Anomaly detection for sea surveillance

Rikard Laxhammar
Saab Systems
Saab AB
Järfälla, Sweden
rikard.laxhammar@saabgroup.com

In this paper, unsupervised clustering of normal vessel traffic patterns is proposed and implemented, where patterns are represented as the momentary location, speed and course of tracked vessels. The learnt cluster models are used for anomaly detection in sea traffic. The Gaussian Mixture Model is used as cluster model and a greedy version of the Expectation-Maximization algorithm is used as clustering algorithm. The models have been trained and evaluated using real recorded sea traffic. A qualitative analysis reveals that the most distinguishing anomalies found in the traffic are vessels crossing sea lanes and vessels traveling close to and in the opposite direction of sea lanes. In order to detect complex anomalies involving multiple vessels and/or behavior that develop over time, a more sophisticated pattern model should be developed. Yet, the generality of the proposed model is stressed, as it is potentially applicable to other domains involving surveillance of moving objects.

Keywords: Anomaly detection, sea surveillance, unsupervised clustering, Gaussian Mixture Models, Greedy Expectation-Maximization.

1 Introduction

The situation picture displaying representations, "tracks", of real objects like vessels over a map, is a crucial component in many sea surveillance centers. The tracks show the objects' current position, course, speed, and sometimes more data like identity and history. The art of producing the tracks using data from radars and other sensors has been developed by many universities and companies, including Saab, over many years.

A major problem in sea surveillance is that the amount of tracks may be very large and difficult to monitor with limited operator resources. To facilitate the work, research is being carried out concerning automated interpretation of the situation picture, in order to increase the operators' situation awareness, and in particular, to draw his or her attention to situations of interest.

Generally, in the context of civil security and wide area surveillance, the vast majority of tracking and surveillance data is associated with routine events which represent an ambient background that is of no interest to the supervisor. Modern threats, often referred to as asymmetric threats, exploit this, as they are camouflaged to a larger extent and hide in the background, thus making it even more difficult to detect them.

Through usability studies performed by Saab at the sea surveillance centre in Malmö, Sweden, typical surveillance scenarios have been identified where an automatic surveillance system has the potential to be a useful support for the operators. According to the study, a general problem is the detection of abnormal traffic patterns that could be related to speeding, prohibited anchoring, grounding, sea drunkenness and other criminal or dangerous activities. Furthermore, operators pay special attention to identifying particular scenarios and behaviors that develop over time that may involve multiple objects, such as smuggling and fish poaching.

The kind of processing we discuss belongs to Level 2 of the well known JDL model [1], called Situation Assessment (or Situation Refinement). It typically involves finding relations between objects, and between objects and the environment. Sometimes the operator knows exactly what situations to look for, and is then able to define rules for them, see e.g. [2][3]. In other cases, the operator looks for situations that deviate from the normal in an unspecific manner, which is the main topic of this paper.

1.1 Top-down template based approaches to situation assessment

Rule-based expert systems [4 *et al.*] and Bayesian networks [5 *et al.*] have been popular computational approaches to situation assessment throughout the years. Common for these approaches is the explicit definition of models, rules and templates for particular events and situations that are identified through a top-down goal driven pattern matching and reasoning. At Saab Systems, a prototype for a rule-based expert system, based on an ontology for situation assessment in the domain of sea surveillance, has been developed [3]. The system is able to identify a number of basic spatial and kinematical relations between objects, and then deduce different situations, e.g. smuggling, hijacking and piloting. It is demonstrated in real-time sea surveillance scenarios, using real recorded data that has been injected with simulated data corresponding to the vessels involved in the situations mentioned above.

Yet, accurately characterizing a priori all events and situations, which may be of interest for the operator, is usually a very difficult task. The set of available examples for each particular event or situation may be very limited, as the events and situations sought for occur relatively rarely and may vary significantly from one case to another. In the context of sea surveillance, operators may face more or less unconventional adversaries with unknown or rapidly changing doctrines.

However, turning it the other way round, these and other rare events and situations can be detected as anomalies with respect to a model of routine behavior. Usually, a large amount of data corresponding to routine behavior is available, which motivates the use of bottom-up data driven techniques for building models of normal behavior.

1.2 The concepts of anomalies and anomaly detection

According to Wikipedia [6], "an anomalous phenomenon is an observed event which deviates from what is expected, an anomaly, according to existing rules or scientific theory …anomaly detection may refer to an unsupervised data mining technique that produces a data mining model for identifying cases that deviate from the norm in a dataset". Holst [7] defines anomaly detection as "a method for separating an often inhomogeneous and hard characterized minority of data from a more regular majority of data, by studying and characterizing the majority, so that data in the minority appears as deviations from the patterns found in the majority". Holst also stresses that the concept of anomaly detection says something about an attempt to *detect something*; it does not say anything about *what* exactly we are actually trying to detect. A similar definition of anomaly detection is suggested by Portney [8] where "anomaly detection approaches build models of normal data and then attempt to detect deviations from the normal model in observed data". Common to these definitions is the concept of a model of normal data which is used to discern anomalous data.

At Saab, the scope and purpose of a system for anomaly detection is to aid a potentially overloaded supervisor in detecting threats, accidents and crimes as early as possible, enabling preventive counter measures to be taken. Yet, it is still up to the supervisor to follow up system alarms, make an assessment and a decision regarding suitable actions.

1.3 Previous work

A common method used in the context of anomaly detection is data clustering [8, 9, 10, 11, 13], which can be regarded as a form of unsupervised learning. The method involves automatic grouping of a data into multiple clusters according to distinguishing features. Assuming that the data set reflects what is considered more or less normal, the resulting set of fairly large clusters is regarded as a model of normalcy. New data presented to the model is regarded as more or less anomalous based on the distance to the nearest cluster, i.e. points located close to a cluster are considered normal, while points ending up far away from all clusters are considered anomalous.

Fundamental to clustering is the feature model, i.e. the representation, of the data in which we want to detect anomalies; what characteristics of the data we chose and how we model these characteristics. As in the case of generic classification, it is important to choose a suitable set of features that adequately distinguish between different relevant categories present in the data; in this case normal or anomalous behavior.

Generally, feature models of vessel motion can be divided into layers according to the level of abstraction and degree of locality in space and time. Holst [7] suggest a simple local feature model for vessel motion, based on the momentary velocities in latitude and longitude direction within a particular area. The whole surveillance area is first discretized by introducing grid. Velocities of vessels present in the training data within each square of the grid are then modeled by a single two-dimensional Gaussian distribution. Anomaly detection is performed simply by calculating the likelihood of a new point belonging to the normal distribution; if the likelihood is below a certain threshold, the point is regarded as anomalous.

Rhodes and his colleagues have proposed and implemented a similar approach where normal vessel speeds for different regions in a port area are learned by clustering, based on a Fuzzy ARTMAP neural network architecture [11]. New data that is not recognized by the network during online operation is considered anomalous. The same research group has also proposed and implemented associative learning of motion patterns for anomaly detection, where associative neural networks learn to predict future vessel location given a current location [12]. Such predictions can later be compared to actual measurements in order to detect anomalies.

Kraiman suggest the use Self-Organizing Maps (SOM) to find cluster centers in a high-dimensional feature space of normal data [10]. A Gaussian Mixture Model (GMM) is then used as a statistical model of normal data, where the location of each individual multivariate Gaussian distribution is determined by the corresponding cluster center found by the SOM, and the variance is given by the dispersion of the training data around each cluster center. Anomaly detection in new data is done based on a Bayesian analysis and the learned GMM. Similar to the previous work, it appears as if the feature model actually implemented is limited to the speed, heading and location of each vessel.

Features of vessel motion can also be analyzed over time by considering trajectories. By clustering similar trajectories corresponding to regular traffic, a model of normal vessel routes can be constructed [13]. Furthermore,

by extracting local events corresponding to maneuvers in the motion patterns, it may be possible to characterize more abstract features of the motion [9]. An example of such model is briefly presented and discussed in the future work section of this paper.

2 Method

Inspired by the approach proposed by Holst, we take a probabilistic approach to anomaly detection by building a statistical model of recorded vessel traffic, where feature values of training data are modeled by complex probability distributions. Anomaly detection in new data is performed by calculating the likelihood that it is generated by the probability distributions; if the likelihood is below a certain alarm threshold, the point is considered anomalous.

2.1 Proposed feature models

Conceptually, the challenge when constructing a system for anomaly detection is how to represent the data in which anomalies are to be found, i.e. how to find an appropriate feature model that captures the "right" type of anomalies. In the case of sea traffic surveillance, a critical aspect is how vessel motion can be parameterized in a clever way. In this paper, two feature models are proposed an implemented for anomaly detection.

The first model corresponds to the Holst model referenced earlier, where the surveillance area is divided into a grid in which each square models the vessel velocities in latitude and longitude direction in that particular area. This model, here referred to as the *base model*, captures anomalies that correspond to vessels traveling in anomalous directions and/or at anomalous speeds. However, the model does not capture anomalous correlations between speed and position within each square. Consider for example the obvious anomaly of a vessel traveling the wrong direction in a two-way sea lane. Because the vessel has a speed and course similar to the regular traffic on the *correct side* of the sea lane, it will not be detected as an anomaly as its speed and course are not correlated to its position within the area.

The second model, referred to as the *extended model*, is an extension of the base model that incorporates the spatial position; this gives us a four-dimensional feature space that captures correlations between speed and position. Theoretically, we could have this model covering the whole surveillance area. However, when surveying a large area, the relatively large number of cluster components required to adequately model local features of the widely scattered training data in the high-dimensional feature space may pose serious constraints regarding computational feasibility. Therefore, the surveillance area is discretized as for the base model, where each square has its local model. When determining a suitable grid resolution, it is important to find a good balance where resolution is sufficiently high for efficiently capturing local features of data, while being low enough to include a fair amount of training data in each square.

The chosen feature models are relatively simple but are thought to serve as a convenient base for technically investigating anomaly detection within sea surveillance. The type of anomalous behavior that was thought to be captured by these models is rather elementary. Examples of such anomalous behavior could be vessels that are traveling too fast in speed restricted areas, crossing sea lanes, traveling the wrong direction in sea lanes and vessels that remain stationary in sea lanes or in areas where anchoring is prohibited.

2.2 Gaussian Mixture Models and Expectation Maximization

In the approach proposed by Holst, velocities within each region are modeled by a single two-dimensional Gaussian distribution. A serious limitation of this model is that it assumes that a single Gaussian component will cover all possible occurrences of regular data points in an adequate way. Unless the data in a particular area is very homogenous, this model is not efficient for modeling normal data. As an illustrative example, consider again the two-directional sea lane where the absolute speed is roughly the same in both directions. Normal data points in the velocity space for this area will gather in two distinct clusters, where each cluster centre corresponds to the mirror of the other. If the clusters are of roughly the same size, a single Gaussian will centre close to zero, i.e. approximately in the middle of the two clusters, and grow rather wide in order to cover both clusters. Data points located close to zero will thus be regarded as perfectly normal occurrences, which is not what we would expect in reality. Such points may correspond to vessels that have stopped in the middle of a sea lane and should thus rather be considered as potential anomalies.

In order to model regular data more efficiently, other approaches involving more complex cluster models have previously been investigated [9]. A natural extension to the Holst model is the introduction of a multivariate Gaussian Mixture Model (GMM) in place of the single Gaussian. Such a model is capable of approximating arbitrarily complex distributions in arbitrarily high dimensions and is a natural choice when there is no reason to believe that data behaves according to any particular distribution [14]. A GMM consists of a number of multivariate Gaussian distributions known as *mixture components*, where each component c has its own parameters; *mean value* μ_c and *covariance* Σ_c. In addition to these parameters each component has an associated weight π_c, where all weights are non-negative and sum to one. The problem is how to place and "stretch" these Gaussians in the feature space, i.e. estimating the parameters, so that the centre and spread of each cluster present in the training data is accurately approximated by a corresponding component distribution.

A well known technique for parameter estimation is the Expectation-Maximization (EM) algorithm [14 *et al.*], which incrementally estimates the set of parameters that maximizes the likelihood of the training data. The algorithm consists of two main steps that are performed iteratively until a certain end condition is fulfilled, e.g. some convergence condition.

During the Expectation step, the algorithm estimates for each data point x_i in feature space the probability that the point was generated by each particular component c, taking into account the component weights π_c. This is done by computing the posterior probabilities $p(c|x_i)$ for each data point x_i belonging to each component c according to Bayes Rule;

$$p(c|x_i) = \frac{p(x_i|c)p(c)}{p(x_i)} = \frac{p(x_i|c)\pi_c}{\sum_{c'} p(x_i|c')\pi_{c'}} \quad (1)$$

where $p(x_i|c)$ corresponds to the likelihood of component distribution c generating data point x_i. This expectation of point to component association is then used in the Maximization step where the estimated parameters π_c, μ_c and Σ_c of each component c are updated according to a maximum likelihood criterion, i.e. maximization. The Maximization step involves adjusting the parameters of each component in such a way that the component better fits the data points, taking the previous posterior probabilities q_{ic} into account, where $q_{ic} = p(c|x_i)$. More specifically, updating the parameters is done according to formulas (2) to (4);

$$\pi_c \leftarrow \frac{1}{n}\sum_{i=1}^{n} q_{ic} \quad (2)$$

$$\mu_c \leftarrow \frac{1}{n\pi_c}\sum_{i=1}^{n} q_{ic} x_i \quad (3)$$

$$\Sigma_c \leftarrow \frac{1}{n\pi_c}\sum_{i=1}^{n} q_{ic}(x_i - \mu_c)(x_i - \mu_c)^T \quad (4)$$

The updated model is then used to compute updated posterior probabilities in the Expectation step, and so on, i.e. the expectation and maximization steps are repeated by turns to incrementally improve the model.

However, one of the major drawbacks of the classical EM-algorithm is that it is very sensitive to initialization. Depending on the starting values of the parameters, the algorithm may, and most probably will, converge to a local optimal solution that is different from the global optimal solution [14]. Therefore it is common to perform multiple runs, restarting the algorithm with a new, more or less random, initialization set of parameters each time it converges to a suboptimal solution. The parameters and the corresponding likelihood for the data are saved for each run, i.e. for each suboptimal solution found. Finally, the solution corresponding to the maximum data likelihood is chosen.

Another drawback of the classical EM-algorithm is that it does not support any inherent mechanism for determining a suitable number of mixture components. When training data is relatively inhomogeneous, a large number of mixture components are required in order to construct an adequate model. However, as the complexity of the model increases, the risk for over-fitting also increases. Thus, finding a balanced number of mixture components may not be a trivial problem.

2.2.1 Greedy Expectation-Maximization

To solve the problem of finding an optimal number of components and avoid the need to run the algorithm multiple times from random initializations, an extension to the classical EM-algorithm has previously been developed [15]. The algorithm, known as *Greedy EM-learning*, is based on a greedy approach that iteratively builds the optimal mixture model adding new components one at a time. Instead of starting with a, more or less, random configuration of a predefined number of components and improve upon this configuration with regular EM, the mixture model is built component wise. The algorithm starts by determining the optimal one-component mixture. It then starts repeating two steps until a stopping criterion is met. The steps are; 1) insert a new component and 2) apply EM until convergence.

Before inserting a new component, a set of randomly initialized candidate components are first evaluated in order to determine the optimal new component for insertion in the current mixture model, i.e. the optimal candidate component that maximizes the likelihood of data in the new mixture. Determining the optimal candidate component is done by partial EM searches, one for each candidate of the candidate set. For details regarding this process, the reader is referred to [15].

To evaluate performance of the current mixture model, the likelihood of an uncorrelated validation set is calculated after each new component insertion and EM process. If the likelihood has decreased since the previous insertion, our stopping criterion is fulfilled and the algorithm terminates, returning the previous mixture model as solution. Should the number of mixture components exceed a certain predefined threshold, the algorithm also terminates, returning the current mixture components.

3 Experimental evaluation

Considering previous work in the domain of sea surveillance [7, 10, 11, 12, 14], there appears to be no well established approach to evaluate a system for anomaly detection. In particular, there is no common benchmark, e.g. a well established and well defined set of maritime

scenarios that should be regarded as anomalous by a system for anomaly detection. Given a benchmarking set where each sample is labeled as positive or negative, i.e. anomalous or normal, we could estimate the system's rate of false alarms based on the number of samples classified as positive negatives and the rate of missed alarms based on the number of samples classified as negative positives. However, besides the fact that an adequate benchmarking set may not be available, we could also argue that this is, in principle, not a feasible approach to estimate the systems ability to detect anomalies. The reason for this is that we in some sense are biased towards evaluating the systems ability to detect particular and well known situations, i.e. where are rather evaluating the system from a top-down goal driven perspective.

In this paper we have evaluated and analyzed the systems ability to detect anomalies from a bottom-up perspective, similar to that of Kraiman [10]. This involves combining a quantitative and qualitative analysis in the sense that the character of the statistically most distinguishing anomalies is manually examined, where the anomaly threshold is set to a level where the estimated rate of false alarms in training data is very low.

3.1 Data description

The surveillance data available in this experiment has been supplied by the Swedish Naval intelligence battalion and consists of recorded sea traffic at the Malmö sea surveillance centre, located in the south of Sweden. The data set contains sea traffic along the coast of south Sweden and parts of the neighboring coasts of Denmark, Germany and Poland and the sea in between. The main parts of the data consist of approximately one week of recorded summer traffic and one week of recorded autumn traffic. In addition, six shorter recordings, spread out over the year, each having a duration of a few hours, were also supplied. The recorded data is assumed to reflect more or less typical vessel traffic. The information in the recordings is stored as vessel reports, where each report includes attributes such as target ID, position, speed, course, timestamp and AIS[1] number (if available).

3.2 Data sets and parameters

One week of traffic was used for training and another week for validation; recall that greedy EM requires a validation set to evaluate the current performance during training. Ideally, in order to get a good estimation of model performance, the training set and validation set should not be correlated. Therefore, the summer recording is used for training while the autumn recording is used for validation. Data from the six shorter recorded scenarios have been used as the test set for evaluating anomaly detection based on the trained models.

Grid size is arbitrarily set to 30 squares in latitude direction and 40 squares in longitude direction. This size is found to be good enough in the sense that the number of training data points in each square is sufficiently high while the complexity of the mixture models is kept sufficiently low.

When training the GMM with greedy EM, the maximum number of mixture components was set to 20. However, this number of components was never reached during training. The number of candidate components per mixture component during insertion was set to 10.

Because the recorded scenario data is assumed to reflect typical traffic patterns, one would expect an anomaly detection system to detect very few, if any, anomalies in this data. Therefore, the anomaly likelihood threshold for each of the two models has been set to a level that generate approximately 0.1% anomalies in the total validation set.

3.3 Results

Let A_1 and A_2 be the total set of test points classified as anomalous by the base model and the extended model, respectively, and let D be the total set of test points. Then, $|A_1|/|D|=0.13\%$ and $|A_2|/|D|=0.10\%$. A degree of similarity of the two sets of anomalous points is calculated according to (5):

$$S(A_1, A_2) = \frac{|A_1 \cap A_2|}{|A_1 \cup A_2|} = 56{,}86\% \qquad (5)$$

This indicates that there is a considerable overlap in the anomalies detected by each model.

In the following figures 2-5, we present qualitative results for anomaly detection in selected areas where anomalies are either jointly detected by the two models or exclusively detected by either one of them. Data points are represented as vectors positioned in the longitude and latitude space. The position, size and direction of the vector correspond to the vessels location, speed and course, respectively. The color coding for the traffic is as follows;

- *Blue* traffic corresponds to the models *training data*.
- *Green* traffic corresponds to the test data that is classified as *regular* by the model.
- *Red* traffic corresponds to the test data that is classified as *anomalous* by the model.

[1] **A**utomatic **I**dentification **S**ystem (AIS). For information on AIS: http://www.imo.org

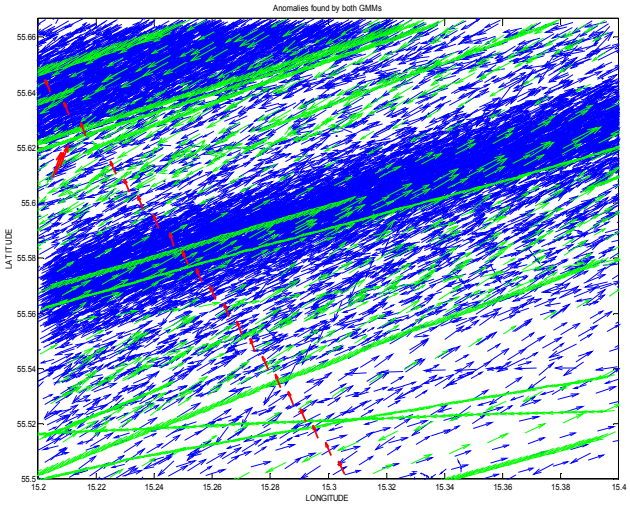

Figure 1: The main two-way sea lane is clearly illustrated by the high concentration of blue traffic in two opposite directions. A minority of the traffic travels in parallel to the main sea lane, but still follows the general direction of motion. However, the anomalies, jointly detected by the two feature models, correspond to a vessel traveling in an anomalous direction as it crosses the direction of travel.

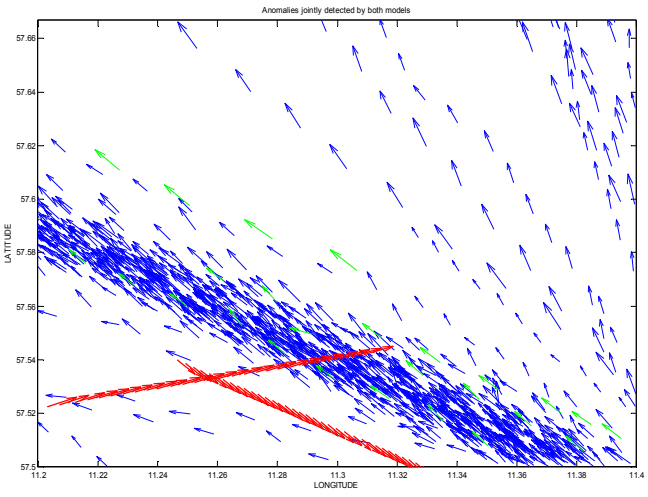

Figure 2: The majority of the tracks of training set are concentrated to the sea lane going in north-west direction while a minority of them deviates from it. Two vessel tracks are jointly detected by the models as anomalous; the first traveling close to the sea lane but in the opposite direction and the other crossing the sea lane in a narrow angle.

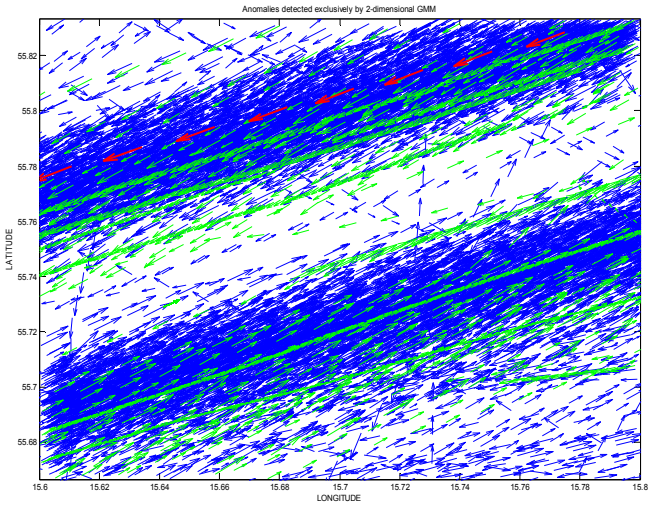

Figure 3: Similar to the previous figure, a two-way sea lane is clearly illustrated. The anomalies, in this case exclusively detected by the base model, correspond to a vessel traveling in a sea lane but at an anomalously high speed, indicated by the length of the speed vector.

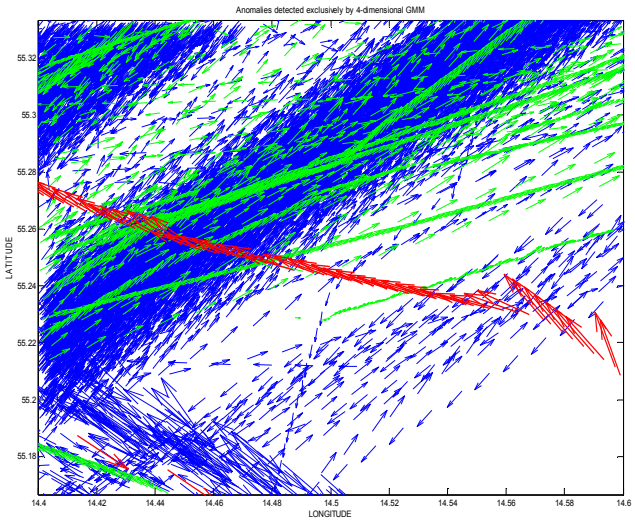

Figure 4: A substantial amount of traffic appears to cross the main sea lane at bottom-left part of the area. However, the anomalous track, exclusively detected by the extended model, clearly distinguish itself as a vessel crossing the main sea lane at an anomalous location and at a relatively high speed.

4 Analysis and discussion

Considering the quantitative results, we observe that the rate of anomaly detections for both feature models correspond well to what we would expect; the test set is assumed to reflect typical traffic, similar to the validation

set, so we would expect it to generate approximately the same rate of anomalies. The intersection of the two sets of anomalous points constitutes about 57% of the corresponding union set, indicating that the two models are complementary to some extent. If the goal is to detect a wide range of anomalies, we might benefit from combining the results from the models.

Examining the results qualitatively, it is found that the most distinguishing anomalies, jointly detected by the feature models, correspond to vessels that are crossing sea lanes and vessels travelling close to and in the opposite direction of sea lanes, e.g. Figure 1 and Figure 2. These anomalies appear rather clear in contrast to the normal data. The location and extension of the major sea lanes are often easily identified. However, information regarding the normal velocities in the sea lanes is less transparent as the high concentration of data vectors makes them rather cluttered. Considering Figure 4, we see that the pattern exclusively considered as anomalous by the extended model correspond to a vessel crossing the main sea lane at a relatively high speed. Yet, there is a substantial amount of tracks in the training set that also cross the main sea lane, but at another part of it, i.e. down in the left corner. This suggests that the base model regards the pattern as normal because it resembles patterns from the training set; recall that the base model learns normal velocity vectors regardless of their position within the area. This supports the prior hypothesis that the extended model is more sensitive to the velocity vector in relation to the spatial position within each particular area.

One of the main issues when configuring a system for anomaly detection is how to find an appropriate anomaly threshold, regulating the systems level of sensitivity. In the case of the GMM, the likelihood threshold corresponds to the anomaly threshold. Raising this value has the effect of making the system more sensitive as it finds more anomalies in data. However, it also implies that the rate of false alarms will increase as the system tends to find more anomalies that are of no interest for an operator. On the other hand, if the threshold is lowered, the system might dismiss more subtle anomalies that are in fact of high interest for an operator. Thus, the anomaly threshold or level of sensitivity highly influences the usability of a system for anomaly detection. To enhance the systems performance, the operator should be able to dynamically adjust the threshold during system operation.

The models implemented in this project are rather limited in the sense that they only consider momentary states of the vessel motion, i.e. without considering previous states. Furthermore, the states of the surrounding vessels are not considered, e.g. spatial relations in time between vessels. This fact implies that anomalies related to situations that develop over time and may involve multiple vessels, e.g. smuggling and hijacking, are difficult to find by the implemented models. However, the simplicity of the feature models makes them rather general, applicable to any domain involving motion in the two-dimensional plane, requiring no particular domain knowledge.

4.1 Future work and improvements

Given the limitations of the current feature models, a natural extension would be a more sophisticated feature model. A complementary feature model based on counting events corresponding to particular maneuvers in the motion pattern within a limited time window has previously been proposed [9]. In particular, vessel trajectories are segmented where each segment corresponds to a particular type of maneuver, characterized by a number of kinematical features. Within a sliding time window, the number of segments of each type is counted, generating a data point in a high-dimensional discrete feature space where each dimension corresponds to the number of occurrences of a particular maneuver (i.e. segment type). As an example, we might consider a seven-dimensional space where the features are the number of 1) straight segments 2) weak yaw segments 3) sharp yaw segments 4) brake segments 5) acceleration segments 6) stop segments and 7) irregular segments. The hypothesis is that clusters in this high-dimensional space correspond to typical maneuver patterns. The clusters could be represented by a mixture of multivariate Poisson distributions that model the expected number of occurrences of each maneuver within each cluster. To estimate the parameters of the Poisson mixture, an adapted version of the EM-algorithm may be used, similar to the case with the GMM. The Poisson distribution has the advantage that it is defined by a single parameter, compared to the Gaussian that is defined by its mean and variance. This implies that the Poisson distribution does not run the risk of collapsing, like the Gaussian distribution, during the EM algorithm as the variance of the Gaussian approaches zero. An alternative to the Poisson mixture model is to introduce a Hidden Markov Model (HMM) that treats the different types of segments as states of the vessel motion. By using a HMM for modeling sequences of segments, the likelihood of an observed sequence of maneuvers can be calculated, thereby identifying more or less anomalous sequences of maneuvers.

As mentioned earlier, the operator should have the ability to regulate the level of false alarms by explicitly adjusting the anomaly threshold. Yet, a complementary and potentially more effective way to enhance system performance and suppress the rate of false alarms would be to introduce on-line supervised learning, offering the operator the option of either confirming or rejecting anomaly alarms during system operation. If the operator chooses to reject the alarm, the data that generated it is assumed to be normal and incorporated into the normal model. Should the operator confirm the alarm, the system should store the anomalous pattern, e.g. by updating the knowledgebase of a rule-based expert system.

5 Conclusion

In this paper, algorithms for unsupervised clustering of normal sea traffic patterns have been proposed and implemented, where the learnt models are used for anomaly detection in sea traffic. Two feature models of the vessel motion have been used during clustering; a two-dimensional model based on the momentary vessel velocities in the two-dimensional plane and the other a four-dimensional extension of the base model incorporating the momentary position. The multivariate GMM have been used as cluster model and a greedy version of the EM algorithm has been used as clustering algorithm.

The implemented models have been trained and evaluated using recorded sea traffic. Quantitative results show that there is a considerable difference regarding the set of anomalies detected by the two feature models. A qualitative analysis reveals that the most distinguishing anomalies found in the typical routine traffic correspond to vessels that are crossing sea lanes and vessels that are traveling close to and in the opposite direction of sea lanes. Furthermore, results indicate support for the hypothesis that the extended feature model is more sensitive to anomalous correlations between the velocity vector and the spatial position of vessels.

The detected anomalies are of a rather elementary nature; the type of feature model essentially determines the character of the detectable anomalies. Therefore, a more sophisticated feature model is suggested for future work. Furthermore, to enhance system performance and suppress the rate of false alarms, we suggest the introduction of online supervised learning.

The generality of the proposed model should be stressed, as it is applicable to other domains, involving generic motion in the two-dimensional plane, requiring minimal adaptation and no specific domain knowledge as the algorithms are based on unsupervised learning.

References

[1] U.S. Department of Defense, Data Fusion Subpanel of the Joint Directors of Laboratories, Technical Panel for C3, "Data fusion lexicon," 1991

[2] J. Edlund, E. Sviestins, *An Agent Based Approach to Situation Assessment*, Proceedings of MilTech2, pages 69-76, FHS, Stockholm, Sweden, October 2005.

[3] J. Edlund, M. Grönkvist, A. Lingvall, E. Sviestins, *Rule-based situation assessment for sea surveillance*, Proceedings of SPIE Vol. 6242 Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006, Belur V. Dasarathy, Editor, 624203 (Apr. 18, 2006).

[4] C. Matheus, M. Kokar, K. Baclawski, J. Letkowski, C. Call, M. Hinman, J. Salerno and D. Boulware, *Lessons Learned From Developing SAWA: A Situation Awareness Assistant*, In Proceedings of FUSION'05, Philadelphia, PA, July, 2005.

[5] S. Das, R. Grey, P. Gonsalves, *Situation Assessment via Bayesian Belief Networks,* Proceedings of the 5th International Conference on Information Fusion, Annapolis, Maryland, July, 2002.

[6] www.wikipedia.org

[7] A. Holst, J. Ekman, *Anomaly detection in vessel motion*, internal report Saab Systems, Järfälla, Sweden, 2003.

[8] L. Portnoy, E. Eskin, S. Stolfo, *Intrusion Detection with Unlabeled Data Using Clustering*, Proceedings of ACM CSS Workshop on Data Mining Applied to Security, November 5-8, 2001.

[9] R. Laxhammar, *Artificial Intelligence for Situation Assessment*, Masters thesis at the School of Computer Science and Engineering, Royal Institute of Technology, Sweden, 2007.

[10] J.B. Kraiman, S.L. Arouh, M.L. Webb, *Automated anomaly detection processor*, Proceedings of SPIE Vol. 4716, p. 128-137, Enabling Technologies, for simulation science VI , July, 2002.

[11] Rhodes B.J., Bomberger N.A., Seibert M.C., Waxman A.M., *Maritime situation monitoring and situation awareness using learning mechanisms*, Military Communications Conference 2005, Atlantic City, NY, USA, October 17-20, 2005. (Presented at the workshop on Situation Management (SIMA)).

[12] B. J. Rhodes, N. A. Bomberger, M. Zandipour, *Probabilistic Associative Learning of Vessel Motion Patterns at Multiple Scales for Maritime Situation Awareness*, The 10th International Conference on Information Fusion, Quebec, Canada, 2007.

[13] Dahlbom A., Niklasson L., *Trajectory Clustering for Coastal Surveillance*, The 10th International Conference on Information Fusion, Quebec city, Canada, 9-12 July, 2007.

[14] Veerbeek J. J., *Mixture Models for Clustering and Dimension Reduction*, PhD thesis, University of Amsterdam, 2004.

[15] Verbeek J.J., Vlassis N., Kröse B., *Efficient Greedy Learning of Gaussian Mixture Models*, Neural Computation, 15(2):469-485, 2003.