A Multi-Agent System for Tracking the

Intent of Surface Contacts in Ports and Waterways

ABSTRACT

Maritime security is especially critical for countries like Singapore, an island nation situated on one of the world's busiest shipping routes, and whose economic prosperity is highly dependent on international trade at its busy port, trans-shipment container terminals, petrochemical complexes and other high-value units located along its coastline. Recent incidents have brought into focus the reality of asymmetric maritime terrorism and the vulnerabilities of ports, waterways and shipping routes.

This article is extracted from the author's recent thesis, inspired by similar work done in the area of air threat assessment. The thesis adopts the ideas and techniques suggested for identifying air threats and uses them in identifying asymmetric maritime threats in a multi-agent system (MAS) for the relatively less investigated but very important area of port and waterways security.

The thesis also features a mock Vessel Traffic System - Command and Control system to evaluate the MAS. Simulations of scenarios with hostilities in the port of Singapore and surrounding waterways test the ability of the models to identify the intent of multiple simulated surface contacts by blending data and information into integration networks. Expansion of the integration networks can yield the intent identification process of a surface contact used by the compound MAS. Face validation by domain experts generated very encouraging results.

Oliver Tan

A Multi-Agent System for Tracking the

Intent of Surface Contacts in Ports and Waterways

BACKGROUND

The Port of Singapore is one of the busiest in the world. It is the focal point of approximately 200 shipping routes that connect Singapore to more than 600 ports in 120 countries, and there are about 1,000 ships in the port at any time[1] (Lewis, 2002). A stone's throw away from the port is the Singapore Cruise Centre, the cruise hub of the Asia-Pacific for passenger liners as well as regional and domestic ferries[1]. Located on nearby offshore islands are oil terminals and refineries managed by many multi-national petroleum companies[2]. Each day, hundreds of vessels of all sizes, ranging from small dinghies and bum-boats to large cruise liners and oil tankers, traverse the deep but narrow band of sea surrounding the island[3]. The Maritime Port Authority of Singapore (MPA) is responsible for overseeing and monitoring the vessel movements in the sea-lanes, ensuring navigational safety in the port and managing the marine environment around the island[4] .

The defence of Singapore Territorial Waters (STW) against potential sea threats lies in the hands of the Singapore Police Coast Guard (PCG) and the Republic of Singapore Navy (RSN). Both agencies work together to combat and deter sea robberies, piracy and hijacks[5]. Although well guarded by the PCG and RSN, the waters around STW remain vulnerable. The Straits of Malacca has received much attention for attacks against vessels at sea (Davis, 2004). However, in terms of relative risk, it is less dangerous than the zone east of Bintan Island. Bintan and neighbouring Batam Island, a free-trade zone that is just outside the STW, have long been recognised as venues where organised crime syndicates and pirate gangs meet, do business and plan major attacks (Davis, 2004). In these waters, ships are like "sitting ducks" as they tend to concentrate and slow as they approach the Straits of Singapore (Davis, 2004).

The types of maritime threats and the ways they can be executed are numerous and unpredictable. For example, terrorists on a perfectly legitimate cruise liner can scuttle it when it is approaching the cruise centre, potentially shutting down the waterways to the port. It is also possible for terrorists to hijack a vessel and ram it against the cruise centre, a container terminal or an oil refinery (Rohan, 2002). Deception and surprise are also tools used by maritime terrorists against naval ships. Even if a naval ship was fitted with long-range guns, a terrorist group can conduct a "wolf-pack" attack where a cluster of terrorist craft simultaneously overwhelms a target craft from multiple directions (Rohan, 2002).

EFFORTS TO ENHANCE INTERNATIONAL MARITIME SECURITY

In November 2001, the International Maritime Organisation (IMO) Assembly adopted a resolution to develop appropriate measures to enhance maritime security in order to preclude a terrorist attack from the sea. In December 2002, the IMO adopted new maritime security measures that included amendments to the 1974 Convention of Safety of Life at Sea (SOLAS 74) as well as a new mandatory International Ships and Port Facilities Security (ISPS) Code (Englebert, 2003). Some of the amendments that have already been adopted or extended by the MPA include:

- The installation of shipboard Automatic Identification Systems (AIS) (Maritime and Port Authority of Singapore, 2003a; International Maritime Organisation, 2001)
- The equipment of silent ship-to-shore security alert systems (Maritime and Port Authority of Singapore, 2004a)
- The request for information related to ship security that a ship may be required to provide prior to entering the port as well as an initial inspection of the ship when in the port (Maritime and Port Authority of Singapore, 2003b)
- The need for vessels to maintain a continuous record of registration, ownership and other information that can be used by port control officers to assess any security risk (Maritime and Port Authority of Singapore, 2004b)

- The extension of the ISPS Code to include mandatory compliance by small vessels and harbour craft that operate solely within the port limits (Maritime and Port Authority of Singapore, 2004c)

A MULTI-AGENT SYSTEM FOR SURFACE CONTACT INTENT TRACKING

The three main agencies that provide surveillance of the waters around Singapore are the MPA, PCG and RSN. As they focused on different areas and regions, it is therefore possible for each agency to develop different surveillance blind spots. A composite surveillance picture may help to mitigate the effects of the surveillance blind spots for each agency. Many information and intelligence sources contribute to a composite surveillance picture. Some important information sources include the Port Traffic Management System (PTMS) and the Vessel Traffic Information System (VTIS) that are used to manage vessel traffic in harbours and waterways[6].

However, with a monthly record of almost 11,000 vessel arrivals into the Port of Singapore[3], and many more unrecorded smaller leisure and fishing vessels, the number of surface contacts presented on a common composite surveillance picture is still overwhelming. It would be very difficult for port control officers to identify surface contacts with mischievous or potentially hostile intention before they strike. Furthermore, knowing the identity of surface contacts is insufficient for discovering potential incoming threats to civilian or military craft.

The idea of using a multi-agent system (MAS) for the identification of potentially hostile behaviour and potential threats in ports and waterways is inspired by Ozkan's work in an autonomous agent-based simulation system for air-threat assessment (Ozkan, 2004). The simulation system incorporated the idea of conceptual blending (Giles and Turner, 2002) together with the research by Amori on a multi-agent system for adversarial plan recognition (Amori, 1992) and Liebhaber's study on airborne threat assessment (Liebhaber and Smith, 1999), to build a model that is capable of predicting the intent of air tracks. Besides predicting track intent, the system was also able to identify co-ordinated activities between air tracks.

Together with ideas from Liebhaber's preliminary research in surface warfare threat assessment (Liebhaber and Feher, 2002), a MAS for threat assessment can be applied in the domain of surface contact intent tracking. The MAS can sieve through hundreds of surface contacts in a composite surveillance picture and highlight any suspicious or potentially hostile tracks. The MAS integrates rules, track attributes and threat assessment cues into intent models. It also uses information provided under the new amendments to the SOLAS convention (Engelbert, 2003). These include the shipboard AIS, registries of vessel registration, vessel ownership, cargo manifests, and vessel transit schedules. All surface contacts that are within the port and STW are also monitored by the MAS for suspicious behaviour. Such behaviour may include loitering, violations of international navigation rules, encroachment into restricted areas, aggressive manoeuvres and even unusual co-ordinated activities among surface contacts.

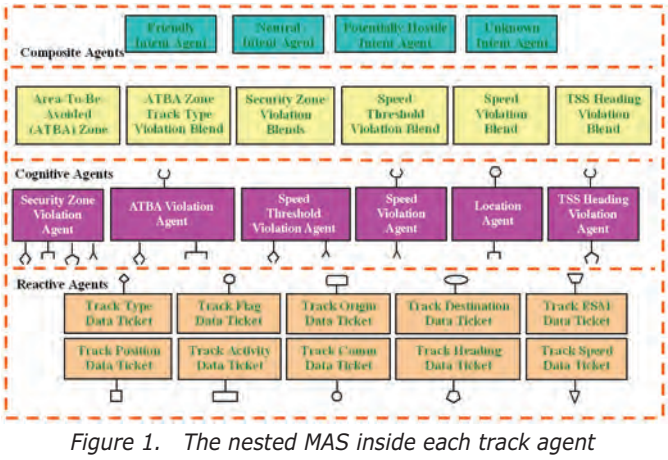

Figure 1. The nested MAS inside each track agent

THE MULTI-LAYERED ANATOMY OF A TRACK AGENT

Every surface contact is represented by a track agent in the MAS. Each of these track agents also contains another MAS so the overall system can be considered a compound MAS. The layered agent architecture nested inside every track agent is shown in Figure 1. There are four layers of agents working in tandem. Information propagates upwards from the lower layers. The information may be processed further to infer more information about a track and the new information is also propagated upwards. Finally, the topmost layer consists of intent agents that decide the current intent of a track.

1. The Layer of Track Data Agents

The lowest level consists of purely reactive data agents, also known as "data tickets". Their primary function is to act like an interface to the outside world and to carry track data from the outside world into the internal MAS environment where all the other agents reside. The cognitive agent layer above will use the information provided by this layer of track data agents.

2. The Layer of Cognitive Agents

The cognitive agents use the information provided by the lower level of data agents to make inferences to discover if a track is

- in a special area like a traffic separation scheme (TSS) or restricted area
- violating any rules or travelling in a dangerous or atypical manner

a. The Location Agent

The Location Agent uses the track's current position to decide whether the track is inside a special area e.g. in a TSS, or inside a restricted zone where rules on track type, speed, activity and other track attributes may apply. This is achieved by investigating user-defined locations and sizes of the TSSs and restricted zones.

b. TSS Heading Violation Agent

A TSS is a sealane with a predefined traffic direction that has been designated by a Vessel Traffic Service operating in a harbour. Under Rule 10 of the International Navigation Rules formalised by the IMO at the Convention on the International Regulations for Preventing Collisions at Sea 1972 (72COLREGS), "a track using a traffic separation scheme shall proceed in the appropriate traffic lane in the general direction of traffic flow for that lane"[8]. If the MAS finds a track violating the traffic direction of a TSS, a TSS heading violation occurs.

c. Speed Violation Agents

Rule 6 of the 72COLREGS states that "every vessel shall at all times proceed at a safe speed so that she can take proper and effective action to avoid collision and be stopped within a distance appropriate to the prevailing circumstances and conditions"[8]. Safe speed is also related to the "manoeuvrability of the vessel with special reference to stopping distance and turning ability"[8].

A TSS may have minimum and maximum speed limits that tracks travelling inside a TSS are expected to comply with for prudent seamanship. There can also be minimum and maximum speed limits defined for other designated areas e.g. in a harbour where there is high traffic density. A speed violation occurs when a track fails to comply with the speed limits defined in these areas. Besides pre-defined speed limits for designated areas, the MAS also checks for speed limits defined for different track types. Different track types can have different maximum speed limit thresholds. If a track is found to be travelling at an atypically excessive speed based on its track type, the system detects a speed threshold violation.

d. Security Zone Violation Agent

Cruise liners, tankers, ferries, military craft are examples of High Value Units (HVUs). The MAS will help monitor for potentially hostile intent against these HVUs by encircling them

with user-defined security zones (Department of Homeland Security and United States Coast Guard, 2003a; Department of Homeland Security and United States Coast Guard, 2003b).

Only certain types of pre-defined tracks such as PCG craft may be allowed within these security zones. Each security zone is associated with an alert time which can be considered as a user-defined time required by a HVU to respond when another track encroaches into one of its security zones. As HVUs move, the MAS continuously monitors the Closest Point of Approach (CPA) and Time to CPA (TCPA) of other tracks around it. When an unauthorised track has a CPA that falls within a security zone of a HVU and its TCPA is less than the Alert Time defined for the zone, a security zone violation occurs, as shown in Figure 2. Security zones can also be defined for static HVUs e.g. military installations, oil refineries, ferry terminals that may be located near or on the coast.

Figure 2. Security Zone Violation

e. Area-To-Be-Avoided Violation Agent

An Area-To-Be-Avoided (ATBA) is defined by the IMO as "an area that all ships or certain classes of ships should avoid because navigation is particularly hazardous or it is exceptionally important to avoid casualties within the area" (Department of Commerce and National Oceanic Atmosphonic Adminstration, 2002). ATBAs may also be defined near restricted areas, such as oil refineries and military installations. Only certain types of tracks and track activities may be allowed within these ATBAs. The MAS detects an ATBA violation when an unauthorised track intrudes into an ATBA.

TRACK VIOLATIONS AND COGNITIVE BLENDING OPERATIONS

The theory of conceptual blending is one possible explanation for how humans are able to think, give meaning to external information and events, compressing the information into integrated networks and eventually learning and gaining experience. Conceptual blending is a set of mental operations for combining cognitive models in a network of discrete mental spaces. Mental spaces are connected to long-term schematic knowledge called "frames" such as the frame of sailing inside a maritime TSS, and to long-term specific knowledge such as a memory of an event such as past track incursions into ATBA zones. Within the mental spaces are elements of these types of knowledge that are structured by frames (Giles and Turner, 2002). A critical aspect of conceptual blending is the finding of relations between the mental spaces that lead to the blend. The theory calls these all-important relations "vital relations". The links between input mental spaces, known as "outer-space" links can be compressed into relations, known as "inner-space" relations, inside the blend itself (Giles and Turner, 2002).

Figure 3. An example of a Security Zone Violation Blend

For example, a Security Zone Violation agent, through the integration of track data, rules and regulations of the VTS and other user-defined information, uses conceptual blending operations to discover track violations. A track's CPA and TCPA from an input mental

space for a track is connected, through Distance and Time Vital Relations, to another input mental space representing the definition of a security zone and the corresponding alert time around a HVU, as shown in Figure 3. Note that the input mental space of a track contains other information besides CPA and TCPA. A generic mental space is required to guide the selective projection of the relevant information into the blended space. In this case, the Violation agent provides the generic space. It contains the rules regarding the conditions that constitute a security zone violation.

The communication and co-ordination among many different agents in the nested MAS is achieved using the Connector-based Multi-agent Simulation Library (CMAS) developed by John Hiles and his team at the US Naval Postgraduate School (Naval Postgraduate School, 2004a). The basic elements for agent communication and control within the CMAS framework are connectors. The agents use these connectors to externalise portions of their internal states into the multi-agent environment. Connectors are like plugs and receptacles that can be extended or retracted as shown in Figure 4. Signalling and co-ordination between the two agents occurs when there are matching pairs of plug-receptacle connectors and they get connected.

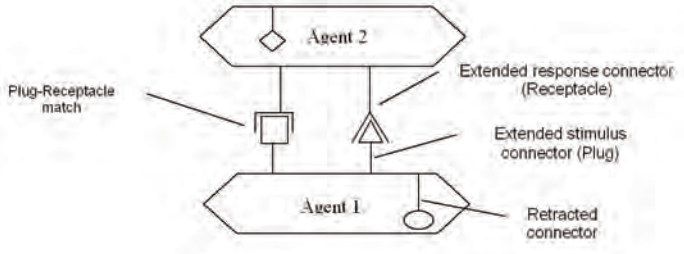

Figure 4. Connectors for agent communication and co-ordination

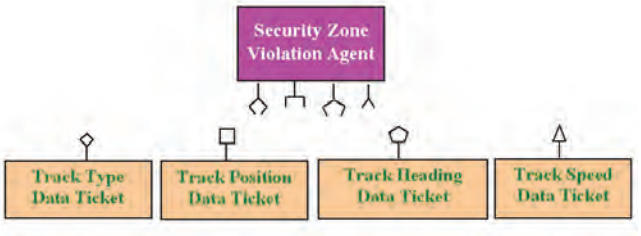

Figure 5. Using connectors to query for track data

The Security Zone Violation agent extends queries (receptacles) into the MAS environment for track data that is specified in the generic space, as shown in Figure 5. The relevant track data agents or data tickets respond to the queries, if their connectors are extended, by plugging their connectors into the corresponding receptacles and transfering the required information to the Violation agent. Based on the track's current position, speed and heading, its CPA and TCPA to surrounding HVUs are calculated by the Violation agent.

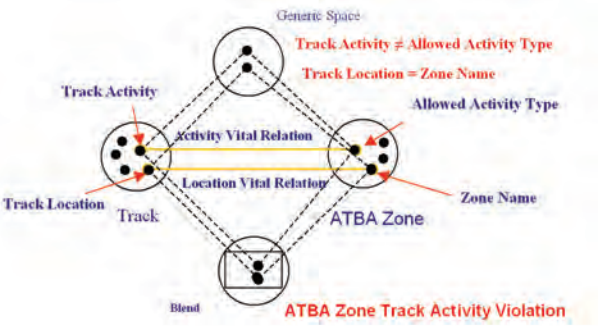

Figure 6. Example of an ATBA Zone Track Activity Violation Blend

Finally, a blended space representing a security zone violation is formed by the inference based, in this case, on the computed CPA and TCPA information projected from the input mental spaces, as shown in Figure 3. The Security Zone Violation Agent spawns the Security Zone Violation blend. The blend can be considered a simple reactive agent.

Another example of how cognitive blending operation is used to detect an ATBA Zone Track Activity Violation is shown in Figure 6. This case generates an ATBA Zone Track Activity Violation blend. These violation blends, together with other violation blends, form an intermediate layer of simple reactive agents that work with the topmost layer of intent agents.

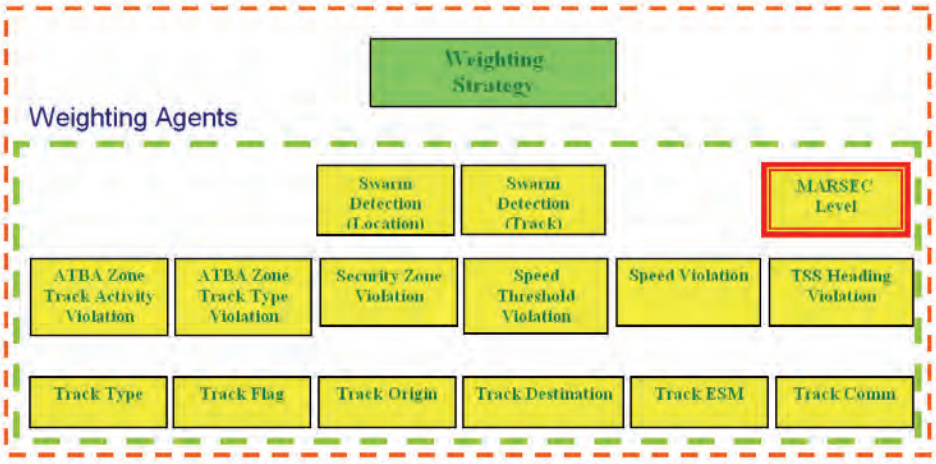

Figure 7. The nested MAS inside each intent agent

THE ANATOMY OF AN INTENT AGENT

The top layer of agents of the nested MAS environment inside a track agent comprises intent agents. There are four intent agents: Friendly, Neutral, Potentially Hostile, and Unknown. Each of these intent agents uses a family of "helper" agents as shown in Figure 7. The intent agents use information provided by agents from the lower layers. This information includes track location, violations, origin, flag, and existence of voice communication with the track, among other indicators.

The family of weighting agents is responsible for obtaining and giving significance to the information, using connectors provided by the CMAS library, from the lower layers of data agents and blends. Note that there is a one-to-one relationship between a weighting agent and a data agent or blend, as shown in Figure 8. The weighting agents then forward information received to a Weighting Strategy. The Weighting Strategy defines the intent model i.e. Friendly, Neutral, Potentially Hostile, Unknown, represented by the intent agent. The Weighting Strategy assigns user-defined weights to each piece of track information that the weighting agents receive, similar to the Threat Level Change Ratings scheme identified from the study of the surface warfare threat assessment process by Liebhaber and Feher (Liebhaber and Feher, 2002).

The Weighting Strategy associated with each intent model has a unique set of weights. When new information about a track is available from the weighting agents, all the Weighting Strategies compute a revised score using its own set of weights for the new information. Effectively, the intent models

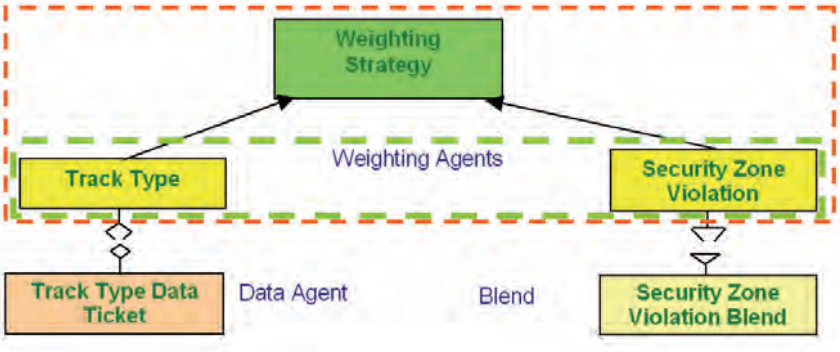

Figure 8. Interaction between the weighting agents and other agents

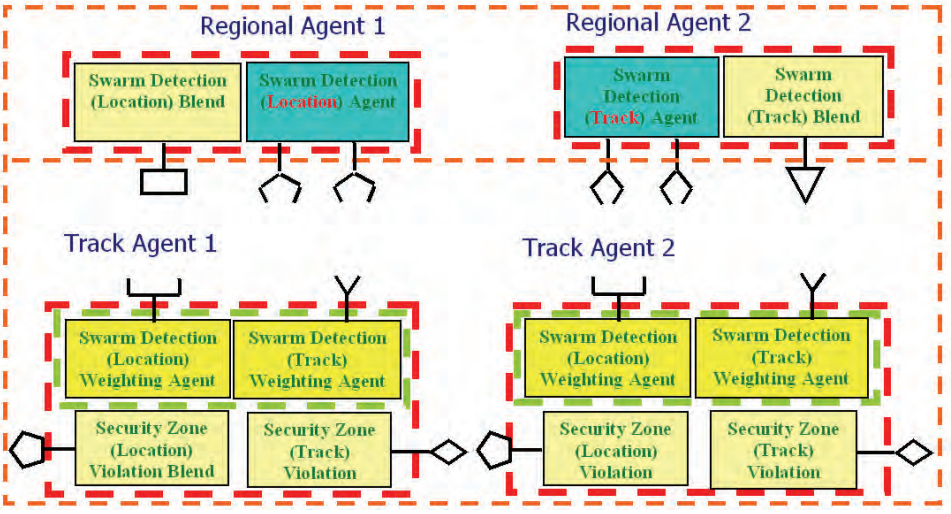

Figure 9. MAS environment of regional and track agents

compete, and the one with the highest score represents the current intent of the track.

The MAS also supports a five-level threat advisory system, similar to the Maritime Security Levels enacted by the US Coast Guard (Poulin, 2003). By defining a threat level for the MAS, a Maritime Security (MARSEC) weighting agent inside every track agent heightens or lowers the alertness of the system by causing the weighting strategies to apply appropriate biases to the intent agents.

THE REGIONAL AGENT LAYER

A track agent appears as a single agent that exists in another external MAS environment. In this external MAS environment, there is a layer of regional agents that monitor the behaviour of all the track agents, as shown in Figure 9.

Currently, two types of regional agents detect coordinated behaviour that resembles an impending swarm or a "wolf-pack" attack on a HVU, a common maritime terrorist tactic (Rohan and Chalke, 2002). Swarm Detection agents compare the Security Zone Violation blends generated by the track agents. If there are several similar violation blends by different tracks against the same HVU, the regional agent produces a Swarm Detection blend, shown in Figure 10. This blend signals the weighting strategies of the track agents suspected of participating in a coordinated

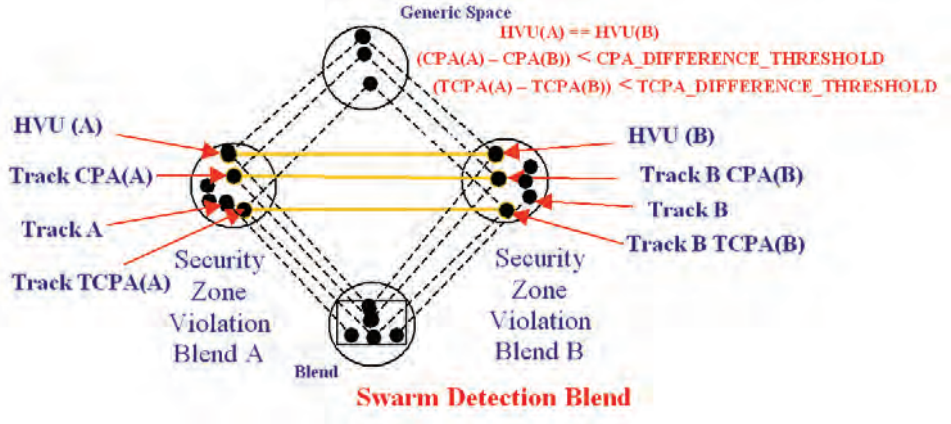

Figure 10. Example of a Swarm Detection Blend

attack. The weighting strategies then use the new information to revise the intent of the track agents involved in the co-ordinated attack.

Figure 11. The VTS-C2 MAS

VERIFICATION, VALIDATION, AND EXPERIMENTATION

To test its effectiveness, the compound MAS is integrated into a mock Vessel Traffic System-Command and Control (VTS-C2) simulation system, enabling assessment of various scenarios incorporating hostility that may exist in a harbour or surrounding waterways. Several validation sessions are conducted with maritime domain experts. The MAS and the intent models are evaluated for their effectiveness in meeting the objectives of the system. A screen snapshot of the mock VTS-C2 with the integrated MAS is shown in Figure 11. The corresponding system architecture of the mock VTS-C2 MAS is shown in Figure 12. The compound MAS is the heart of the entire system.

The user can specify the weights used by the various weighting strategies using one of several weight tables shown in Figure 13. These weight tables also include the bias settings, based on the MARSEC level setting, which the weighting strategies apply on the weights. The values of the weights and biases underlie the weighted scores computed by the competing intent models and therefore predicate the deduced intent of the surface contacts. It is also possible to set additional agent threshold parameters that the cognitive

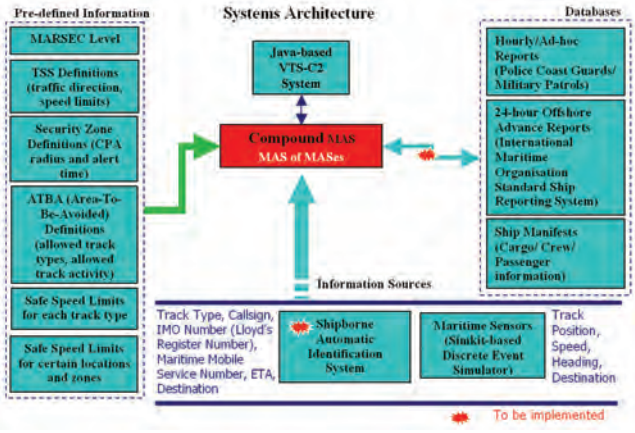

Figure 12. The systems architecture of the VTS-C2 system

agents use to detect security zone violations and coordinated attacks, as shown in Figure 14. This allows for some fine-tuning on the frequency and quantity of the violation blends produced by the cognitive agents.

The MAS reports computed intents of surface contacts through intent score graphs, shown in Figure 15. The user is also able to get more information on how the scores are computed through a corresponding set of tables shown in Figure 16. The top table shows aggregated weighted scores of the intent models within track agents representing each surface contact and the bottom table shows the breakdown of the aggregate scores into score updates and the reasons for the updates. These detailed breakdowns represent important decompressions of integration networks comprising information spaces of different

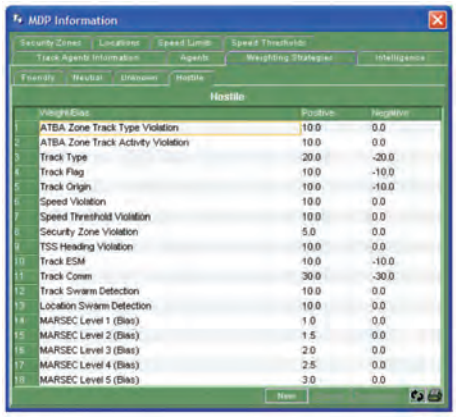

Figure 13. Weights and biases set-up screen

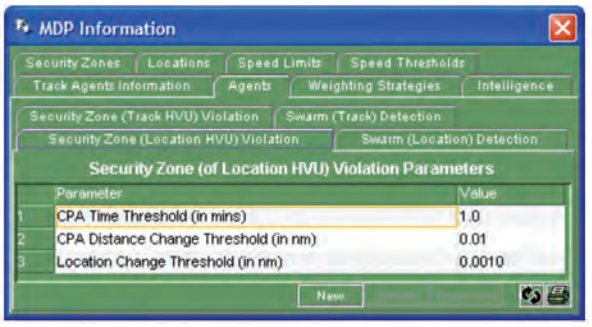

Figure 14. Agent threshold parameters set-up screen

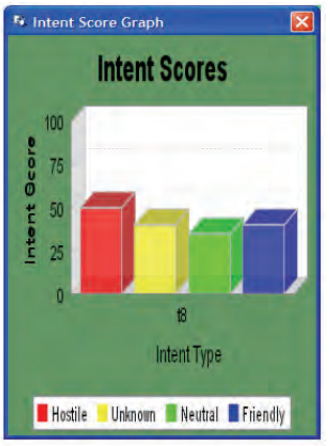

Figure 15. Intent score graph

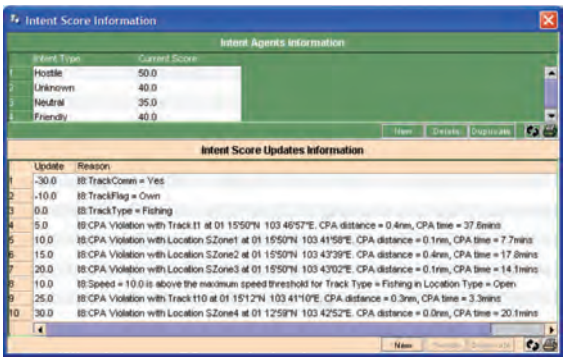

Figure 16. Breakdown of aggregated intent score

entities (tracks, TSSs, ATBAs, security zones) and blends produced by the cognitive agents. This feature of the MAS helps the user understand how track intent is deduced by the system.

The general consensus among the participants of the validation session is that the MAS is a great advancement in decision aids using compound MAS. It can be a very useful system for monitoring movement in busy ports and waterways and alerting decision-makers to potentially hostile activity. They agreed on the importance of monitoring all surface contacts, security zones of HVUs and restricted areas. However, there are also concerns that despite the large amount of information that the system is able to process, there will still be an overwhelming information glut.

With regards to ensuring that vessels comply with the safety and security rules of the port and waterways, the domain experts agreed that the MAS has met this requirement satisfactorily. However, the possible false alarms that may arise during heavy traffic conditions in the Port of Singapore may be compounded by the clutter caused by non-moving surface contacts located in many areas in the congested STW. However, it is important to note that false alarms are better than no alarms. The domain experts advised that the weights used by the system have to be calibrated carefully in order to minimise the number of false alarms.

The domain experts also agree that the system is a good "proof of concept" that demonstrates how a decision support tool can help the decision maker identify suspicious or potentially hostile surface contacts. It is important to note that system performance is highly dependent on the accuracy and reliability of information and intelligence, a point made by some domain experts during the validation sessions. Although the MAS uses information that may be obtained automatically from the ship-borne Automatic Identification System (AIS), it may also be important to explicitly consider how to interpret the presence or absence of an AIS with respect to the threat level posed by a surface contact.

RECOMMENDATIONS

Before the MAS can be used as a decision support tool, it needs to be verified that the MAS works well in real traffic situations in the waters of Singapore. Objective measures for verifying system performance may include:

- the number of Type I errors (false negatives)
- the number of Type II errors (false positives)
- the time taken by the system to identify hostilities compared to a decision-maker
- the amount of lead time the system is able to provide in situations of impending hostilities
- the number of factors that the system can process as compared to a human operator.

The MAS can also be further enhanced with the capability to detect more atypical track behaviour or manoeuvres such as:

- concealment or evasion from PCG/ military vessels.
- suspicious course changes by monitoring for course/heading of a track in more detail, for example, in terms of Steady and closing/opening or Turn to closing/opening to discover if the track is changing its course frequently to "hug" a nearby HVU.

A noted drawback of the current system is that once a track has been considered as potentially hostile, the system will not modify its designation of the track's intent i.e. the system will neither forgive nor forget the track's behaviour and violations. A future enhancement can allow the system to use a decaying intent weighting strategy that allows the gradual readjustment of track designations over a specified time constant.

The agents in the current MAS are considered "passive" consumers of information that is fed into the system. It is possible that agents can be proactive in automatically searching for more track information, i.e. form a paper trail from information sources such as databases of ship registration, sail plans, Offshore Advance reports, recent inspections or boardings, cargo/passenger manifests, etc. The system can also use context-specific intelligence based on track attributes to identify and focus on a vessel of interest. The cognitive agents can also act as proxies to external decision support services such as rule-based systems and fusion engines.

CONCLUSION

The research and work done in the MAS is timely. There is increased focus on global maritime surveillance, with the priorities placed on global maritime intelligence integration and global awareness of civil maritime activities. Preliminary validation results of the surface contact intent models and their usefulness in threat identification for maritime security are very encouraging. The models can be refined and integrated into an existing decision support system or be the basis of a future one for maritime security. Ultimately, it is hoped that the efforts and results of this research can be used to enhance the security of Singapore's sea lines of communication.

ENDNOTES

1. Maritime and Port Authority of Singapore - The Port of Singapore. http://www.mpa.gov.sg/aboutmpa/portofsg/port.htm

2. Maritime and Port Authority of Singapore - Achievements and Awards. http://www.mpa.gov.sg/homepage/achieve.html

3. Maritime and Port Authority of Singapore - Port Statistics. http://www.mpa.gov.sg/homepage/portstats html

4. Maritime and Port Authority of Singapore - Roles of the MPA. http://www.mpa.gov.sg/homepage/roles.html

5. Ministry of Defence, Ministry of Home Affairs, Singapore Police Force - News Release : Ministerial Visit to the Police Coast Guard and the Republic of Singapore Navy. http://www2.mha.gov.sg/mha/detailed.jsp?artid=393&type=4&root=0&parent=0&cat=0&mode=arc, January 2005.

6.Singapore Maritime Portal - Navigational Safety. http://www.singaporemaritimeportal.com/worldbusiestport.htm

7. Department of Homeland Security & United States Coast Guards, "Steering and Sailing Rules - Rule 6 - Safe Speed", Navigation Rules International-Inland, M16672.2D.

8. Department of Homeland Security & United States Coast Guards, "Steering and Sailing Rules - Rule 10 - Traffic Separation Schemes", Navigation Rules International-Inland, M16672.2D.

REFERENCES

Amori, R. D. (1992) An Adversarial Plan Recognition System for Multi-agent Airborne Threats. Symposium on Applied Computing (1992): 500.

Center for Strategic and International Studies (2004) Transnational Threats Update. In Transnational Threats Initiative, Vol. 2, No. 6, March 2004.

Davis, A. (2004) Piracy in Southeast Asia Shows Signs of Increased Organization. in Jane's Intelligence Review, 1 June 2004.

Department of Commerce, National Oceanic Atmospheric Administration (2002) Amendments to the Area To Be Avoided Off The Olympic Coast National Marine Sanctuary. Federal Register, Vol. 67, No. 229, November 2002.

Department of Homeland Security and United States Coast Guards (2003a) Security and Safety Zone: Protection of Large Passenger Vessels, Puget Sound, WA. Federal Register, Vol. 68, No. 61, March 2003.

Department of Homeland Security and United States Coast Guards (2003b) Safety Zone: Protection of Tank Ships, Puget Sound, WA. Federal Register, Vol. 68, No 61, March 2003.

Endsley, M. R. (1995) Toward a theory of situation awareness in dynamic systems. Human Factors, Vol 37, pp 32 - 64, 1995.

Englebert, S. E. (2003) IMO Moves to Enhance International Maritime Security. In The Coast Guard Journal of Safety at Sea Proceedings of the Marine Safety Council, Vol. 60, No. 2, pp 14 – 18, April – June 2003.

Gilles, F., and Turner, M., (2002) The Way We Think. Basic Books, New York.

International Maritime Organization (2001) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS). Resolution A.917 (22), 29 November 2001.

Klein, G. A. (1998) Sources of Power. The MIT Press, 1998.

Lewis, Brian (2002) Background Information Regarding the Port of Singapore and the Port of Savannah. In Technical Report, The Logistics Institute, Georgia Tech, and The Logistics Institute – Asia Pacific, National University of Singapore.

Liebhaber, M. J., and Smith, C. A. P. (1999) Naval Air Defense Threat Assessment: Cognitive Factors Model. Command and Control Research and Technology Symposium (1999): 2.

Liebhaber, M. J., and Feher, B. A. (2002) Surface Warfare Threat Assessment: Requirements Definition. Technical Report 1887, SSC San Diego, 2002.

Maritime and Port Authority of Singapore (2003a) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification Systems (AIS), Marine Circular to Ship, No. 15 of 2002, August 2003.

Maritime and Port Authority of Singapore (2003) Promulgation of Legislation to Effect Special Measures for the Enhancement of Maritime Security. In Port Marine Circular to Shipping Community, Harbour Craft Community, Owners and Operators of Port Facilities, No. 12 of 2004, June 2003.

Maritime and Port Authority of Singapore (2004a) Revised Performance Standards and Guidance on Provision of Ship Security Alert Systems Marine Circular to Shipowners, No. 23 of 2003, October 2004. http://www.mpa.gov.sg/homepage/ms/mc03-23.htm

Maritime and Port Authority of Singapore (2004b) Continuous Synopsis Record. In Shipping Circular to Ship Owners and Ship Managers of Singapore Ships, No. 7 of 2004, March 2004.

Maritime and Port Authority of Singapore (2004c) Harbour Craft Security Code and Security Log. In Port Marine Circular to Harbour Craft Community and Shipping Community, No. 18 of 2004, June 2004.

Naval Postgraduate School (2004) "CMAS System Library User's Guide", Revision 1.1, Naval Postgraduate School.

Naval Postgraduate School (2004) "Red Team Intent User's Guide", Naval Postgraduate School.

Ozkan, B. E. (2004) Autonomous Agent-Based Simulation of a Model Simulating the Human Air-Threat Assessment Process. Masters Thesis, Naval Postgraduate School, Monterey, California.

Poulin, S. D. (2003) U.S. Enacts Measure for Maritime Security. The Coast Guard Journal of Safety at Sea Proceedings of the Marine Safety Council, Vol. 60, No. 2, pp 19 – 23, April -June 2003.

Rohan, G. (2001) The Asymmetric Threat From Maritime Terrorism. In Jane's Navy International, pp 24-29, October 2001.

Rohan, G. and Chalk, P. (2002) Terrorist Tactics and Targets. In Counter Terrorism, chapter 3, 2nd edition, Jane's Information Group, October 2002.

BIOGRAPHY

Oliver Tan is Project Manager (Integrated Knowledge-based Command and Control). His current area of research involves decision-support systems, multi-agent modelling and simulation, and service-oriented enterprise architectures. He graduated with a Bachelor of Engineering (Honours) in Electrical Engineering from the Nanyang Technological University, and attained a Master of Technology in Knowledge Engineering from the National University of Singapore in 2002. He was also awarded the Singapore Press Holdings Medal for graduating as the top student in his Masters cohort. In addition, he received the DSTA Postgraduate Scholarship and has since attained a Master of Science in Modelling, Virtual Environment and Simulation from the Naval Postgraduate School (NPS) in 2005. He was awarded the Surface Navy Association's Award for Excellence in Surface Warfare Research and the George L. Philips Modelling, Virtual Environment and Simulation Award during his time at NPS.