Australian Government
Department of Defence
Defence Science and
Technology Organisation

A Rule-based Track Anomaly Detection Algorithm for Maritime Force Protection

S.Boinepalli and A.J.Knight

Weapons and Combat Systems Division
Defence Science and Technology Organisation

DSTO-TR-3012

ABSTRACT

We developed an anomaly detection tool using a Rule-based Algorithm that can detect anomalies in a set of pre-recorded tracks using their curvature, speed and weave. We devised a method that can quantify the amount of curvature in a recorded surface track. The anomaly detection tool uses the limiting values for curvature, speed and weaving provided by the user to classify a track as "normal" or "anomalous".

We tested two data sets consisting of radar tracks recorded in May and August 2007. We varied the threshold values that the tool uses. We compared the results of the tool's analysis of the data sets with a visual inspection performed by a navy combat system operator. The results of the tool's analysis were in good agreement with those of the visual inspection.

RELEASE LIMITATION

Approved for public release

Published by

Weapons and Combat Systems Division
DSTO Defence Science and Technology Organisation
Edinburg, Australia

Telephone: 1300 333 362
Fax: (08) 7389 6567

AR 016-049
August 2014

APPROVED FOR PUBLIC RELEASE

A Rule-based Track Anomaly Detection Algorithm for Maritime Force Protection

Executive Summary

Royal Australian Navy (RAN) ships are vulnerable to attack from asymmetric threats such as Fast Inshore Attack Craft (FIAC), either when they are alongside in harbour or in the littoral. Defending ships against such attacks comes under the term 'Force Protection' (FP). Sufficient Situational Awareness is required for effective Force Protection, in harbour, in littoral areas and the open ocean. These are areas which are particularly problematic due to the increased amount of non-threatening sea traffic. The RAN would benefit from a capability to assess the intent of a vessel, allowing them to take early action if a particular track appears suspicious or abnormal.

The aim of the current task is to develop a concept that could be potentially developed into an anomaly detection tool to detect suspicious or anomalous tracks in previously recorded radar data. We used a rule-based algorithm to detect these tracks.

To build the rules that the algorithm can use, we identified the characteristics of a recorded radar track. These track characteristics capture essential information of a track, viz., the track length, turns, speed and weave. The recorded tracks are analysed to determine thresholds on these features. The rule-based algorithm classifies a track from a given data set as "normal" or "anomalous" depending upon whether its characteristics lie within the set thresholds.

The curvature signatures that we developed are used initially to eliminate clutter from tracks. The clutter-free tracks are input into the tool that uses a combination of the limiting values to identify anomalous tracks.

We generated sets of simulated tracks with various speeds and turn for initial testing. Then we used the tool on radar data that were recorded near Sydney harbour. The data set was examined for anomalies by independent visual inspection by RAN personnel. The results of the analysis by the tool were compared against the results of visual inspection. The agreement between the results of the tool and visual inspection is about 80%. That is, the classification of tracks by the tool and visual inspection agreed for 80 tracks out of every 100 tracks, irrespective of the classification of the track.

The tool needs more robust and rigorous testing, against another anomaly detection tool and against visual inspection by a group of operators. The threshold levels used by the tool should be set considering various factors, e.g., sea state and geographical location (littoral against deep ocean). Such a decision aid would reduce operator work load and avoid potential errors due to operator fatigue.

Contents

1. Introduction

Royal Australian Navy (RAN) ships are vulnerable to attack from asymmetric threats such as Fast Inshore Attack Craft (FIAC), either when they are alongside in harbour or in the littoral. Defending ships against such attacks comes under the term 'Force Protection'.

Sufficient situational awareness is required for effective Force Protection, in harbour, in littoral areas and the open ocean. Towards this end, the RAN needs a capability of assessing the intent of a track and taking action if a particular track exhibits suspicious or abnormal behaviour. The aim of this work is to develop a tool that detects tracks as behaving in a suspicious or anomalous way. The tool developed and assessed in this work identifies anomalous tracks within a batch of recorded tracks. Future work will address the development of a tool that identifies anomalous tracks in real time, that is, as the tracks are updated.

This report captures the details of the tool design, implementation and results of testing. Section 2 describes the scope and aims of this task while Section 3 briefly gives an overview of existing techniques in this area. Section 4 captures the details of the tool. Sections 5 and 6 explain the simulated and real data used to test the tool. Section 7 gives details of the results. In Section 8, conclusions with future plans are touched upon.

2. Scope

The long-term aim of this work is to improve the way the RAN performs Force Protection. This will be achieved by exploring the operational concepts of an integrated Very Short Range Surface Defence for the protection of surface ships against asymmetric threats in the littoral and in harbour. The RAN's Rules of Engagement, by definition, have a significant impact on response options, and appropriate restrictions will need to be incorporated into response planning and threat assessment. However, these are not considered in this current task.

The scope of this particular Force Protection activity covers the maritime surface domain, specifically against asymmetric surface threats. The detection of asymmetric threats becomes particularly problematic in harbour and littoral situations where non-threatening sea traffic is to be expected. Although there is interest in Force Protection against Fast Inshore Attack Craft, only Force Protection against harbour traffic will be considered, as only in-harbour data is available.

3. Algorithms and Tools Review

Much work has been done in developing anomaly detection tools and many algorithms have been reported in the literature [1, 2, 3, 4, 5, 6]. Most of these algorithms depend upon providing a "training data set" to the tool. The tool analyses the training data set and develops a model to fit the training data set. Then the data set to be analysed is fed into the tool for anomaly detection. Vast quantities of data from the Automatic Identification System (AIS) are available for the training of these tools [1, 4]. The development of these models is based on K-d trees [2], Bayesian [4] or clustering methods [3, 5].

Apart from these model-based algorithms, there also exist rule-based algorithms. The rule-based algorithms use a set of rules developed by subject matter experts based on their experience and domain knowledge [2]. The normal and abnormal behaviours are codified as rules. R.Jasinevicius *et al* developed a rule-based fuzzy expert system that considered vessel type, persons on board and the risk factor associated with the cargo [7].

Our tool is rule based and requires no prior training. It uses a set of rules with threshold values for track characteristics. It requires approximate predicted values for track characteristics (speed, course, rate of change of course) in the region of interest. The tool then tests each track against pre-set thresholds for these values to decide upon the nature of the track.

4. Anomaly Detection Tool

The main features of a track being acquired in the harbour are the position coordinates (latitude and longitude), speed, course and the time stamp. These properties are used to identify anomalous tracks in a given set of tracks.

For the purpose of identifying anomalous tracks, it is important to firstly define an anomalous track. An "anomalous" track is one whose behaviour doesn't fit in with that of the rest of the tracks in a given area. Although the tool can be customised to any area (in-harbour, littoral or open ocean), our focus is in and around Sydney Harbour.

The tool that we developed focuses on analysing track characteristics. The features that the tool takes into account are the curvature of a track, the speed and the amount of weaving in a track. We define threshold values for each of these features. When the features exceed the pre-set threshold values, the track is flagged as an anomalous track. The features considered for anomaly detection are discussed in the following sections.

4.1 Curvature of Tracks

A track is a set of data points, with each data point consisting of latitude, longitude, speed and course at a particular time instant. The curvature of a track indicates the distance covered by a vessel to reach a destination point from an initial point. Curvature is minimal for a normal, straight track, where the vessel takes the shortest route from an initial point to an end point. The farther a track moves away from the shortest path, the more anomalous the track becomes.

For the purpose of anomaly detection, we defined two signatures of a track that indicate its curvature. For computing these signatures, the starting coordinates of the track $S\ (long_s, lat_s)$ and the coordinates at the end of the track $E\ (long_e, lat_e)$ must be known. The shortest distance, *D*, between these two points, assuming a flat earth, is given as

$$D(long, lat) = \sqrt{(long_e - long_s)^2 + (lat_e - lat_s)^2} \quad (1)$$

However, the surface of the earth is not flat and the spherical coordinates (longitude, latitude) must be converted into Cartesian coordinates relative to a reference location, *R*, in the vicinity of the track. These Cartesian coordinates (x_i^R, y_i^R) are a projection onto a plane that is tangential to the surface of the earth at the reference location. Therefore, (1) becomes

$$D_c = \sqrt{(x_e^R - x_s^R)^2 + (y_e^R - y_s^R)^2} \quad (2)$$

The distance covered by the recorded tracks analysed in this study is much smaller compared to the radius of earth, hence the curvature of earth can be ignored. Hence the distances between the data points are calculated as the distances from the reference location in each coordinate.

4.1.1 Curvature Signature 1 (*CS1*)

The first Curvature Signature *CS1* gives an indication of a track's tendency to deviate from the shortest path between its starting and ending coordinates. It is the ratio of the shortest distance, *D(x, y),* between the starting and ending points of the track to the total length of the track. The shortest distance is calculated as a two dimensional distance between *S* and *E* using the Cartesian geometry assumption. The track length is calculated as a sum of distances between successive points on the track,

$$CS1 = \frac{D(x, y)}{\sum_{i=2}^{N} \sqrt{(x_i^R - x_{i-1}^R)^2 + (y_i^R - y_{i-1}^R)^2}} \quad , (3)$$

where (x_i^R, y_i^R) is the i^{th} recorded data point for the track under consideration.

Figure 1 depicts a sample track as a plot of latitude against longitude. The pink curve is the recorded track data, while the blue line is the shortest two dimensional path between the start and end points of the track. *CS1* is the ratio of the length of the blue line to that of the pink track.

For a track that covers the distance without deviating from the shortest path, *CS1* is equal to 1 since in that case the track length is equal to the shortest distance. *CS1* approaches zero when the track length is much larger than the shortest distance *D(x, y)*. Therefore it is possible to filter out tracks by eliminating tracks with a value of *CS1* lower than a threshold value. The threshold low value is generally chosen by analysing historical data.

However *CS1* is not sufficient in detecting anomalous tracks. *CS1* can identify tracks that cover a larger distance than expected. It cannot pick up tracks that accelerate in a straight line or change course rapidly. Therefore we define another curvature signature CS2, to locate clustering, rapidly weaving, and accelerating tracks.

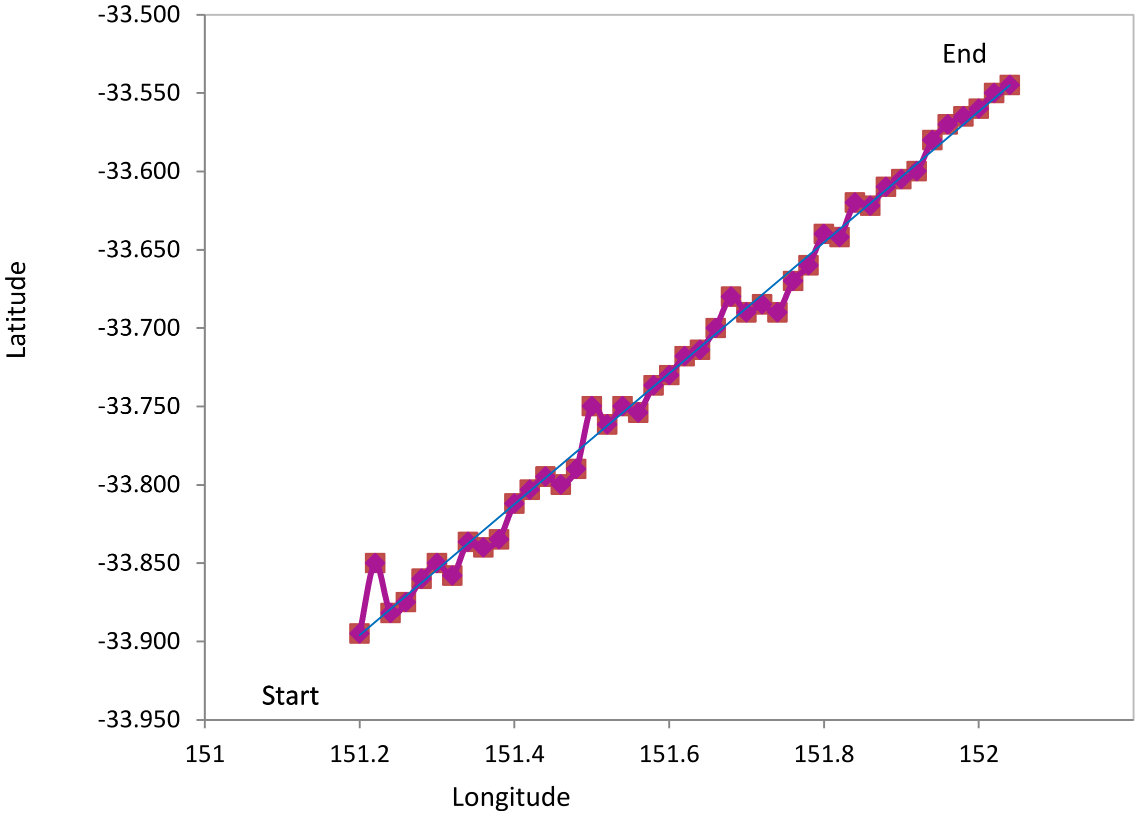

Figure 1 A sample radar track showing the recorded track (pink) and the shortest distance (blue line) between the start and end points of the track.

4.1.2 Curvature Signature 2 (*CS2*)

Curvature Signature *CS2* is used to augment the characterisation provided by *CS1*. *CS2* is very similar to *CS1* in definition.

To calculate *CS2*, the shortest track (blue line in Figure 1) between the starting and end coordinates of the given track is divided into equidistant points, equal in number to the number of data points in the original track, *N* (pink curve in Figure 1).

Let $P^r{}_i$ denote the i^{th} point on the real track and $Q^s{}_j$ denote the j^{th} point on the shortest track. *CS2* is the ratio of the cumulative distance of all the points $Q^s{}_j$ from the start point to that of all the points $P^r{}_i$ from the start point. The start point is common, therefore $S = Q_1^s = P_1^r$.

$$CS2 = \frac{\sum_{j=2}^{N} \overline{Q_j^s S}}{\sum_{i=2}^{N} \overline{P_i^r S}} \qquad (4)$$

In the above equation, $\overline{Q_j^s S}$ denotes the two dimensional distance between the point $Q^s{}_j$ on the shortest track and the starting point *S*. $\overline{P_i^r S}$ denotes the two dimensional distance between the point $P^r{}_i$ on the real track and the starting point *S*.

CS2 gives an indication of spread of the track data points from the linear track with constant speed track points. For a linear track with constant speed, *CS2* is equal to 1. *CS2* is large for tracks that drift too far away from the ideal shortest possible track. A small value of CS2 indicates clustering of points near the starting point of the track.

The threshold values for *CS1* and *CS2* are chosen by trial and error using a visual examination of data. Together, the two curvature signatures are the first level of filtering. If a track is rejected by *CS1* and *CS2*, it is no longer tested for the subsequent tests given below. The combined application of *CS1* and *CS2* is discussed in more detail in the following sections.

4.2 Speed Limit

Speed is a good indicator of threat intent, especially with FIACs. Upper and lower bounds can be placed on speeds to filter out anomalous tracks. In the current task, a speed limit was chosen depending upon the data and information available for small boats.

For every data point on a given track, the speed is compared to a preset speed limit and a flag is raised if the speed exceeds the speed limit. The total number of flags raised is normalised against the track length, giving the average number of speed flags raised per unit length (e.g., kilometre) of track. If the average number of flags raised per unit length of a track exceeds a certain preset number, the track is deemed an "anomalous" track.

If a track is qualified by the curvature signature test and the speed test, then it proceeds to the final weave test.

4.3 Weave Rate

A track is considered suspicious if it changes course too quickly, or too many times. To perform this test, the rate of change of course (ROCC) is calculated for each time step of a given track. The weave rate or the ROCC is calculated as the ratio of the difference in course to the difference in time between successive track readings. In a fashion similar to the speed test described in the previous section, a limit is placed on the ROCC. The entire track's ROCC is examined and every time it exceeds the limit a flag is raised. The total number of ROCC flags raised in a track is normalised against the track length, giving the number of flags raised per unit length. If this average number of flags for a track exceeds a certain preset number, the track is considered anomalous.

5. Simulated Data

For a preliminary evaluation, we simulated various types of tracks and analysed them using the tool. The simulation consisted of 81 tracks in total. For consistency with the real AIS data, these tracks are in the same geographical location, viz., in Sydney Harbour. The tracks included

a) Simple linear tracks
b) Tracks with varying accelerations
c) Tracks at different bearings
d) Tracks with varying weaving forms
e) Randomly moving tracks.

Figure 2 shows some sample tracks simulated for evaluation purposes. As seen from the figure, the simulated tracks include various accelerations and turn rates. These simulated tracks were used as a proof of concept, rather than for rigorous testing. However simulated data is highly synthetic; hence testing on simulated data doesn't suffice. Therefore another set of data obtained from SAAB Australia was used for a more thorough evaluation.

6. Real Data

6.1 Radar recorded data

SAAB Australia provided two sets of radar tracks with recordings of latitude, longitude, speed, course and time stamp. The radar data were collected in May and August 2007 in Sydney Harbour. Each data set comprised more than 3000 tracks. As the tool does not require training, both the data sets were used to evaluate the tool.

6.2 Clutter Removal

Unlike AIS data, radar data includes lot of noise and spurious returns. Figure 3 depicts some sample tracks from the May data set. As seen from the figure, there are many tracks that look spurious and like noise. When the track data with noise is analysed by the tool, it classifies them as "anomalous tracks". Therefore, for a better anomaly detection analysis, the data was cleared of the noise first. We used the feature *CS1* to remove clutter and any other false tracks.

Figure 3 contains some randomly selected tracks from the May data set. The number on each plot indicates the track identification number. From the figure it can be seen that some of the track plots look like clutter, false tracks or false radar detections. If these are left in the data set, they would be classified as "anomalous tracks", while in fact we wish to disregard them entirely as not genuine tracks.

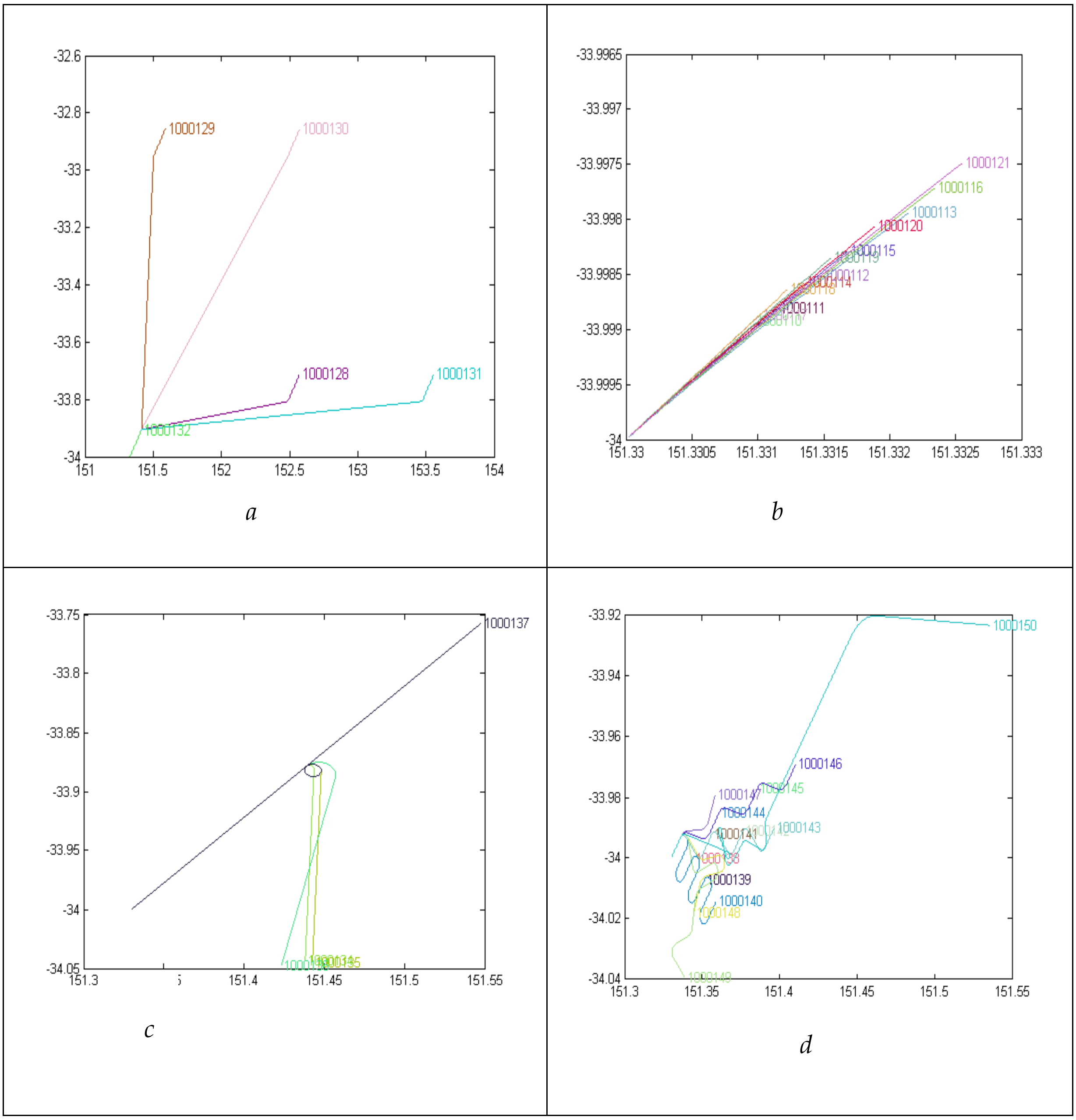

Figure 2 Sample set of simulated tracks. The set of tracks in (a) and (b) are linear tracks with various accelerations. Those in (c) and (d) are weaving tracks. Some of these are classified as "anomalous tracks" by the tool, depending on the threshold on weave rate.

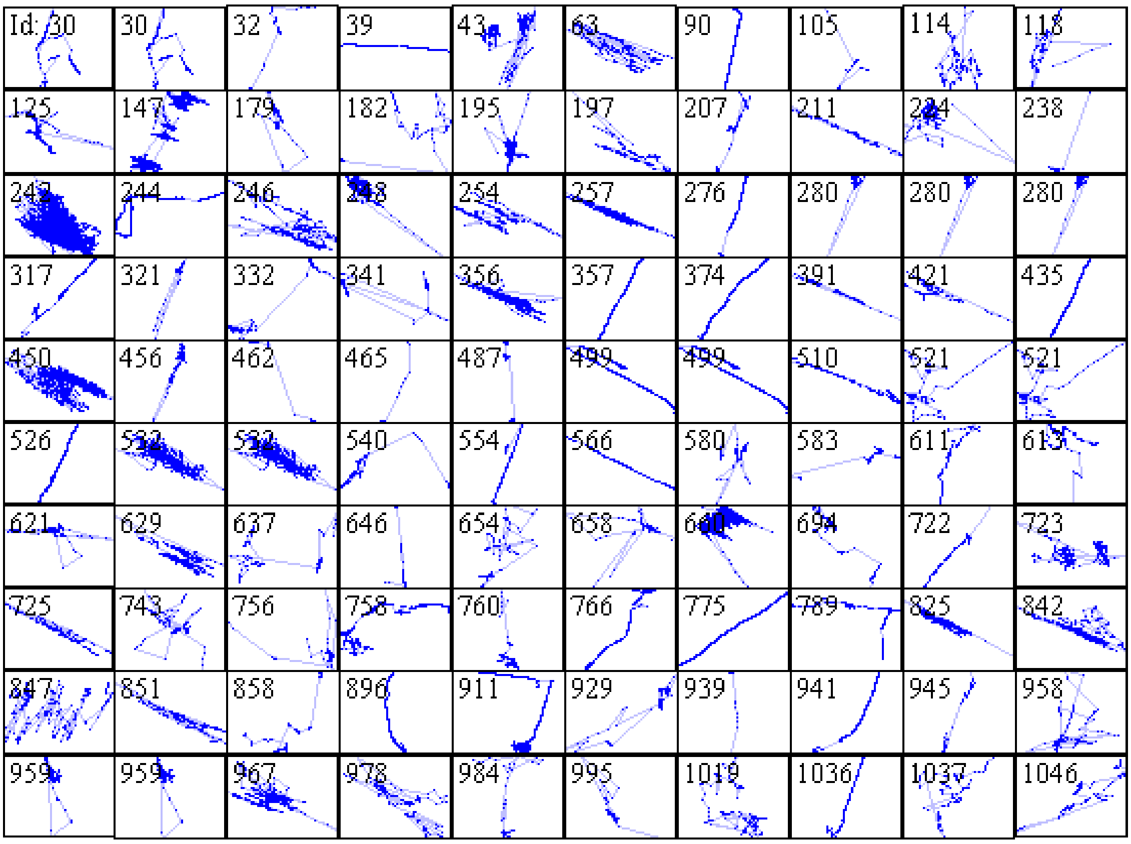

Figure 3. Randomly selected tracks from the May data set. The number included with the track is the track identification number.

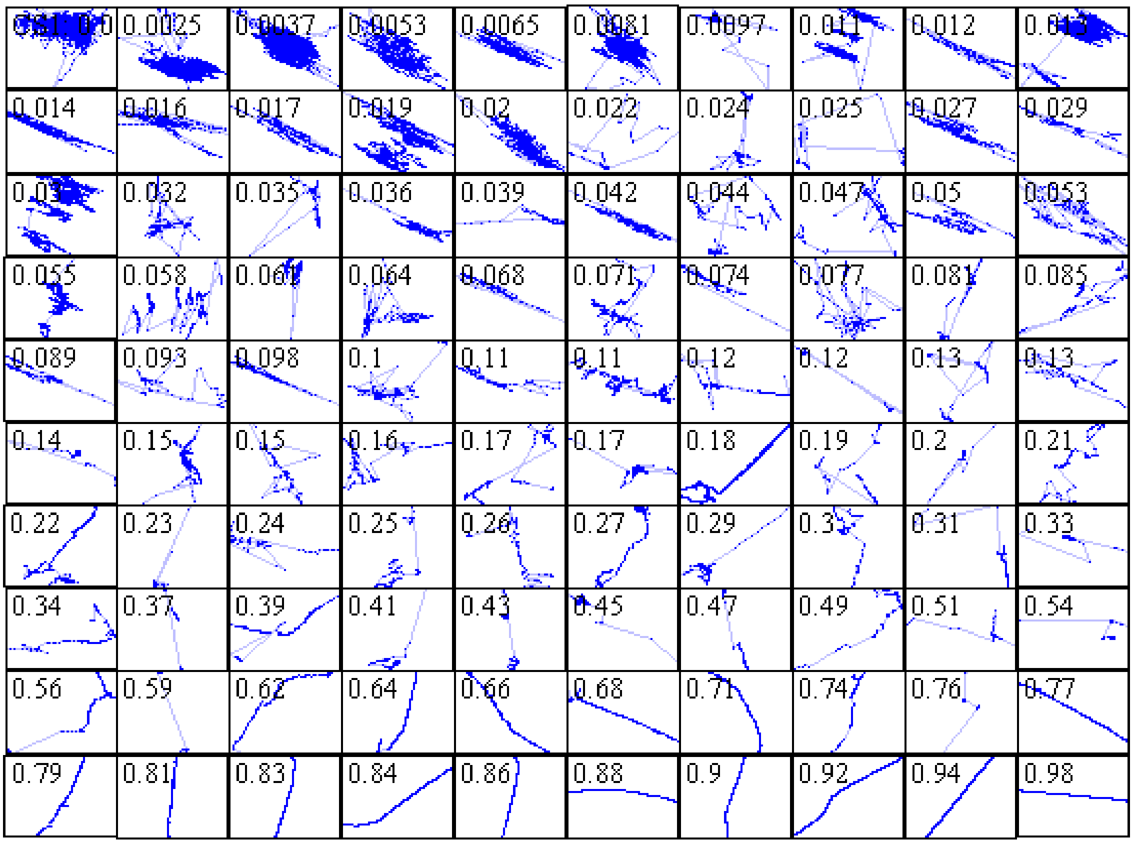

Figure 4. Randomly selected tracks organized in increasing order of CS1. The number inside the figures indicates the CS1 value of the track.

Figure 4 contains some randomly selected tracks arranged in increasing order of *CS1*. A very low value of *CS1* indicates that the track length is much larger than the shortest distance. The lower the value of *CS1* the noisier the track is. A value of 0.2 was used as a threshold to remove the clutter. Tracks with a *CS1* less than 0.2 were rejected as clutter and only tracks with *CS1* higher than 0.2 were analysed further. From the figure it can be seen that the data with very low value for *CS1* does indeed look like noise. The tracks that are cleaner have a *CS1* closer to 1.

7. Results

7.1 Simulated data

The tool was first tested using simulated data as discussed in Section 5 for proof of concept. The results were as expected—the tracks that had too many loops, were accelerating, or with speed above the threshold were flagged by the tool as suspicious.

7.2 Recorded data

The two sets of recorded data, recorded in May and August 2007 were tested separately after removing the clutter. The data recorded during May 2007 consisted of 1242 tracks. Removing the clutter using the *CS1* criteria yielded 560 tracks. The data recorded during August 2007 consisted of 3456 tracks. Removing clutter using the *CS1* criteria yielded 1438 tracks.

We applied various thresholds to the track feature parameters. These threshold values were arrived at after discussions with RAN personnel and analysing the data sets for mean values and standard deviations. Given below are two different sets of thresholds applied separately.

Table 1 Thresholds on the track features

Track Feature	Threshold set 1	Threshold set 2
CS1	0.5	0.7
CS2	W_a =[0.5-1.5]	W_b =[0.2-1.2]
Speed	15m/s	17m/s
ROCC	5 degrees/s	10 degrees/s

As discussed above, *CS1* alone is not sufficient to classify a track as anomalous. It needs to be used in conjunction with the second signature *CS2*. The various thresholds used to analyse the data using the tool are listed in Table 1. Unlike *CS1*, *CS2* has no upper limit numerically. A too low value and a too high value are both indicators of a suspicious track (with clustering). Hence the thresholds on CS2 include a lower bound and an upper bound. The first threshold we used for CS2, (0.5 <=CS2 <= 1.5) is named as W_a and the second threshold (0.2<=CS2<=1.2) is named as W_b for simplicity of notation.

After a data set is analysed by the tool, every track is labelled with a number of red flags (normalised with respect to the track length) corresponding to speed limit and ROCC limit. Apart from varying the threshold values, one can also vary other factors, like "allowed number of red flags per km".

For example, when a given set of data is tested with the Threshold set #1, it means that a track is "non-anomalous" (or normal) only if all the following conditions are satisfied.

a) Its CS1 >= 0.5
b) Its CS2 lies within the values of 0.5 and 1.5
c) Its speed doesn't exceed 15m/s consistently for a pre-set number of times continuously
d) Its turn rate does not exceed 5 degrees/s for a pre-set number of continuous time intervals.

A track that fails even one of the above tests is deemed "anomalous".

The various combinations of the thresholds yielded 16 sets of different threshold sets which are listed below and hereafter will be referred to by their serial number.

Table 2 Combinations of thresholds in Table 1, yielding different "sets of thresholds"

Set No.	Threshold set (CS1, CS2 Window, Speed , ROCC)
1	(0.5, W_a , 15, 5)
2	(0.5, W_a , 15, 10)
3	(0.5, W_b , 15, 5)
4	(0.5, W_b ,15, 10)
5	(0.5, W_a , 17, 5)
6	(0.5, W_a , 17, 10)
7	(0.5, W_b , 17, 5)
8	(0.5, W_b , 17, 10)
9	(0.7, W_a , 15, 5)
10	(0.7, W_a , 15, 10)
11	(0.7, W_b , 15, 5)
12	(0.7, W_b 15, 10)
13	(0.7, W_a , 17, 5)
14	(0.7, W_a , 17, 10)
15	(0.7, W_b , 17, 5)
16	(0.7, W_b , 17, 10)

From Table 2 it can be understood that the sets, when ordered in decreasing order of stringency, would appear as 11, 15, 12, 16, 9, 13, 10, 14, 3, 7, 4, 8, 1, 5, 2, and 6. All the 16 sets of thresholds were used with a limit on normalised flag count (speed and ROCC) of 5 per km.

The number of tracks classified as "anomalous" for each set of thresholds is listed in Table 3 for both the data sets. The number in brackets indicates the total number of tracks analysed in that data set. The sets are listed in decreasing order of stringency. As we would expect the most stringent set of conditions (Set 11) has the greatest number of anomalous tracks, while the least stringent set of conditions (Set 6) has the smallest number of anomalous tracks.

Figures 5 and 6 depict some randomly selected anomalous tracks and good tracks, respectively, from the 2007 August data set tested with Threshold set 1. From Figures 5 and 6, the difference between the anomalous tracks and non-anomalous tracks is clear.

Table 3 Number of tracks qualified as "anomalous" for all the threshold combinations, for both the data sets.

Set Number	Anomalous Tracks			
	May 2007 Total Tracks = 560		August 2007 Total tracks =1438	
	Number	Percentage	Number	Percentage
11	347	62 %	1073	75%
15	347	62%	1069	74%
12	345	61%	1054	74%
16	345	61%	1053	73%
9	331	59%	1049	73%
13	331	59%	1045	72%
10	327	58%	1032	73%
14	327	58%	1028	71%
3	309	55%	954	66%
7	309	55%	935	65%
4	301	53%	935	65%
8	301	53%	916	63%
1	276	49%	893	62%
5	274	49%	872	60%
2	260	46%	868	60%
6	258	46%	845	59%

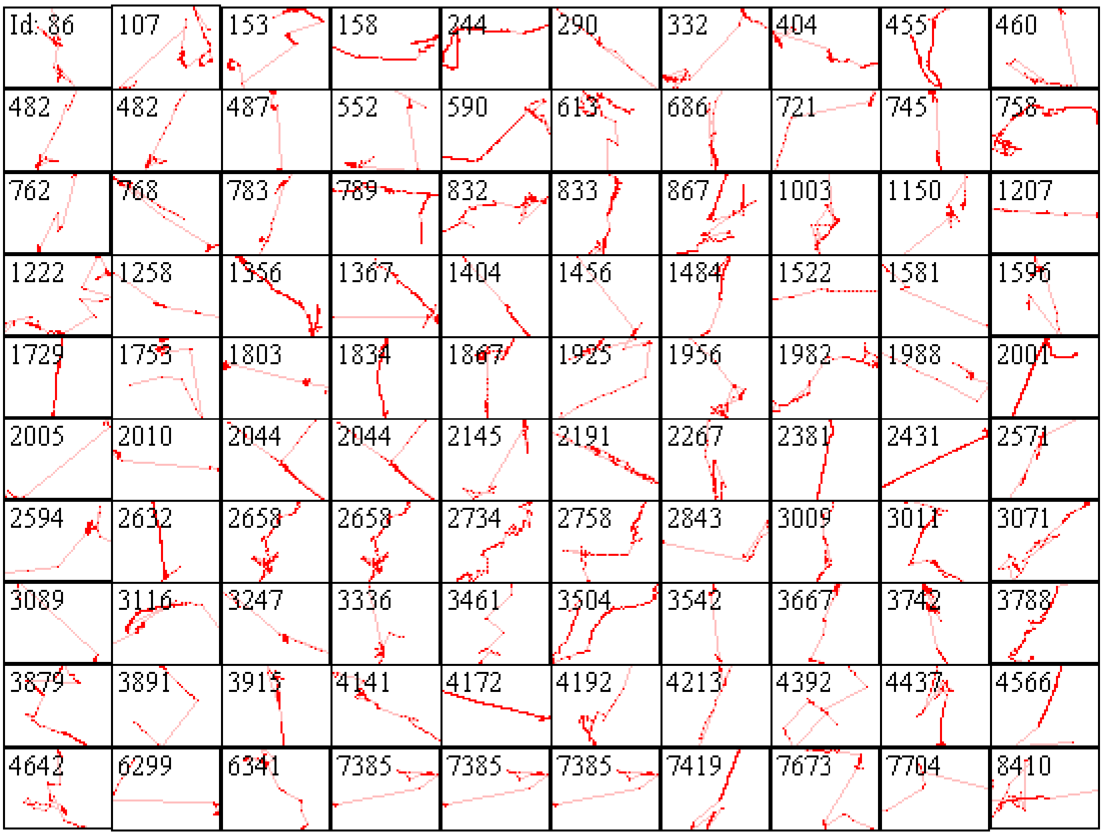

Figure 5 Randomly selected sample of anomalous tracks

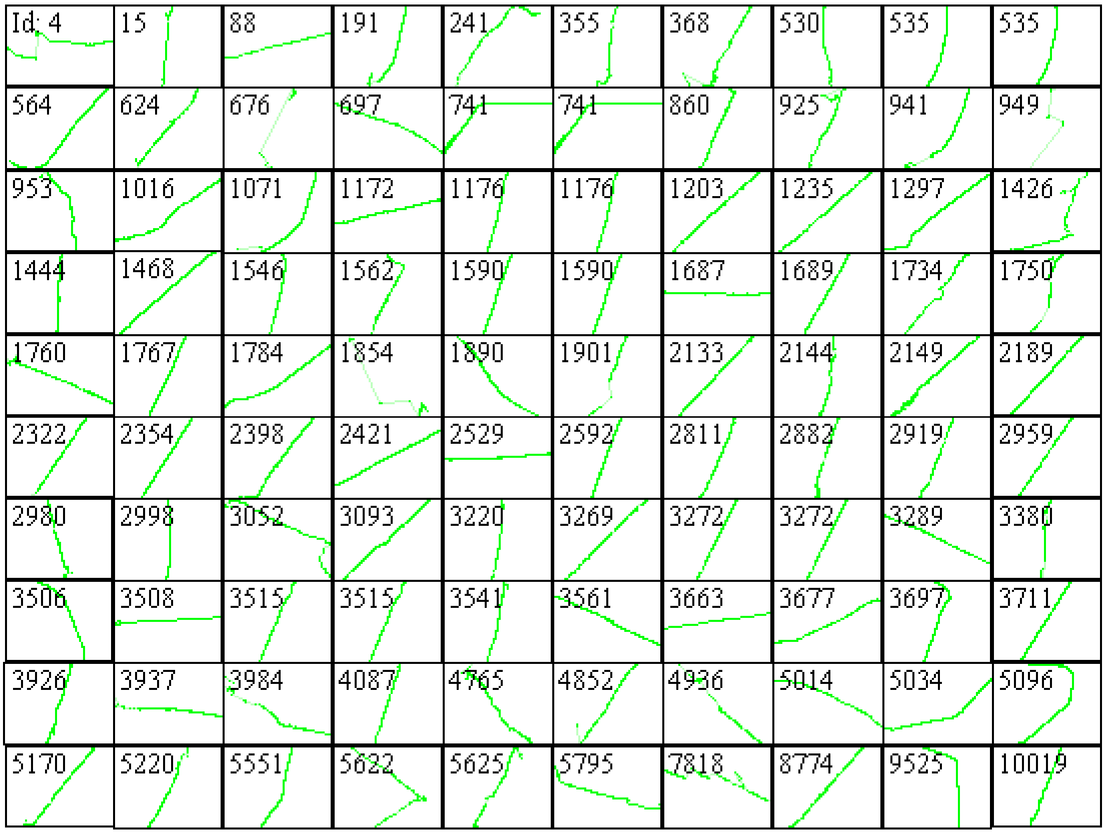

Figure 6 Randomly selected sample of non-anomalous tracks

7.3 Verification of results

7.3.1 Visual Inspection

For an independent verification, the results of the tool were also verified against a visual inspection of a sample data set. We provide a brief discussion of the verification.

A sample of 200 randomly selected tracks from each of the data sets (2007 May and 2007 August) were provided to a navy Combat System operator (CSO), who is a subject matter expert (SME) in track analysis. The CSO was also provided with a tool that could plot the track, speed and weave of any selected track from the data set. The CSO was requested to visually inspect the plots and make a decision about the quality of the track and qualify the track as "normal" or "anomalous".

The results of the visual inspection were compared against the results of tool on the same set of tracks. Table 4 captures the results of visual inspection of the 2007 May data. The third column in the table gives the number of tracks for which the tool and the visual inspection are in agreement (irrespective of the classification being 'normal' or 'anomalous').

Table 4 Results of a visual inspection of sample data from May 2007 tracks.

Set Number	Total Tracks examined	Agreement with the tool	Percentage of agreement
6	198	163	82
3	198	170	85
14	198	165	83
11	198	169	85

Similar visual inspection of randomly selected tracks from the 2007 August data yielded the following table.

Table5 Results of a visual inspection of sample data from August 2007 tracks.

Set Number	Total Tracks examined	Agreement with the tool	Percentage of agreement
6	264	218	82
3	264	210	79.5
14	264	209	79
11	264	202	76.5

Further analysis of the results of visual inspection indicated that the disagreement was greater for the anomalous tracks than for the non-anomalous tracks. The agreement on the tracks classified as non-anomalous by the tool was about 70%, while that on the tracks classified as anomalous was about 90% (averaging approximately 80% in the table above). This implies that the tool tended to err on the safe side i.e., the tool classified more tracks as anomalous than the navy operator did. This is indicative of an expected false alarm rate.

It is important to note here that visual inspections tend to be subjective and it is difficult to draw hard conclusions from them. While also agreeing that a single visual inspection is inadequate, we wish to point out that the analysis here is at a proof-of-concept phase and will undergo more rigorous testing before developing into a full-fledged anomaly detection tool. The rigorous testing should include multiple visual inspections by different operators, and comparing the performance against other independent established tools.

8. Conclusion

We developed an anomaly detection tool that uses a rule-based algorithm. The rules are pre-set on the track characteristic features, including curvature, speed and weave rate. The tool is a batch algorithm that processes recorded data.

The tool was tested on simulated data and two sets of data recorded near Sydney Harbour using various combinations of threshold values for two curvature measures, speed and rate of change of course to identify tracks exhibiting anomalous behaviour. The results of these tests were validated against visual inspection. The validation yielded approximately 80% agreement between the tool and the visual inspection. But the visual inspection was done only on a randomly chosen subset of the total tracks. While this agreement is sufficient to accept as a proof-of-concept, a more exhaustive testing of perhaps the entire data set with multiple visual inspections or a validation against another tool needs to be done for higher confidence.

The thresholds that were used for the tool in this study are perhaps too strict given that in most instances the datasets were classified with around 50% of tracks being anomalous.

The use of a sensor with adequate accuracy is vital and the sensor should be capable of detecting small watercraft. AIS data provides clean tracks, but this is not always available for smaller watercraft. AIS data used in conjunction with raw sensor data would be a desirable approach.

The available datasets used for testing contained only simple kinematics. The inclusion of additional information in the datasets such as the physical size of the tracked object, and whether it is civilian or commercial would be beneficial to the algorithms. The values of such parameters would have a significant impact on the expected behaviour and what is considered to be normal. For instance a commercial cargo-shipping vessel would be expected to be more constrained and follow a more uniform path along shipping lanes, whereas a smaller pleasure craft may deviate in its course and speed irregularly and travel in a non-uniform and somewhat random manner.

The tool needs the dataset to be cleaned of noise and clutter. Otherwise, it classifies all the noisy tracks as “anomalous”. Therefore it is likely to perform better with AIS data than with primary radar data.

Rule-based algorithms are transparent, easy to use, and use less computation time than the algorithms that need a training data set. In addition, they can handle huge amounts of data. However, if the rules are set incorrectly, it can lead to high false alarm rate. Therefore care must be taken in setting the pre-defined rules and parameters appropriately. If the rules are set with caution, the variation in results is small (not very sensitive to the values of thresholds, if the thresholds are chosen wisely). Historical data helps in setting the threshold values on track features. If there are no historical data available, the setting of rules might be tricky. The other issue is, once the rules are set, it is difficult to change them midway through a run. Therefore, there is no way for the algorithm to correct itself with the help of incoming data. A possible improvement might be using an adaptive or moving threshold window for each track feature.

Currently the tool uses just two options, “normal track” or “anomalous track”. The algorithm can be improved by including intermediate stages, with probabilities attached to them.

A natural extension of this tool would be to make it applicable to real time sequential use on a vessel. Such a decision aid would considerably reduce operator work load by drawing attention to ambiguous and anomalous tracks and also avoid errors due to operator fatigue. However, the anomaly detection tool would have to undergo more exhaustive testing before being deployed operationally.

9. References

1. Lane R., Nevell D., Hayward S., Beaney T., “Maritime Anomaly Detection and Threat Assessment”, Conference on Information Fusion, 2010.
2. Will J., Peel L., Claxton C., “Fast Maritime Anomaly Detection Using Kd-Tree Gaussian Processes”, Conference Proceedings, 2 IMA Conference on Mathematics in Defence, 2011.
3. Picicarelli C., Foresti G., “Trajectory-Based Anomalous Event Detection”, IEEE 2008.
4. Mascaro S., Korb K.B., Nicholson A.E., “Learning Abnormal Vessel Behavious from AIS Data with Bayesian Networks at Two Time Scales”, Bayesian Intelligence Publications, http://bayesian-intelligence.com/publications/TR2010_4_AbnormalVesselBehaviour.pdf .
5. B.Ristic, N.Gordon, J.Legg, “Clustering Motion Trajectories with Outliers Using Gaussian Mixtures”, DSTO report 2009, http::/dspace-dsto.dso.defence.gov.au/dspace/handle/dsto/8039.

6. Kadar I., “Perceptual Reasoning Managed Situation Assessment for harbour protection”, Springer Science 2009.
7. Jasenvicius R., Petrauskas V., “Fuzzy expert maps for risk management systems”, US/EU-Baltic International Symposium, IEEE 2008.

Page Classification: UNCLASSIFIED

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION **DOCUMENT CONTROL DATA**	 1. DLM/CAVEAT (OF DOCUMENT)
2. TITLE Threat Intent Assessment for Force Protection- A Rule-based Track Anomaly Detection Algorithm	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION) Document (U) Title (U) Abstract (U)
4. AUTHOR(S) S. Boinepalli and A.J.Knight	5. CORPORATE AUTHOR

6a. DSTO NUMBER DSTO-TR-3012	6b. AR NUMBER AR 016-062	6c. TYPE OF REPORT Technical Report	7. DOCUMENT DATE August 2014

8. FILE NUMBER 2013/1187577/1	9. TASK NUMBER NAV07/392	10. TASK SPONSOR COM WAR	11. NO. OF PAGES 17	12. NO. OF REFERENCES 7

13. DSTO Publications Repository http://dspace.dsto.defence.gov.au/dspace/	14. RELEASE AUTHORITY Chief, Weapons and Combat Systems Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS

Anomaly Detection, Force Protection

19. Abstract

We developed an anomaly detection tool using a Rule-based Algorithm that can detect anomalies in a set of pre-recorded tracks using their curvature, speed and weave. We devised a method that can quantify the amount of curvature in a recorded surface track. The anomaly detection tool uses the limiting values for curvature, speed and weaving provided by the user to classify a track as "normal" or "anomalous".

We tested two data sets consisting of radar tracks recorded in May and August 2007. We varied the threshold values that the tool uses. We compared the results of the tool's analysis of the data sets with a visual inspection performed by a navy combat system operator. The results of the tool's analysis were in good agreement with those of the visual inspection.

Page Classification: UNCLASSIFIED