector on the other hand will typically set such limits based on historical data, such that an alert is generated for unusually high speeds instead. So the user need not know the exact limit, but must on the other hand specify a time window or subset of objects to compare the speed with to find out what is normal.

Another difference is that a rule typically focuses on a specific situation, whereas a statistical model may consider a larger time span. A symbolic rule may catch something every time and immediately when it happens, whereas the statistical model considers the number of hits integrated over a longer period but ignores the one-time offenders.

In general, a symbolic rule may be very specifically tailored to catch a certain situation, whereas a statistical model is typically broader, looking at a longer time span and also considering features with more vague information. This is what makes the combination of the two principles useful and important. No single technique can in itself detect all interesting situations. A joint solution such as the one presented here will reach further than either symbolic or statistical models by themselves. As we have shown, the two techniques take advantage of each other to make the combination even more powerful than if they are merely used in parallel.

**ACKNOWLEDGMENT**

This work was financed by MSB, the Swedish Civil Contingencies Agency, as part of the "Statistical Anomaly Detection and Visualization for Maritime Domain Awareness" project.

**REFERENCES**


[15] X. Li, J. Han, S. Kim, H. Gonzalez. ROAM: Rule- and Motif-Based Anomaly Detection in Massive Moving Object Data Sets, Proceedings of the Seventh SIAM International Conference on Data Mining, April 26–28, 2007, Minneapolis, Minnesota, USA


