ANOMALY DETECTION IN VESSEL TRACKING – A BAYESIAN NETWORKS (BNs) APPROACH

(DOI No: 10.3940/rina.ijme.2015.a3.316)

D Handayani, Department of Computer Science, Faculty of Information and Communication Technology, International Islamic University Malaysia, **W Sediono**, Department of Mechatronics Engineering, Faculty of Engineering, International Islamic University Malaysia and **A Shah,** Department of Information Systems, Faculty of Information and Communication Technology, International Islamic University Malaysia

SUMMARY

The paper describes the supervised method approach to identifying vessel anomaly behaviour. The vessel anomaly behaviour is determined by learning from self-reporting maritime systems based on the Automatic Identification System (AIS). The AIS is a real world vessel reporting data system, which has been recently made compulsory by the International Convention for the Safety of Life and Sea (SOLAS) for vessels over 300 gross tons and most commercial vessels such as cargo ships, passenger vessels, tankers, etc. In this paper, we describe the use of Bayesian networks (BNs) approach to identify the behaviour of the vessel of interest. The BNs is a machine learning technique based on probabilistic theory that represents a set of random variables and their conditional independencies via directed acyclic graph (DAG). Previous studies showed that the BNs have important advantages compared to other machine learning techniques. Among them are that expert knowledge can be included in the BNs model, and that humans can understand and interpret the BNs model more readily. This work proves that the BNs technique is applicable to the identification of vessel anomaly behaviour.

1. INTRODUCTION

The number of threats facing vessels at sea, and the security of coastal countries, increases daily in the form of collision, illegal fishing, smuggling, pollution, and piracy. Some of these problems are caused by human actions and some arise from natural causes. For example, in the Straits of Malacca and Singapore, more than 150 vessels a day (over 70,000 vessels annually) transit this strategic and important international waterway. Thus, the International Chamber of Shipping (ICS) believes in placing safety and security as its priority for all nations across the globe [1].

With the advancement of technology in surveillance and the immediate need for better protection of the environment, automated solutions have become an important issue. Such solutions can be applied for detecting anomaly behaviour in moving objects, such as road vehicles, planes and vessels.

Anomaly detection of a massive moving object is one of many techniques for improving environment security, especially in surveillance [2-4]. The pattern of the moving object can become very complex which makes the work more challenging.

One of the sources of vessel movement information is data from the Automatic Identification System (AIS). Maritime surveillance authorities used AIS data to reveal threats to security, for instance, smuggling, illegal trafficking, illegal fishing or other risks. With the amount of information retrieved, the need for an automated system to analyze the vessel behaviour increases.

Some previous work was devoted to research and development in the area of anomaly detection. In 2011, Etienne Martineau [5] determined that the purposes of anomaly detection are: for manpower optimization, support in the decision making process, prediction and early notification, and maintaining a complete and continuous surface picture.

1.1 MANPOWER OPTIMIZATION

The number of vessels at sea grows every year. Aligned with this, the increasing number of pirate attacks has raised the performance expectations for security systems. It becomes more of an issue as countries reduce the number of coastal security staff.

To overcome this issue, it is desirable to combine the strengths of humans and computers. Human reasoning is superior to that of the machine but machines can process massive amount of data in a short period. Therefore, the proposed approach is to let the machine carry out routine and simple tasks leaving the complex problems to be solved by the operator (human) [6, 7]. The combination of human and machine can thus, improve overall performance.

1.2 SUPPORT OF DECISION PROCESSES

The computer is used to support the operator while monitoring the maritime traffic and reduce the operator's cognitive load. This is to improve the performance of operators, not to fully replace them. The surveillance of large sea areas typically involves the analysis of vast amount of data, and this cannot be managed and interpreted solely by humans [8].

For this reason, when the operator needs to make decisions, the system will aid the decision process by helping operators interpret the data [9].

1.3 PREDICTIONS AND EARLY NOTIFICATION

One of the aims of the anomaly detection process is to detect a threatening situation as it develops. This helps the operator to prevent such a situation from occurring or, if that can't be done, to prepare a response to it.

The prediction must be made as early as possible to give time for the operator to process the related information. For example, travelling at high speed in the wrong direction in a waterway may lead to a collision and the warning alert should be raised as soon as the situation is detected.

1.4 MAINTAINING A COMPLETE AND CONTINUOUS SURFACE PICTURE

The limitations of the human brain have been proven to have a significant impact for humans operating in dynamic environments with large quantities of information available [10, 11]. It is difficult for a human to maintain and monitor the surveillance system at all times. This kind of task can be done better by machines. The reasoning of a computer is deterministic and it has an exact memory with a large capacity. Machines can process data to maintain a constant and complete monitoring picture and notify the operator when an anomaly is detected.

Here, we used the BNs approach to identify the anomaly behaviour by developing a model that represents the normal situation. In this case, the extent of the anomaly situation is defined by the degree to which a vessel deviates from the normal situation.

In this paper, we focus on the vessel anomaly behaviour based on speed data. With an appropriate speed limit, a vessel can take effective action to avoid collision. The speed limit will also reduce emissions by up to 70% [12].

This paper is organized as follows. Sec. II is a literature review on anomaly detection. Sec. III is an overview of our approach with the theory of BNs, while Sec. IV presents the BNs based approaches to anomaly detection. Sec. V describes the simulation process. Sec. VI describes data used for the simulation process. Sec. VII presents the experimental results with discussion, and Sec. VIII presents the conclusions.

2. LITERATURE REVIEW ON ANOMALY DETECTION

In computer science, anomaly detection has been an active research topic for a long time. The advancement of research in this area provides a variety of practical examples and studies concerning classifications of techniques and research challenges. Even if anomaly detection is an immature field of research in other domains, we believe that this body of knowledge, at least at its core, can be used and applied in many areas, including maritime surveillance.

Anomaly detection is extensively studied in areas such as network security, road surveillance, video surveillance, and military surveillance [13]. The non-consistent pattern is given various names such as anomaly, outliers, exceptions, etc. [2]. In the case of the maritime surveillance domain, the diverged patterns are referred to as anomaly.

According to Kazemi (2013), the anomaly detection techniques can be divided into two groups, namely the data-driven techniques and knowledge-driven techniques [2]. Data-driven techniques determine the normal situation using machine learning or statistic algorithm to analyze the historical data [14]. Meanwhile, knowledge-driven techniques encode the expert knowledge into the system [15, 16].

2.1 DATA-DRIVEN TECHNIQUE

The data-driven technique is based on a classification that learns a normal situation using unsupervised or supervised learning. Data are considered as anomalous when they do not match the model. The data-driven technique is divided into two kinds of approach: the machine learning and statistical approaches.

2.1 (a) Machine Learning

The machine learning approach makes decisions based on the learning process from data. In the case of maritime surveillance, after the learning process, the machine learning model can be used to classify the normal and anomaly situation.

Some popular techniques belonging to this field include clustering, neural networks (NNs), support vector machines (SVMs), Bayesian Networks (BNs), etc.

- Clustering

A study done by Dahlbom and Niklasson (2007) [17] used the trajectory clustering technique for anomaly detection. In this case, the anomaly is determined by looking at the probability that the path that does not match the normal trajectory.

- Neural Networks (NNs)

The NNs use a learning algorithm inspired by the structure and function of the neuron. They are often referred to as black boxes. Some previous studies have used anomaly detection using NNs in the maritime domain [18-22]. The NNs predict the behaviour of various phenomena through the learning process.

According to Patcha and Park (2007) [22], the main advantage of NNs is the inclusion of tolerance when it comes to imprecise data and uncertain information [22]. NNs can perform with non linear data, it is learns and does not need to be reprogrammed. NNs also has disadvantages, such as the high processing time and needs training before we operate the network.

- Support Vector Machines (SVMs)

SVMs are supervised learning methods using the binary classification that needs some pre-knowledge before classification. SVMs map the training data, which is consist of nonlinear data through the kernel function [23]. The role of kernel function is to induce such a feature space by implicity mapping the training data into higher dimensional space where the data is linear separable.

Similar to the NNs, the SVMs methods are capable of learning arbitrary complex regions in the input feature space. A key parameter of the SVMs is the kernel function, such as polynomial or Gaussian, which maps input data to high dimensional feature space where data can be perfectly or close to linear separated. A study done by Li et.al., [3] implemented SVMs to analyze vessel behaviour at a higher level of abstraction.

- Bayesian Networks (BNs)

The BNs is a machine learning technique based on the probability that represents a set of random variables and their conditional independencies via directed acyclic graph (DAG).

Previous studies have been done using the BNs, in which it is applied for anomaly detection on maritime domain and some other domains [7, 24, 25, 31]. Helldin and Riveiro (2009) [31] use the BNs in an anomaly detection research study. The AIS is used as the input data. The study focuses on how reasoning capabilities of the BNs can assist the operator in the control room.

A study done by Mascaro et. al. (2013) [26] defined the advantages of BNs and disadvantages of both the NNs and SVMs approaches. The BNs potentially have two substantial advantages: (1) The models are easy to understand by lay people (including the operator in the control room or other domain experts) and (2) They can include knowledge from the experts as input to the BNs model [26]. On the other hand, the NNs and SVMs do not present a transparent model to the user. Therefore, it is complicated for users like the operator in the control room to understand, interact and explore the model.

2.1 (b) Statistical Methods

Some studies using the statistical or probabilistic approach model have been done, e.g. the hidden Markov model (HMM) [32], Gaussian mixture model (GMM) [14, 33], and adaptive kernel density estimator (KDE) [14, 34].

Statistical techniques are simple to implement. However, their capability is limited to specific problems. Vessel speed is a good example of a variable in which these techniques are effective because of their extreme values. In cases where anomalies are uniformly dispersed in the sample, these techniques are ineffective.

There are two types of statistical technique, parametric and non-parametric. In parametric techniques, when the data correspond to a particular statistical model, anomaly can be detected rapidly and without supervision. With the non- parametric techniques, no assumption is made about the underlying distribution of data. Although more resources are required to develop them, these methods are effective for automated anomaly detection.

2.2 KNOWLEDGE-DRIVEN TECHNIQUE

In order to partially replace domain experts with the computer system, one must emulate the expert's capabilities. The knowledge-driven approach should be constructed to provide computer systems that can reason, communicate and interact. The more complete the knowledge support, the greater the ability to understand the situation and provide support for the process of anomaly detection.

There are several studies on knowledge-driven techniques for anomaly detection systems with different techniques such as rule based and description logic [15, 16]. However, in a previous study [7, 24] the *hybrid* approach was proposed where the expert's knowledge together with a data-driven approach are combined.

3. OVERVIEW OF OUR APPROACH

According to [23], the BNs is a directed acyclic graph (DAG) comprising a set of nodes and edges which represent the probabilistic dependencies among variables. The nodes with direct edges to other nodes are called the "parent" nodes. However, the nodes with edge pointing into them are known as the "child" nodes. A good example is found in the probabilistic relation between season and temperature. Given the temperature, the network can be used to compute the probabilities of various seasons.

3.1 BAYES' THEOREM

The BNs characterizes a problem domain consisting of a set of variables (attributes) $E = \{E_1, E_2, \dots E_n\}$. In the Bayesian terms, *E* is considered as the "evidence", *H* is considered as the hypothesis, and data *E* belongs to a specific class *C*. For the classification problems, our goal is to determine $P(H|E)$, i.e. we are searching for the probability that sample *E* belongs to class *C*, given that we know the attribute and description of *E*.

$$P(H|E) = \frac{P(E|H)P(H)}{P(E)} \quad (1)$$

$P(H) =$	Prior probability of hypothesis *H*
$P(E) =$	Prior probability of training data *E*
$P(H\|E) =$	Probability of *H* given *E*
$P(E\|H) =$	Probability of *E* given *H*

3.2 NAÏVE BAYESIAN CLASSIFIER

The naïve Bayesian classifier works as follows:

1. Let *E* be a training set of samples, each with class labels. There are *k* classes, C_1, C_2, …, C_k. Each sample is represented by an *n*-dimensional vector, $E = \{E_1, E_2, \dots E_n\}$, depicting *n* measured values of the *n* attributes, A_1, A_2, …, A_n, respectively.
2. Given a sample *E*, the classifier will predict that *E* belongs to the class that has the highest posteriori probability, conditioned on *E*. *E* is predicted to belong to class C_i if and only if

$$P(C_i|E) > P(C_j|E)\ for\ 1 \le j \le k, i \ne j$$

Thus, we find the class that maximizes $P(C_i|E)$. The class C_i for which $P(C_i|E)$ is maximized is called as the maximum posteriori hypothesis. By the Bayes' theorem

$$P(C_i|E) = \frac{P(E|C_i)P(C_i)}{P(E)} \quad (2)$$

3. Maximize $P(E|C_i)P(C_i)$ as $P(E)$ is constant

4. In order to reduce the computational process in evaluating $P(E|C_i)P(C_i)$, the naïve assumption of class conditional independence is made. This presumes that the values of the attributes are conditionally independent of one another, given the class label of the sample. Mathematically, this means that

$$P(E|C_i) \approx \prod_{k=1}^{n} P(E_k\,|C_i) \quad (3)$$

The probabilities $P(E_1|C_i)$, $P(E_2|C_i)$, …, $P(E_n|C_i)$ can be easily estimated from the training set.

3.2 BNS-BASED APPROACHES TO ANOMALY DETECTION

According to [7], the BNs can be learnt from:

1) Domain experts' knowledge;
2) Data set; or
3) Combination of the two.

In this paper, we focus on learning the BNs from data without the support of human knowledge. The AIS reporting data are used for the purpose of our research. When learning the BNs from data, an assumption has to be made so that there is a fundamental process that follows a probability distribution. Hence, it is possible to represent the fundamental probability distribution with the BNs.

4. SIMULATION

As illustrated in Figure 1, the simulation begins with the cleaning of the AIS raw data and the assigning of each record to separate tracks based on the Maritime Mobile Service Identity (MMSI). The next step is the interpolation process which will improve the accuracy of the anomaly detection. This process interpolates each row's value into the nearest three minutes interval and eliminates duplicated data.

The data are categorized into normal and anomaly tracks data. Each group of tracking data will be randomized and divided into two groups using hold-out process. Hold-out is the process in which data is divided into two parts; the first part is reserved for the testing process, and the second is reserved for the training process. The last step is the BNs classification.

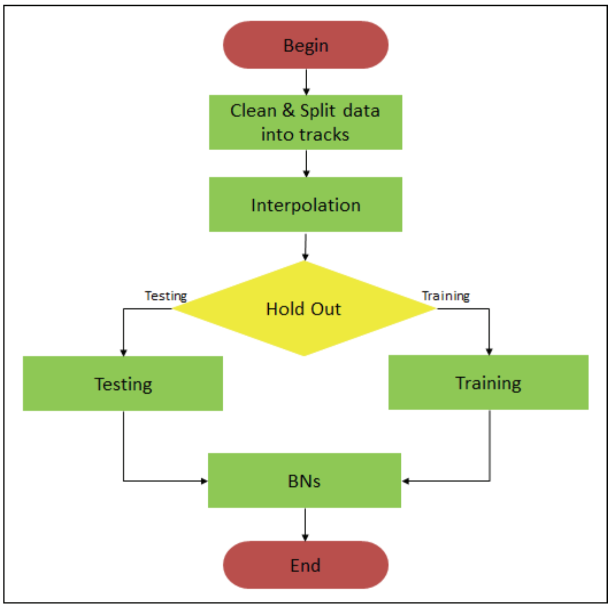

Figure 1. Flowchart of the simulation process

In this paper, we use the visual analysis method for the detection of vessels anomaly behaviour. For small data sets, the visual analysis approach will produce a very good result. However, when the data set is too large to be captured by human analysis, the result will fail [35]. The design process of the overall anomaly detection process can be organized into the following step:

1. *Categorize* data, separate and label into two sets, *normal* tracks and *anomaly* tracks data
2. *Randomized* normal tracks data

3. *Randomized* anomaly tracks data
4. *Divide* normal tracks data into two groups using hold-out methods
5. *Divide* anomaly tracks data into two groups using hold-out methods
6. *Combine* first group of normal tracks data and first group anomaly tracks data, and randomized it for *training process*
7. *BNs classification*, get the accuracy of training data (memory test)
8. *Combine* second group of normal tracks data and second group anomaly tracks data, and randomize it for testing process
9. *BNs Classification*, get the accuracy of testing data (blind test)

The flowchart of the above design process is presented once again in Figure 2.

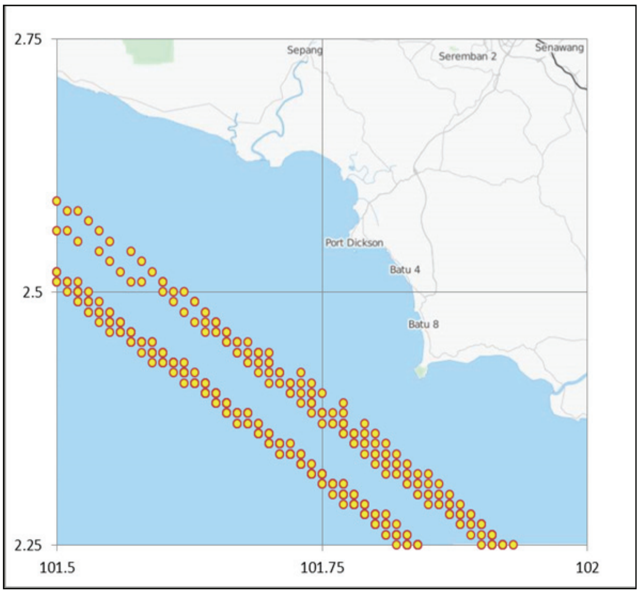

Figure 2. Scenario of vessel anomaly behavior with normal route

5. THE DATA

We use the AIS raw data of Port Klang from July to September 2013. The AIS raw data consist of 9,845 rows of data, including the vessel's MMSI, status, speed, longitude, latitude, course, heading and timestamp (see Table 1). All information is obtained from the public website, marinetrafic.com.

Below is an example of seven different vessel movements' data from the original AIS data. To retain the anonymity, some details are removed.

The AIS data were cleaned and separated into 'tracks' based on the MMSI. The above data consist of 367 tracks with 7 unique MMSI averaging at 1,400 rows each.

The vessel record data contains 8 variables, including the MMSI, status, speed, longitude, latitude, course, heading and timestamp.

6. RESULTS AND DISCUSSION

Figure 3 displays the scenario of vessel anomaly behavior with the normal route of the Straits of Malacca with the longitude from 101.5^0 to 102^0, and latitude from 2.25^0 to 2.75^0. As shown, the yellow circle indicates the normal speed of the vessel.

Here, we present the example of the vessel anomaly behavior in a speeding scenario. The variables that we used for training the model include the MMSI, speed, course, longitude and latitude. The spatial variable is also important in detecting the vessel anomaly behavior. For example, if the vessel moves with low speed and the location is near the port, it is considered as a normal behaviour. However, if the location is far from the port, it has the potential to be an anomaly behavior. On the other hand, the vessel also has the potential to be anomalous when moving on the waterway with speed exceeding the maximum speed.

Table 1. An example of Seven different vessel data from the original AIS data

MMSI	Status	Speed	LON	LAT	Course	Heading	TIMESTAMP (UTC)
47724****	5	0	101.3038	2.951465	246	210	7/10/2013 9:20:00 PM
52501****	9	222	101.3763	2.997293	269	511	7/31/2013 5:15:00 AM
53301****	0	76	101.9443	2.274085	304	511	8/23/2013 9:22:00 AM
53301****	0	96	101.1952	2.9433303	29	511	8/5/2013 5:03:00 PM
53301****	0	106	101.3227	2.981503	46	47	7/12/2013 8:26:00 AM
53313****	5	0	101.3039	2.951412	227	30	7/18/2013 6:32:00 AM
53386****	1	36	102.1907	2.185028	164	308	7/31/2013 9:44:00 PM

Figure 4 shows the vessel anomaly behavior in the speedy scenario. As shown in the figure, the yellow circle denotes the normal behavior, while the red square indicates the anomaly behavior of the vessel. In this scenario, the vessel is moving with the speed of more than the maximum speed of the vessel.

The anomaly behaviour can include many cases; e.g. vessels with random movement in the middle of water, vessels with unexpected stops, vessels with a close track in the middle of water, vessels with very short tracks, vessel tracks with many interactions, vessel tracks with many loops, travel over land, deviations from standard routes, speeding, traffic direction violation, etc. [26, 33].

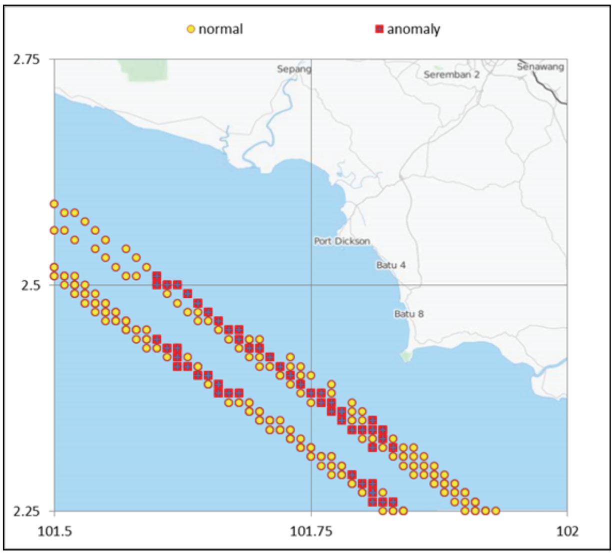

Figure 3. Scenario of vessel anomaly behavior (speedy route)

A model to describe normality is constructed using a training data set. The testing data set will be compared to the training data set to classify them into two categories: normal or anomaly. In the experiments, we use the holdout method. The holdout method partitions data into two subsets called as the training set and testing set [23, 36]. It will give significantly different results depending on how the training and testing data are distributed.

Here, we perform two types of testing, the memory test and blind test. Memory test is the prediction accuracy on training data set. However, blind test is prediction accuracy on testing data. For the classification process, we select four types of experiments:

(i) 50% of the data is used for training, and 50% of data for testing (50-50).
(ii) 60% of the data is used for training, and 40% of data for testing (60-40).
(iii) 70% of the data is used for training, and 30% of data for testing (70-30).
(iv) 80% of the data is used for training, and 20% of data for testing (80-20).

The result is presented in Table 2. As illustrated, the best accuracy result appears from dividing the raw data into 80% for training and 20% for testing. In Figure 5, we can view the line chart of the experimental results. The blue line with the diamond marker shows the memory test result, whereas the red line with the square marker presents the blind test result.

Table 2. The Experimental Result from four Types of Partition Data

	Type of Experiments			
	50-50	**60-40**	**70-30**	**80-20**
Memory Test	94.78%	95%	94.05%	94.58%
Blind Test	94%	93.46%	95.19%	94.72%

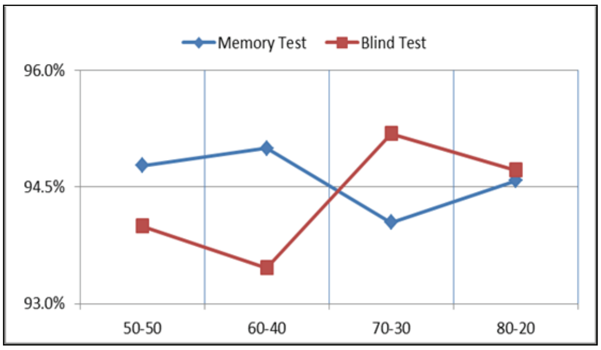

Figure 4. Line chart from experimental result

From the figure we can see that that the lowest percentage appears in the (70-30) point which is 94.05%. The memory test result obtains the best accuracy in the (60-40) point which is 95%. From the blind test result, we can see that that the lowest percentage appears in the (60-40) point which is 93.47%. The blind test result gets the best accuracy in the (70-30) point which is 95.19%.

By performing experiment on the AIS data, we are able to identify the anomaly such as vessels with speed deviating from the normal behavior. Not only speed, here we combined the speed and spatial data to define the vessel anomaly behavior. However, the relation between objects (e.g. distance to closest vessel) has not been considered.

7. CONCLUSION

In this paper, we have explored vessel anomaly behaviour with visual analysis and vessel tracking data using the BNs approach in the speed scenario.

From our experiment, we found that the BNs method can be used for vessel anomaly detection. As for the holdout method, it is shown that the partitions 60% for training and 40% for testing from the data yield the best result for memory test (95%). For the blind test accuracy, the best result is 95.19% for partitioning, 70% for training and 30% for testing set.

One of the advantages of the BNs approach is that it is possible to include human knowledge in the model, and that human can validate the model. However, how this should be implemented requires further investigation. This advantage has not been explored in our experiment.

Further work is also needed to evaluate other machine learning approaches on the AIS data to identify vessel anomaly behaviour. The use of another machine learning approach, e.g. the SVMs and NNs as comparison, and extending the experiment with additional variables are suggested for future works.

8. ACKNOWLEDGMENT

We would like to express our gratitude to Miluše Tichavska, Academic Relation from marine traffic.com for providing the data and valuable feedback.

9. REFERENCES

1. MaritimeSecurityAsia, "ICS calls for improved navigation safety in Malacca, Singapore Straits," 2011. [Online]. Available: http://maritimesecurity.asia/free-2/strait-of-malacca-free-2/ics-calls-for-improved-navigation-safety-in-malacca-singapore-straits/. [Accessed: 12-Mar-2013].
2. KAZEMI, S. ABGHARI, S. LAVESSON, N. JOHNSON H., and RYMAN, P. "Open data for anomaly detection in maritime surveillance," Expert Syst. Appl., vol. 40, no. 14, pp. 5719–5729, Oct. 2013.
3. LI, X. HAN, J. and KIM, S. "Motion-alert: automatic anomaly detection in massive moving objects," Intell. Secur. Informatics, 2006.
4. RIVEIRO, M. and ZIEMKE, T. "Improving maritime anomaly detection and situation awareness through interactive visualization," Proc 11th Int Conf Inf. Fusion(IF-08), Los Altos, CA, pp. 47–54, 2008.
5. MARTINEAU, E. and ROY, J. "Maritime anomaly detection: Domain introduction and review of selected literature," 2011.
6. FOOLADVANDI, F. BRAX, C. GUSTAVSSON, P. and FREDIN, M. "Signature-based activity detection based on Bayesian networks acquired from expert knowledge," 12th Int. Conf. Inf. Fusion, pp. 436–443, 2009.
7. JOHANSSON, F. and FALKMAN, G. "Detection of vessel anomalies - a Bayesian network approach," 2007 3rd Int. Conf. Intell. Sensors, Sens. Networks Inf., pp. 395–400, 2007.
8. MILES, J. A. H. EDMONDS, T. J., QinetiQ PTP. "Automated Situation Assessment in a Maritime Combat System," 12th ICCRTS, pp. 1–9, 2006.
9. PALLOTTA, G. VESPE, M. and BRYAN, K. "Vessel Pattern Knowledge Discovery from AIS Data: A Framework for Anomaly Detection and Route Prediction," Entropy, vol. 15, no. 6, pp. 2218–2245, Jun. 2013.
10. ENDSLEY, M. R. "Theoretical Underpinnings of Situation Awareness: A Critical Review," Situat. Aware. Anal. Meas., pp. 1–24, 2000.
11. DAS, S. GREY, R. and GONSALVES, P. "Situation assessment via Bayesian belief networks," Proc. Fifth Int. Conf. Inf. Fusion. FUSION 2002. (IEEE Cat.No.02EX5997), vol. 1, pp. 664–671, 2002.
12. E. L. LLC, "Speed Limits on Cargo Ships Could Cut Emissions 'Up to 70%,'" 2012. [Online]. Available: http://www.environmentalleader.com/2012/10/25/speed-limits-on-cargo-ships-could-cut-emissions-up-to-70/. [Accessed: 16-Jan-2914].
13. CHANDOLA, V. BANERJEE, A. and KUMAR, V. "Anomaly detection: A Survey," ACM Comput. Surv., vol. 41, no. 3, pp. 1–58, Jul. 2009.
14. LAXHAMMAR, R. "Anomaly detection in sea traffic-a comparison of the gaussian mixture model and the kernel density estimator," 12th Int. Conf. Inf. Fusion, 2009. FUSION '09., pp. 756 – 763, 2009.
15. GUYARD A. and ROY, J. "Towards Case-Based reasoning for maritime anomaly detection: A positioning paper," Proc. 12th IASTED Int. Conf. Intell. Syst. Control, 2009.
16. NILSSON, M. RIVEIRO, M. and ZIEMKE, T. "Investigating human-computer interaction issues in information-fusion-based decision support," 2008.
17. DAHLBOM A. and NIKLASSON, L. "Trajectory clustering for coastal surveillance," 2007 10th Int. Conf. Inf. Fusion, pp. 1–8, Jul. 2007.
18. RHODES, B. J. BOMBERGER, N. A. SEIBERT, M. and WAXMAN, A. M. "Maritime Situation Monitoring and Awareness Using Learning Mechanisms," MILCOM 2005 - 2005 IEEE Mil. Commun. Conf., pp. 1–7.
19. RHODES, B. J. BOMBERGER, N. A. and ZANDIPOUR, M. "Probabilistic associative learning of vessel motion patterns at multiple spatial scales for maritime situation awareness," 2007 10th Int. Conf. Inf. Fusion, pp. 1–8, Jul. 2007.
20. RHODES, B. J. BOMBERGER, N. A. FREYMAN, T. M. KREAMER, W. KIRSCHNER, L. L'ITALIEN, A. C. MUNGOVAN, W. STAUFFER, C. STOLZAR, L. WAXMAN, A. M. and SEIBERT, M.

"SeeCoast: Persistent Surveillance and Automated Scene Understanding for Ports and Coastal Areas," Def. Transform. Net-Centric Syst. 2007, vol. 6578, no. 1, p. 65781M–65781M–12, Apr. 2007.

21. BOMBERGER N. and RHODES, B. "Associative learning of vessel motion patterns for maritime situation awareness," 2006 9th Int. Conf. Inf. Fusion, pp. 1 – 8, 2006.

22. PATCHA A. and PARK, J.-M. "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput. Networks, vol. 51, no. 12, pp. 3448–3470, Aug. 2007.

23. BISHOP, C. M. Pattern Recognition and Machine Learning, 9th ed. Springer, 2009.

24. FOOLADVANDI F. and BRAX, C. "Signature-based activity detection based on Bayesian networks acquired from expert knowledge," 12th Int. Conf. Inf. Fusion, pp. 436–443, 2009.

25. LANE, R. NEVELL, D. HAYWARD, S. and BEANEY, T. "Maritime anomaly detection and threat assessment," 13th Conf. Inf. Fusion (FUSION), 2010, pp. 1–8, 2010.

26. MASCARO, S. NICHOLSO, A. E. and KORB, K. B. "Anomaly detection in vessel tracks using Bayesian networks," Int. J. Approx. Reason., pp. 1–15, Apr. 2013.

27. WONG, W. MOORE, A. COOPER, G. and WAGNER, M. "Bayesian network anomaly pattern detection for disease outbreaks," proceeding Twent. Int. Conf. Mach. Learn., 2003.

28. CANSADO A. and SOTO, A. "Unsupervised Anomaly Detection in Large Databases Using Bayesian Networks," Appl. Artif. Intell., vol. 22, no. 4, pp. 309–330, Apr. 2008.

29. LOY, C. C. XIANG, T. and GONG, S. "Detecting and discriminating behavioural anomalies," Pattern Recognit., vol. 44, no. 1, pp. 117–132, Jan. 2011.

30. DAS, K. SCHNEIDER, J. and NEILL, D. B. "Anomaly pattern detection in categorical datasets," Proceeding 14th ACM SIGKDD Int. Conf. Knowl. Discov. data Min. - KDD 08, p. 169, 2008.

31. HELLDIN, T. and RIVEIRO, M. "Explanation methods for Bayesian networks: Review and application to a maritime scenario," 3rd Annu. Skövde Work. Inf. Fusion Top. (SWIFT 2009), pp. 11–16, 2009.

32. ANDERSSON, M. and JOHANSSON, R. "Multiple sensor fusion for effective abnormal behaviour detection in counter-piracy operations," Proc. Int. waterside Secur. Conf., 2010.

33. LAXHAMMAR, R. "Anomaly detection for sea surveillance," 11th Int. Conf. Inf. Fusion, pp. 55–62, 2008.

34. RISTIC, B. LA SCALA, B. MORELANDE, M. and GOR, "Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction," 11th Int. Conf. Inf. Fusion, 2008.

35. KEIM, D. MANSMANN, F. and THOMAS, J. "Visual analytics: how much visualization and how much analytics?," ACM SIGKDD Explor. Newsl., vol. 11, no. 2, pp. 5–8, 2010.

36. SCHNEIDER, J. "Cross Validation," 1997. [Online]. Available: http://www.cs.cmu.edu/~schneide/tut5/node42.html. [Accessed: 07-Dec-2013].