LITERATURE REVIEW: Parallel Risk Evaluation for Maritime Assets

Alexander Teske
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, Canada K1N 6N5
atesk062@uottawa.ca

October 18, 2016

1 Introduction

The Risk Management Framework (RMF) is a modular system for managing risk in generic distributed systems. One of the modules, "risk assessment" is responsible for assessing the risk level of each system unit in the environment. As the number of system units grows, this becomes an increasingly expensive operation. This can be a real hindrance given that the RMF is intended to provide results in real-time.

An example of a domain where the RMF can be applied is maritime domain awareness (MDA), particularly maritime risk assessment. Here the system units are vessels at sea, and risk factors range from the possibility of two vessels colliding to the possibility of hostile actions against a vessel. Given the massive number of vessels which can potentially be at sea at any given time, a concern is that the risk assessment step can become a bottleneck for the RMF.

The objective of this research is to parallelize the risk assessment step of the RMF. The hope is that this will increase the RMFs ability to assess the risk values for large numbers of systems units in real-time.

To the best of my knowledge there have been no efforts to parallelize calculations in the maritime domain awareness domain, nor have there been any efforts to parallelize the RMF.

2 Literature Review

2.1 Maritime Domain Awareness and Maritime Risk Assessment

Maritime Domain Awareness (MDA) is defined as the situational understanding of activities that impact maritime security, safety, economy or environment. One goal of MDA is to effectively coordinate assets to respond to illegal activities, disaster situations, and rescue scenarios in the maritime domain [1].

Maritime risk assessment is a task within MDA that involves monitoring and managing risk, for example the risk of two vessels colliding. There are many potential data sources which can be inputted to maritime risk assessment systems. Typically, these sources are classified as hard vs. soft. Hard data tends to be reliable, with a high sampling rate and good precision. Examples of this include radar data and automatic identification system (AIS) data. Soft data is usually considered less reliable. It may have an infrequent sampling rate and can be less precise. Examples of this include human recorded data such as field reports or text mining data.

To be effective, a maritime risk assessment system must be able to ingest large volumes of such data and produce outputs in real-time. The system must deal with data sources with high volume, velocity, veracity, and variety. Thus, maritime risk assessment can be considered a big data problem.

Many techniques have been put forward to handle the big data problem introduced by MDA. Hidden Markov Models (HMM) [7] [9] have been proposed to monitor risk in networks. However, [3] points out that HMMs but can be unstable in dynamic situations such as MDA. In particular, if several interconnected HMMs are used in maritime monitoring, a single change in the environment would require all models to be updated. This quickly becomes prohibitively expensive.

Recently, [8] used genetic programming and linear scaling along with AIS data to perform vessel path prediction. This approach was shown to outperform two different versions of genetic programming as well as three non-evolutionary algorithms.

[10] applied Bayesian belief networks to assess risk for vessels in the approach channel of the Tianjin port. This work identified areas where traffic was being managed inefficiently. However, the approach was tested on a dataset of only 234 collision reports. Furthermore, the timeliness of the calculation was not reported.

In [6], artificial neural networks were used to combine data from multiple optical sensors (e.g. visual, thermal, multi-spectral) to classify maritime targets in near real-time.

2.2 Risk Management Framework

The Risk Management Framework (RMF) is a modular system for managing risk within generic distributed systems in real-time. It was first proposed by Falcon et all in [5]. The primary functions of the RMF are (1) to assess the risk level for system units using data reported from the units themselves, (2) visualizing the risk landscape for human operators, and (3) generating potential responses to mitigate risk in the environment. In essence, the potential responses create a closed loop between the RMF and the environment; once the response is enacted upon the environment, the risk landscape changes and the risk values are reassessed.

In [2] the RMF was applied to the maritime domain. Here the system units are vessels at sea, and risk factors such as risk of collision with another vessel and regional hostility are calculated using information such as each ship's position, heading, and speed. When a vessel's risk level exceeds an acceptable threshold, the vessel is deemed a *vessel in distress* (VID). Vessels in distress must assisted in what is called a search and rescue (SAR) mission. This mission involves one or more vessels in the vicinity of the VID coming to the aid of the distressed asset. The RMF is capable of identifying VIDs and generating potential SAR missions using the remaining maritime assets. The potential responses are ranked according to several competing objective functions and the best ones are presented to a human operator.

In [4] the RMF, as applied to the maritime domain, was augmented with the ability to ingest soft data such as textual reports of maritime incidents. It was shown that the approach effectively converted soft information into quantitative data which could be used to evaluate risk.

References

[1] Rami Abielmona. Tackling big data in maritime domain awareness. *Vanguard Magazine*, Aug/Sep:42–43, 2013.

[2] R. Falcon and R. Abielmona. A response-aware risk management framework for search-and-rescue operations. In *2012 IEEE Congress on Evolutionary Computation*, pages 1–8, June 2012.

[3] R. Falcon, R. Abielmona, S. Billings, A. Plachkov, and H. Abbass. Risk management with hard-soft data fusion in maritime domain awareness. In *the 2014 Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pages 1–8, Dec 2014.

[4] R. Falcon, R. Abielmona, S. Billings, A. Plachkov, and H. Abbass. Risk management with hard-soft data fusion in maritime domain awareness. In *the 2014 Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, pages 1–8, Dec 2014.

[5] R. Falcon, A. Nayak, and R. Abielmona. An evolving risk management framework for wireless sensor networks. In *2011 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA) Proceedings*, pages 1–6, Sept 2011.

[6] M. Pothitos, M. Tummala, J. Scrofani, and J. McEachen. Multi-sensor image fusion and target classification for improved maritime domain awareness. In *2016 19th International Conference on Information Fusion (FUSION)*, pages 1170–1177, July 2016.

[7] X. Tan, Y. Zhang, X. Cui, and H. Xi. Using hidden markov models to evaluate the real-time risks of network. In *Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on*, pages 490–493, Dec 2008.

[8] Leonardo Vanneschi, Mauro Castelli, Ernesto Costa, Alessandro Re, Henrique Vaz, Victor Lobo, and Paulo Urbano. *Improving Maritime Awareness with Semantic Genetic Programming and Linear Scaling: Prediction of Vessels Position Based on AIS Data*, pages 732–744. Springer International Publishing, Cham, 2015.

[9] Yuping Wang, Yiu-ming Cheung, and Hailin Liu, editors. *Computational Intelligence and Security, International Conference, CIS 2006, Guangzhou, China, November 3-6, 2006, Revised Selected Papers*, volume 4456 of *Lecture Notes in Computer Science*. Springer, 2007.

[10] Jinfen Zhang, ngelo P Teixeira, C. Guedes Soares, Xinping Yan, and Kezhong Liu. Maritime transportation risk assessment of tianjin port with bayesian belief networks. *Risk Analysis*, 36(6):1171–1187, 2016.