Towards an Understanding of Security, Privacy and Safety in Maritime Self-Reporting Systems

Mark McIntyre, Lynne Genik, Peter Mason, and Tim Hammond
Defence R&D Canada
http://www.drdc-rddc.gc.ca/

Abstract. Global satellite navigation systems such as GPS enable precise tracking of vessels worldwide and pervasive global networks such as the Internet allow sharing of this information almost instantaneously between locations anywhere on Earth. This ability to monitor vessels globally is a topic of current debate among those concerned with national security, those who are mainly interested in safety at sea and those who advocate for privacy rights at the personal, commercial and national level. In this paper we discuss two maritime self-reporting systems, namely the Automatic Identification System and Long Range Identification and Tracking, which have given rise to this debate. The benefits and drawbacks of each are discussed with safety, security and privacy in mind. Also, some connections are drawn between these systems and Mobile Ad Hoc Networks and Radio Frequency Identification where security and privacy are also of current interest.

1 Introduction

Global satellite navigation systems such as the Global Positioning System (GPS) have revolutionized our ability to precisely locate entities in both time and space in a common global reference system. Modern communication and networking systems, such as cell-phone networks, the INMARSAT satellite system and the Internet, provide the capability to access this precise track information, together with other ancillary information about the entity, virtually anywhere on earth. Taken together, these systems offer tremendous potential for improving the efficiency and safety of any enterprise that relies on movement of goods and/or people. This is especially true for sea and air transportation – those transportation modes for which navigation systems like GPS were originally designed. But, the benefits of geospatial reporting systems are being realized much more broadly to include many land applications and there are examples proposed where these technologies can be used to continuously monitor individuals thorough the course of their daily lives [1]. Such examples suggest the impact that geospatial reporting systems could have in national security applications but equally they raise concerns about the potentially invasive nature of such systems on personal privacy.

Because terrorists have exploited commercial transportation systems in the past, there is concern that they will do it again. Since September 11, 2001 significant advances have been made towards securing the air transportation system and land border security issues have been a high priority. However, particular attention is now being paid to the maritime environment since the seas have been relatively unregulated in the past and a tremendous amount of trade flows into, and out of, North America in a globalized economy. Unregulated flow of goods and people in the maritime domain raises fears of terrorist threats but it also provides a vector for illegal smuggling of goods and people, for proliferation of traditional weapons and weapons of mass destruction and for environmental exploitation and crime. Because of these worries, measures are being taken both nationally and internationally to improve general awareness of activity on the world's oceans and waterways.

There are three objectives of this paper. The first is to provide a general discussion of two self-reporting systems (SRS) that have been recently introduced in the maritime domain - namely the Automatic Identification System (AIS) and Long Range Identification and Tracking (LRIT). Through a discussion of self-reporting systems in general and the safety, security and privacy issues that are currently under debate regarding AIS and LRIT we hope to stimulate interest in the academic community to address some of these concerns. Secondly, we attempt to draw parallels between these maritime self-reporting systems and two fields of current interest in information and network security – namely Mobile Ad Hoc Networks (MANETs) and Radio Frequency Identification (RFID) systems. Security and privacy investigations for MANETs and RFID systems may be directly applicable to AIS and LRIT. Finally, we try to identify some key questions that need to be addressed in order to understand the tradeoffs between privacy, security and safety properties in self-reporting systems such as AIS and LRIT.

In Section 2 the general concept of a geospatial self-reporting system is introduced and several properties that characterize them are discussed. In Section 3, AIS and LRIT are presented in sufficient detail to allow a discussion of the drawbacks and benefits of each with respect to security, privacy and safety in Section 4. Next we discuss MANETs and RFID systems in Section 5 and discuss some parallels between these classes of systems and both AIS and LRIT.

2 Self-Reporting Systems

Self-reporting systems enable sharing of position, velocity, time and identity information among parties that either need or want such information. Specifically, we define self-reports as messages, in some pre-defined format, that include at least position, velocity and identity information about some entity. Other ancillary information, such as status or intention information may be included in self-reports. A self-reporting system is characterized by the form of its self-reports in conjunction with a well-defined communication system used for passing these messages between participating parties. Typically, defining a communication system involves defining a communication path together with a protocol for passing the self-report messages. A simple example is one where operators on a ship at sea are expected to fill out a paper form with self-report information and fax the information to some central site that requires the information at regular intervals. This is current practice for all ships that wish to visit ports in North America – a notification report must be filed with national authorities at least 96 hours before arrival in a port. We will use this highly-manual example to motivate the following section where we discuss the characteristics of more automated SRSs. Another example of a self-reporting system is one in use by the crab fishing industry as illustrated in Figure 1. The figure shows the history of self-reports from fishing boats that are collected by the crab fishing authority.

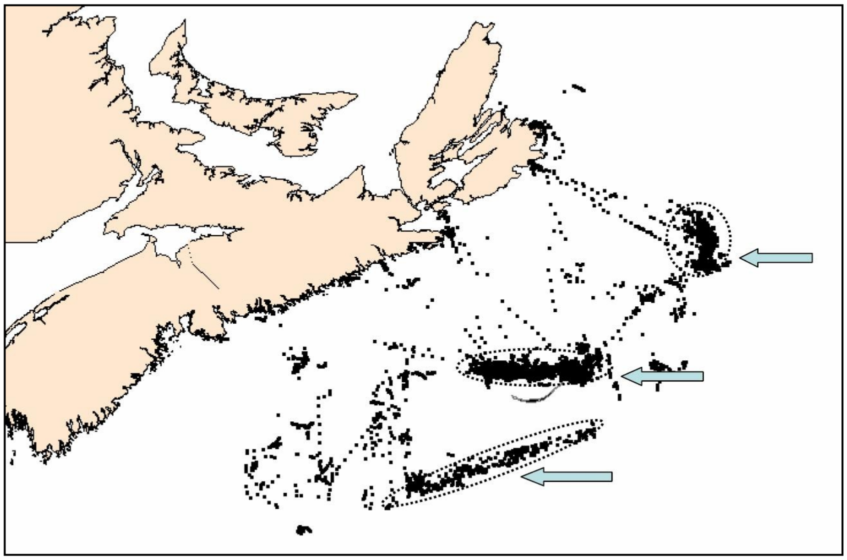

Figure 1. Vessel Monitoring System (VMS) data from 35 vessels of the snow crab fishery off the coast of Nova Scotia [2]. The black dots indicate position reports and the arrows show concentrated areas.

2.1 Characteristics of Self-Reporting Systems

There are a number of properties that characterize automated or semi-automated self-reporting systems and here we attempt to characterize them from the point of view of the entity providing the self-reports. The goal in this section is to provide a general characterization that will be made more concrete in the following section where two specific maritime SRSs are discussed.

The first characteristic of an SRS is the information *content* provided in the self-reports. As mentioned earlier, the key information considered here is position, velocity and time information, together with identity information, related to each of the participating entities. Furthermore, there may be some form of intention information contained in a self-report such as the intended track for that entity. This information is distinguished by the fact that it is information about the future. Ancillary static information about each entity will also be considered but only as amplifying information.

A second important characteristic of an SRS is the class of entities that provide self-reports. In practical terms this determines which entities must participate in an SRS. For example, certain classes of maritime vessels are required by international marine law to carry certain self-reporting systems while others may participate by choice alone. We will refer to this as *carriage* requirements. Note that entities that are not required to carry an SRS system may still benefit from the information available from the system if they have access to it

Two other characteristics of a SRS are *coverage* and *resolution* and these can be broken down into spatial and temporal components. The *spatial coverage* is roughly the geographic area over which a SRS is expected to operate. From the reporting entities viewpoint, this is the geographic region over which self-reports are required to be available. *Spatial resolution* is the accuracy with which entities are expected to report their geospatial information while *temporal resolution* is the accuracy of the temporal component of the self-reports. Finally, *temporal coverage* is the period of time over which an SRS is meant to operate.

Finally, we characterize an SRS by its *enrolment policies and protocols* and the *information sharing policies and protocols* used to exchange information between two entities within the SRS. The joining policy determines what new entities are permitted to join an SRS and the enrolment protocol specifies the procedure that new entities must follow to join an SRS. Information sharing policies determine what information can be shared among entities within an SRS and the information sharing protocols determine how this sharing takes place. These in turn help to determine the information sharing architecture that is needed to support an SRS.

3. Examples of Maritime Geospatial Self-Reporting Systems

Two self-reporting systems that are of topical interest to the maritime community are discussed in this section and described using the characteristics discussed in the previous section. The Long Range Identification and Tracking system is planned for initial operation in January 2008 while the Automatic Identification System has been in limited operation since 2004 with full scale operation due in 2007.

3.1 Long Range Identification and Tracking (LRIT)

Long Range Identification and Tracking (LRIT) is a self-reporting system mandated for worldwide adoption that is designed to allow maritime nations to achieve three objectives. The first is to allow a maritime nation (referred to as flag states) to maintain global, continuous awareness of the location and movements of ships that are flagged under that country. Secondly, it will allow countries (port states) to maintain a detailed awareness of the ships that are destined for their national ports. And lastly, it will allow maritime nations (coastal states) to achieve much better awareness than they currently have of vessels that transit past their coastlines, largely for reasons of national security [3]. The main technology enabler for this system is the growing availability of global communication networks, particularly satellite systems, that allow a flag state to communicate with vessels worldwide. It is noteworthy that the adoption of technologies to improve awareness of vessels at sea has been slow compared to that of airspace awareness for the aerospace community.

The content of LRIT messages is specified by the International Maritime Organization (IMO) which requires vessels to provide time-stamped position and identity reports when requested by an authorized agency. Passenger ships and cargo ships larger than 300 gross tonnes on international voyages as well as mobile off-shore drilling units will be required to carry LRIT information systems [4]. These carriage requirements are also decided by the IMO. The spatial coverage is meant to be global to insure that flag states and vessel owners can access LRIT reports from wherever a vessel may be. As well the system is meant to operate continuously to provide full temporal coverage. However, there are provisions to allow delays of up to four hours for LRIT message reporting, depending on the distance a vessel is from a state requiring the reports [3].

The LRIT information collection policies, together with the policies for sharing LRIT reports nationally and internationally, have been quite contentious issues over the past few years. The main contention has been the coastal state requirements. The desire by some coastal states to access LRIT reports for ships transiting up to 2000 nautical miles off their coasts [3] appears to contravene a long-standing “right of innocent passage” for marine vessels. This boundary is well outside the traditional 12 nautical mile national maritime boundaries and is also well beyond the 200 nm exclusive economic zone of maritime nations, suggested by the Russian Federation [5]. The range of 1000 nm was finally adopted in 2006 [4].

The LRIT system architecture is shown in Figure 2. LRIT information is transferred from the ship to the Application Service Provider (ASP) by a Communication Service Provider (CSP). The ASP adds additional information and sends the data to the LRIT Data Centre (DC), where it is stored. The International LRIT Data Exchange is effectively a router that routes messages between DCs without processing or storing the position data within the messages. The LRIT Data Distribution Plan defines how LRIT information will be distributed to other governments.

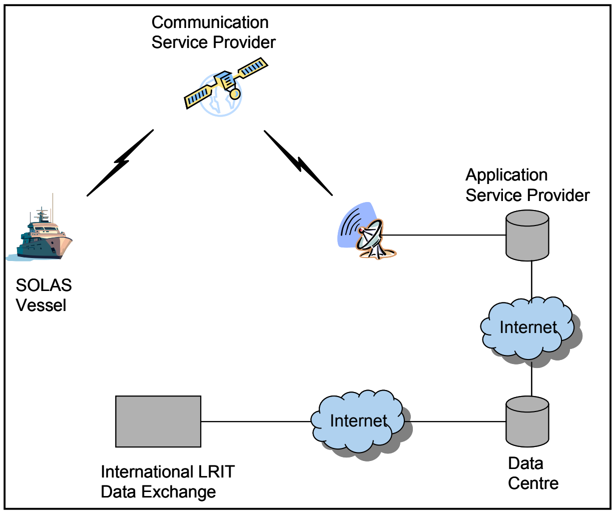
Communication Service Provider
Application Service Provider
SOLAS Vessel
Internet
Internet
International LRIT Data Exchange
Data Centre

Figure 2. Typical LRIT System Architecture

The LRIT Coordinator helps to establish the international components of the system and performs administrative functions, reviews and audits. In late 2006 the Maritime Safety Committee (MSC) appointed the International Mobile Satellite Organization (IMSO) as the LRIT Coordinator, who had offered to take on the role “at no cost” to the participants although the details of the cost structure remain to be confirmed [6]. The overwhelming majority of nations supported this.

It should be noted that LRIT is an example of general vessel tracking / vessel management systems that have been in use for many years for various reasons. Companies that own fleets of vessels have been employing modern vessel tracking technologies based on self reporting for fleet awareness and efficiency reasons for some time. They have tended to keep this information to themselves as commercially sensitive information although they are often willing to share the information for safety at sea reasons as is the case in the Automated

Mutual-Assistance Vessel Rescue (AMVER) system. In ecologically and environmentally sensitive marine regions governments or other responsible agencies may require self-reporting while within a protected area. These areas will generally be quite small in size to protect, for example, breeding grounds of marine mammals, but they could be much larger as is the case of a self-reporting system known as Reef Rep put in place to insure awareness of vessel activity on the Great Barrier Reef [7].

3.2 Automatic Identification System

The Automatic Identification System (AIS) is a self-reporting system that was originally developed in Sweden as an inter-vessel maritime information exchange system to support safety of navigation. Specifically, it was designed as a self-reporting system where participating vessels continuously broadcast self-reports and exchange collision avoidance information once they are in radio reception range of each other. The system has been in development since 1992 and has been strongly promoted by both the US and Canadian Coast Guards. Carriage of AIS equipment has been mandated by the IMO for all vessels of 300 gross tonnes and above and has been in the process of being phased in since 2004 with all SOLAS ships expected to carry AIS equipment by 2007. Smaller vessels are not required to carry the system although a significant number choose to. There is also growing interest in so-called Class-B AIS for use on small boats. Interestingly, fishing vessels of all kinds are not required to employ AIS.

There are in fact many types of AIS reports [8], depending on the reporting scenario and the type of transmitter, but we will focus on basic AIS vessel position reports which are most directly comparable to LRIT position reports. The content of an AIS self-report is similar to that of an LRIT self-report but has additional information. It contains static information such as vessel identification in the form of its Maritime Mobile Service Identity (MMSI) number, which is meant to be a unique identification number assigned to a vessel and encoded in the AIS transceiver. These numbers are controlled by the telecommunications regulations agency in the various countries and are overseen by the International Telecommunications Union. The static information also includes the size and type of ship as well as the positioning information for the AIS antenna on the ship. This information is required for high-accuracy collision avoidance calculations. Vessel self-reports contain dynamic data such as GPS position and velocity information as well as rate of turn. They also include rough time information although it is not meant to be an accurate time stamp on the information. Finally, AIS reports may also include voyage-related data such as next port and information regarding hazardous goods onboard.

With respect to spatial coverage of the AIS system, it is mandated as a global system and two frequencies in the VHF band have been reserved. Although there were some difficulties with reserving this spectrum worldwide, the importance of the system for both safety at sea and awareness of maritime activity facilitated international agreement and the system has been operating since 2004. The spatial resolution of the system is that of the underlying GPS position data. Without spatial information of this quality, the system could not be relied on as a collision avoidance system.

The temporal coverage of the AIS system has to be continuous while a vessel is at sea in order to insure that it provides the safety benefits (although one could argue that the safety mandate could be met by a system that could be turned on in designated areas that are deemed to be high-traffic). Furthermore the temporal resolution has to be high in order to guarantee collision avoidance when vessels are in close proximity. Typically the frequency of vessel reports vary between once every 2 seconds to once every 10 seconds and the information is transmitted immediately without any delay.

As discussed earlier, carriage of AIS is mandated for most large vessels that travel internationally but other vessels can install the equipment on a voluntary basis. The equipment is relatively inexpensive and the enrolment procedure simply involves applying for an MMSI number from the national authorities. Sharing of AIS vessel reports once the system is operating on a ship is completely open as it needs to be for safety purposes. The broadcast nature of the AIS system insures that any vessel in RF reception range of the transmitter will be able to make use of the AIS information. There are AIS messages that can be directed to specific vessels via MMSI addressing.

4. Benefits and Drawbacks of AIS and LRIT

Major distinctions between AIS and LRIT are the short range of AIS versus the long range of LRIT, the peer-to-peer nature of AIS as opposed to the centralized architecture of LRIT, and the end-to-end security features of LRIT for point-to-point communications versus the unsecured broadcasts of AIS. As outlined in the previous section, AIS was intended to support safety at sea and is now being considered for maritime domain awareness (MDA), while LRIT is being developed to provide MDA for national security and can provide location information for search and rescue missions. These different purposes and capabilities lead to a series of benefits and drawbacks for each.

4. 1 AIS

A primary benefit of AIS is safety, providing ships with a means for exchanging identity, location and other important information to prevent at-sea collisions and facilitate traffic management in ports, and aiding in search and rescue missions [9]. The system offers a substantial improvement over radar tracks in providing situational awareness and institutes automatic reporting between devices without human intervention/operation, which reduces the need for radio voice communications, especially in high traffic areas. It should be noted, however, that there is still a fair bit of manual input required on set-up, which is a potential cause of errors.

The wealth of information provided in AIS transmissions significantly enhances maritime domain awareness. The Maritime Domain Awareness Data Sharing Community of Interest (COI) was formed in February 2006 with members from the US Department of Defense and Department of Homeland Security (including the US Coast Guard) [10]. Under this COI, a pilot working group was formed to share AIS data between members. The goal is to evolve the pilot into an operational capability, leading to a national coastal AIS capability. Canada also has an AIS pilot project that, similarly to the US, is based primarily on AIS collection networks that have been set up for research and evaluation purposes. Discussions are underway to share local and regional AIS information to provide more complete coastal AIS coverage across North America.

AIS devices range from US $1500 to $5000 [11], with installation costs ranging from CA $5000 to $10000. The cost is considered to be relatively inexpensive. Governments can also benefit economically since traffic monitoring helps in enforcing pollution regulations and managing fisheries [9].

Safety-related text messages and short binary text messages can be sent via AIS, and can either be broadcast or sent to a specific station[1]. Through the binary text messages there is potential to carry other, non-AIS data, which means that information could be piggy-backed on the AIS system and may reduce other communications costs. AIS can also play a role in assisting search and rescue missions.

At present there appear to be no nationally and internationally accepted guidelines with respect to the collection and handling of AIS data. This has privacy implications associated with it. AIS information is broadcast in the clear and is accessible by any receiver within range. This means that anyone with the proper equipment can collect information on an individual ship and its history. For example, the UK company AIS Live Ltd.[2] collects AIS information worldwide and sells access to it online. This information could be used in clandestine activities such as developing a competitive advantage between shipping companies, determining prime fishing areas, pirate attacks, etc. Given that vessels broadcast AIS information in the clear, should they have an expectation of privacy? On the other hand, given that the intent of the information is for safety purposes, one could expect that it only be used as intended, and not for MDA. These issues have yet to be resolved.

From a technical standpoint, AIS is vulnerable to both unintentional and intentional misreporting. Devices are not required to authenticate to each other and there is nothing to ensure the integrity of a ship's data. This allows for malicious activity, such as false identity and/or location information reporting. Steps taken to make the system more robust against accidental misreporting can often make intentional misreporting more difficult; however, devices can be powered off at any time, resulting in no reports.

[1] http://emmel.alfahosting.org/english/message_en.htm

[2] http://www.aislive.com/AISLivePortal/DesktopDefault.aspx

AIS is dependent on GPS for time-slot governance and position fixing[3] [12] and GPS is susceptible to interference. Therefore, adequate backup systems (for example, Loran, a network of coastal transmitters put in place for marine navigation) and procedures must be in place. The AIS frequencies are also susceptible to intentional and unintentional interference. If there is significant interference on the AIS frequencies the system becomes virtually useless.

AIS is considered to be a short-range system (typically on the order of 20-30 nm) [2]. Methods of significantly extending its range, such as by using satellite and high altitude balloons, are currently being investigated, but this is usually for passive reception of the signals only. At this point it is not clear who would be responsible for supporting any infrastructure costs for receptions past the close coastal areas.

Fishing boats are not obligated to use AIS. This is a case where vessel owners may trade safety for privacy. Typically fishermen are not concerned with national security but are very concerned with preserving privacy (for example, of their fishing areas). They may opt to forego the safety features of AIS rather than make their location and other details known.

4.2 LRIT

LRIT was designed to enhance national security and is being spearheaded by the US with support from other coast guards. As previously noted, LRIT will provide awareness of the location and movements of ships intending to enter a nation's ports, ships traversing a nation's coastal waters within 1000 nm, and global awareness of ships flying a country's flag (hence the "long" range). Data will be stored for up to two years for auditing purposes. By providing maritime domain awareness, LRIT can aid in thwarting potential maritime attacks. Although the full economic impact of a successful attack would be difficult to project, Cairns states that an attack on US west coast ports is estimated to be $140 million to $2 billion over eleven days [3].

[3] If GPS, as opposed to Differential GPS, is being used a ship's position may be off by up to 100 m, http://www.esri.com/news/arcuser/0103/differential1of2.html

The IMO claims that only recipients who are entitled to receive LRIT information will have access and that safeguards regarding confidentiality have been built into the regulatory provisions[4]. The MSC's performance standards for LRIT address the security of LRIT data in transit and in storage [13]. ASPs must ensure the reliable and secure collection, storage and routing of LRIT information, CSPs are responsible for the secure point-to-point transfer of LRIT information, and DCs need a secure transmission method with the International LRIT Data Exchange and a secure authentication method with data users. The International LRIT Data Exchange is required to use a secure access method with the DCs and cannot archive LRIT information. Landline communications must provide security using methods such as authorization, authentication, confidentiality and integrity [13].

The technical specifications for LRIT contained in [14] are more precise when it comes to system security. LRIT components must authenticate each other using digital certificates and information can only be shared with authorized components. Digital cryptography with a minimum 128 bit key length must be employed during data transit. However, no anti-spoofing mechanisms have been designed into the system.

Governments are expected to protect the LRIT information they receive from unauthorized access or disclosure [4]. Nations are able to prevent governments from receiving LRIT information when traversing their coastal waters for security or other reasons [4]. This is specified in their Data Distribution Plan, which is shared with the IMO and subsequently all contracting governments. This caveat only holds for coastal water traversal. For safety purposes, LRIT DCs must provide LRIT information for all transmitting ships in any geographic region specified by a search and rescue (SAR) service [13]. The LRIT information is to be used only for SAR and not for any other reason, which may require special handling.

Unlike AIS, data storage policy for LRIT is fairly well defined. LRIT information can only be stored by the data centre receiving the ship's information, which for many countries will be the national data centre. There has been mention of the establishment of a European (that is,

[4] http://www.imo.org/Safety/mainframe.asp?topic_id=905

regional) Data Centre [6], which could store LRIT information for small European countries, such as Cyprus. Brazil may also be utilized as a regional data centre. In the event that a country cannot afford to establish and maintain a national data centre and is not supported by a regional data centre, the data would go to the International Data Centre (IDC).

The US has offered to build and operate an IDC and International LRIT Data Exchange. This has met with opposition, likely due in part to the US Patriot Act[5] but also for political and other reasons. Several countries expressed the view that the IDC and exchange should be neutral and truly international. A Request for Proposal has gone out for the International LRIT Data Exchange and IDC and it is expected that the IMSO, as LRIT Coordinator, will make a decision on the location in the fall of this year.

Cost and billing issues are complicated and have not yet been resolved. The LRIT Ad Hoc Engineering Group identified billing as a major policy issue needing to be addressed by the MSC [15], and the absence of billing discussions was raised as a concern by International Radio-Maritime Committee (CIRM) members working on LRIT. In their view communications costs and billing need to be studied in order for LRIT to be implemented [6]. It was suggested that the issue of communications billing be added to the Ad Hoc Engineering Group's Terms of Reference. One of the biggest issues is the cost and support of the International Data Centre.

5. Mapping to Other Wireless Broadcast Systems

As discussed previously, both LRIT and AIS are self-reporting systems that enable the sharing of information with specific purposes in mind. The security and privacy issues of these systems should be addressed while keeping in mind some lessons learned in other wireless broadcast systems. AIS was designed with safety as the primary benefit while LRIT is intended for enhancing the coastal security of nation states. This difference in purpose naturally leads to the divergences in the structure/protocol of each system as described

[5] In particular, Section 215: Access to Records and Other Items Under the Foreign Intelligence Surveillance Act

above. It can be argued that through aggregation and persistence of data, leakage of information and subsequent analysis that the lines between the two systems blur to the point that either could, potentially, be used to accomplish many of the goals set out for each. The entities enrolled in the self-reporting system must be aware that the information they are providing may be used for purposes other than that stated as the primary goal.

To assist with the understanding of the tradeoffs among security, privacy and safety, we can map these two systems onto more developed areas of wireless research that have grappled with these same issues. LRIT can be seen to be analogous to a Radio Frequency Identification (RFID) tag system. With RFID systems, an RFID tag is embedded into an object and filled with information tied to that object. The tag can be active, periodically broadcasting its information, or passive, responding only to a poll from an RFID reader. With LRIT, ships report their position periodically and can respond to polls from their flag states or states whose coasts are within the specified range, so they can be seen to be mimicking both passive and active RFID systems. Like RFIDs, which only communicate with a reader (not with other tags), LRIT does not facilitate inter-ship communication. In contrast, AIS is an active, periodic, broadcast system specifically designed to enable ship-to-ship reporting with no mandate to report information back to a centralised data collection centre. AIS message routing also allows for base stations to have a repeat mode that enables a base station to essentially route AIS packets between mobile units (ships) [9]. From this perspective, AIS consists of peer-to-peer connections and can be viewed as a very basic instantiation of a Mobile Ad Hoc Network (MANET). In particular, MANETs with proactive routing protocols send out periodic messages for the purposes of neighbour discovery. The information compiled from, and provided in, these periodic messages is then used for constructing an awareness of the local environment and for building routing tables for the network as a whole. Having access to reports beyond the local range of AIS does not enhance the safety of a vessel, so AIS may not require multihop exchange of information. However, nations can (and do) deploy AIS sensors to collect AIS messages and feed them back to data centres. The result is that the AIS reports are often captured by an external sensor network, a reality that dramatically alters the range of functionality of the system. Subsequent traffic analysis of this report data is one concern – a well-known problem in MANETs [16].

Privacy and confidentiality concerns of RFID systems are also well documented [17, 18, 19 (and references therein)]. The use of RFID tags by the US military to control and maintain their inventory and supply chain provides a prime example of the caveats of such systems. An adversary can themselves scan tagged items or eavesdrop while an item is legitimately scanned. Information illicitly collected at the point of scanning may itself be of local value, for example knowing that a specific container carries munitions while another simply food supplies, but aggregated information on flows of goods may be even more concerning, revealing information about troop movements and mobilisations. To protect against the former, information can be secured through encryption so that it is recognisable only by an authorised reader. The second problem, which is essentially one of traffic analysis, is much more difficult to deal with. Even if the information is encrypted the fact that it is broadcast means that it constitutes an event. These events can be aggregated, correlated and analysed for patterns and meaning. Therefore, a self-reporting system like RFIDs naturally sacrifices privacy for some end goal. Researchers are actively working on solutions (see [17] for a recent example) but they are generally application-dependent.

LRIT is designed with security as the primary goal and the self-reports can have three different destinations – the flag state, the port state, or the coastal nations within range. However, a ship that is dutifully broadcasting reports that go to a coastal nation when within its limits cannot expect that it can no longer be tracked when it moves outside these limits and is reporting back to its flag state only. Even though the flag state information is encrypted, given the information a coastal nation has already received it could continue to monitor the traffic intended for the flag state and, with some effort, tie the information back to the appropriate vessel. This would essentially give a coastal nation the ability to track worldwide every ship that passes through its reporting zone until that ship reaches its port of call. While subscribers and proponents of LRIT may be comfortable with self-reporting for legitimate security purposes, it is unlikely they would agree to having their movements continuously tracked by every coastal nation they pass by.

The primary intent of AIS as a system designed for safety purposes accentuates some of the concerns mentioned above. There are two safety components – avoiding ship-to-ship collisions and tracking of the last known location of a vessel should it become lost or disabled. The first issue is solved by the local peer-to-peer exchange of the shorter-range (compared to LRIT) messages which allow ships to have situational awareness within the range of their messages. The second requires the deployment of the AIS sensor network by a coastal state to collect the (unsolicited) periodic broadcasts. In effect, this system is like a simple single-hop MANET with each node simultaneously reporting back to the AIS sensor network, connected to a central server. If it is accepted that AIS exists solely for safety reasons it could be argued, then, that the only information collected by the sensor network that serves this purposes is the last known location of the vessel. If privacy is truly a concern, the nodes in the sensor network could simply buffer self-reports, storing only a single report per vessel. When a new report is received from an existing contact, the previous report could be overwritten. Only when a new report is not received within a certain timeframe (given by the protocol) should a safety alert be raised and the information transmitted back to the centralised authority. If, instead, all AIS reports are intercepted, stored, and shared among nations, it could be argued that many of the aims of the LRIT system could be achieved by AIS. That is, sacrificing the privacy of a local broadcast system greatly enhances its ability to function as a security system. Using AIS explicitly for such purposes would almost certainly require participant permission. A further complication is that broadcast AIS information can be captured by third parties who can publish it. There are already companies that could facilitate such a scenario (ICAN[6], Shine Micro[7]).

A party interested in preserving its privacy within AIS may purposely alter its reports to provide misinformation. The problem of authentication and establishment of trust in peer-to-peer systems such as MANETs is complex [20]. Without access to a centralised authentication server or the distribution of pre-shared keys or certificates bound to each vessel, the possibility of inaccurate (deliberate or accidental) information compromising the safety of a vessel remains a possibility. If trust can be established between participants, they may choose to share more information in their self-

[6] http://www.icanmarine.com/maritimeadmins.htm

[7] http://www.shinemicro.com/Govt.asp

reports if they feel it can enhance the effectiveness to their benefit. Effective ways in which this can be done is an open area for research.

6. Discussion and Conclusions

There remain a number of important questions to be addressed in both LRIT and AIS with respect to the tradeoffs among security, privacy and safety. These questions are more than academic as the functionality of the systems and the user "buy-in" depend strongly on the details of the implementations. It may prove to be a useful exercise to consider the lessons from other self-reporting wireless systems, such as RFIDs and MANETs, when examining the interplay among these three features, as security, privacy and safety concerns have been the objects of investigation by many researchers in these areas. In both of these analogous systems, many problems remain unresolved.

For AIS, of paramount importance is the authenticity of the self-reports. Without assurance of authenticity, neither safety nor security is achievable. Mutual authentication enhances security but does not appear to be well-considered in the current implementation of AIS. A host of other problems such as eavesdropping, message alteration, spoofing, traffic analysis and attacks (such as replays) should also be given consideration. Some of these problems may also apply to LRIT. A great deal of policy work needs to be done regarding the collection, storage and exchange of data in order to address the legitimate privacy concerns of participants. AIS information is being used for maritime domain awareness and takes the system beyond its original intent at the price of privacy. Researchers in other areas, such as radar systems, may find AIS data to be of great benefit to their work, but measures may need to be taken to anonymize (at least partially) historical data in order to obscure information that infringes upon privacy. This is a common practice for network data being analysed by security researchers.

With LRIT, privacy is willingly sacrificed for security purposes but only under certain circumstances (for example, within 1000 nm of a coastal state). This does not mean, however, that privacy is always preserved. The nature of a wireless broadcast system makes it vulnerable to traffic analysis and once LRIT information is divulged, privacy may be compromised indefinitely. The issue of the location of the International Data Centre and International LRIT Data Exchange are still in question, in large part because of concerns of who has access to the information.

One goal of this paper has been to introduce both the AIS and LRIT systems to the information security and privacy community in the hope that some of the security and privacy concerns for these systems can be addressed. A second goal has been to begin to draw links between these two maritime self-reporting systems and both RFID systems and MANETs. This goal has been partially accomplished but further work is needed to better understand the linkages and draw conclusions about the applicability of security and privacy results for RFIDs and MANETs to both AIS and LRIT.

7. References

[1] K.R. Foster and J. Jaeger, RFID Inside: The Murky Ethics of Implanted Chips, *IEEE Spectrum*, March 2007, pp. 41-48

[2] Fisheries and Oceans Canada, Vessel Monitoring System (VMS), (2005), retrieved June 2006 from http://www.glf.dfo-mpo.gc.ca/fm-gp/cp-cp/vms-ssn/vms_presentation-e.pdf

[3] W.R. Cairns, AIS and Long Range Identification and Tracking, *The Journal of Navigation* (2005), 58, pp. 181–189.

[4] Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as Amended, Annex 2 Resolution MSC.202(81), adopted May 19, 2006, retrieved April 2007 from http://www.imo.org/includes/blastDataOnly.asp/data_id%3D15576/202%2881%29.pdf

[5] Development of the Draft SOLAS Amendments on Long Range Identification and Tracking, Submitted by the Russian Federation, IMO Intersessional MSC Working Group on Long Range Identification and Tracking, MSC/ISWG/LRIT 1/3/4, September 20, 2005, retrieved April 2007 from http://www.state.gov/documents/organization/58690.pdf

[6] Draft Report of the Maritime Safety Committee on its Eighty-Second Session (continued), IMO MSC 82/Wp.8/Add.1, December 8, 2006

[7] K. Abercrombie, N. Trainor and J. Huggett, Enhancing Navigation Safety and Protection of the Marine Environment of the Great Barrier Reef and Torres Strait Region, Australian Maritime Safety Authority, retrieved April 2007 from http://www.amsa.gov.au/About_AMSA/Corporate_information/AMSA_speeches/Austmarine_East_conf.pdf

[8] W.R. Cairns, On Watch: Vessel Tracking Technologies for Maritime Security, *US Coast Guard Proceedings*, Spring 2006, pp 32-35.

[9] T. Hammond, R. Kessel, The Implications of the Universal Shipborne Automatic Identification System (AIS) for Maritime Intelligence, Surveillance, and Reconnaissance, Defence R&D Canada – Atlantic Technical Memorandum, DRDC Atlantic TM 2003-143, August 2003.

[10] Macaluso, Capt J.J., “Maritime Domain Awareness Data Sharing Community of Interest: A new partnership explores net-centricity”, The Coast Guard Journal of Safety & Security at Sea Proceedings of the Maritime Safety & Security Council, Vol. 63, Number 3, Fall 2006, pp 62-64.

[11] AIS Frequently Asked Questions, US Coast Guard Navigation Center, available April 2007 from http://www.navcen.uscg.gov/enav/ais/AISFAQ.HTM#0.4_7

[12] Review of AIS, International Sailing Federation, available April 2007 from http://www.sailing.org/default.asp?ID=j/qFni6v&MenuID=t67mGMnon~824QM6/%60xAM4Y1TU0d6YZUhv~JMBMq/RNTdbdlYpYP3PWct8Ulz4

[13] Performance Standards and Functional Requirements for the Long Range Identification and Tracking of Ships, Annex 13 Resolution MSC.210(81), adopted May 19, 2006, retrieved April 2007 from http://www.emsa.eu.int/Docs/LRIT/msc210_81_lrit_ps.pdf

[14] Interim LRIT Technical Specifications and Other Matters, IMO Ref. T2-OSS/1.4, MSC.1/Circ.1219, December 15, 2006, retrieved April 2007 from http://www.imo.org/includes/blastDataOnly.asp/data_id%3D16797/1219.pdf

[15] Informal Record of Discussions, LRIT Ad Hoc Engineering Group, June 2006, available April 2007 from http://www.emsa.eu.int/Docs/LRIT/lrit_ad_hoc_engineer_vancouver.pdf

[16] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in mobile ad hoc networks: challenges and solutions, *IEEE Wireless Communications*, Vol 11, Issue 1, Feb 2004, pp 38- 47.

[17] J. Cichon, M. Klonowski, and M. Kutylowski. Privacy Protection in Dynamic Systems Based on RFID Tags*, PerSec 07*, March 2007.

[18] S.A. Weis, S.E, Sarma, R.L. Rivest, D.W. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *Security in Pervasive Computing (SPC) 2003*, LNCS 2802, 201-212.

[19] A. Juels, RFID security and privacy: a research survey*, IEEE Journal on Selected Areas in Communications*, Vol. 24, Issue 2, Feb 2006, pp 381-294.

[20] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva, J-J. Quisquater, Authentication protocols for ad hoc networks: Taxonomy and research issues, *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, October 2005.