Securing Marine Data Networks in an IoT Environment

Mohammed Al-Khalidi*, Rabab Al-Zaidi+, John Woods+, Martin Reed+, and Ella Pereira*

*Department of Computer Science, Edge Hill University, Ormskirk, UK
+School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK

***Abstract*—With the huge proliferation of sensory applications, the Internet of Things (IoT) is promising connectivity capacity far beyond the conventional computing platforms, with an ultimate goal of connecting all everyday objects. Sensory applications in the marine environment are foreseen to be an integral part of this connected world, forming the Internet of Marine Things (IoMaT). While some efforts that aim to establish network connectivity in such a sparse environment exist, securing these networks is still an unreached goal. This paper introduces a secure Mobile Ad-hoc/Delay Tolerant routing protocol (S-MADNET) for the marine environment over VHF equipment available on the majority of ships. The proposed secure network is designed to use the existing Automatic Identification System (AIS) that ships use for positioning and navigation aid. An IoMaT routing module that forwards marine sensory data using the proposed secure protocol is also presented, taking the AIS system level considerations into account. Furthermore, a new AIS message format with IoMaT support is proposed that accommodates the requirements of the secure routing protocol. Evaluation results show that the proposed S-MADNET routing protocol outperforms its counterparts in terms of packet delivery rates and packet duplication rates, while maintaining data security.**

***Index Terms*—Mobile Ad-hoc Networks, Delay Tolerant Networks, Internet of Things, Marine Cartography, Security, VHF.**

I. Introduction

Marine cartography systems aim to provide a seamless, consistent and standardised database of marine climatic, environmental and navigational data using photogrammetric, sensing or laser scanning based approaches. However, the methods exploited so far are either remote monitoring based methods such as satellites which lack the required accuracy due to contaminants in the atmosphere that may corrupt the measurements [1]; or exploration based methods such as research vessels including hydrographic and oceanographic ships that can not cover the vast areas of oceans and seas due to the physical constrains, and limited number of deployed research vessels. Therefore, the marine cartography systems available usually either lack the required level of accuracy, geographic comprehensiveness or recency of the data samples. This necessitates exploring new alternative methods that can address these drawbacks, especially with the tremendous growth in data communications and the advancements in data analytics. For example, the emerging Internet of Things (IoT) aims to inter-connect physical devices, vehicles, home appliances and any other object with built-in sensors to gather data and take action on that data across a network. In preparation for the revolutionary 5G Networks, the UK Office of communications (Ofcom) has allocated more radio spectrum for the Internet of Things (IoT), specifically VHF spectrum aiming to encourage Machine to Machine (M2M) applications to use spectrum that will enable them to connect wirelessly over longer distances. This VHF spectrum has different properties to other frequencies, already in use for the IoT, and can reach distant locations which other frequencies may not [2]. This provides the motivation of this work to exploit marine band VHF communication for the Internet of Marine Things (IoMaT).

Networks in the marine environment possess unique properties that differentiate their routing needs. When ships are moving, links can be obstructed by intervening objects. In addition, ship movement in sparse areas will likely lead to link disconnections due to communication range limitations. These events result in intermittent connectivity. For this reason, applications in the marine environment must tolerate delays beyond conventional IP forwarding delays. Mobile Ad-hoc Networks (MANETs) Routing protocols do not work properly in sparse areas because when packets arrive and no contemporaneous end-to-end paths for their destinations can be found, these packets are simply dropped [3]. On the other hand, Delay Tolerant Network (DTN) routing protocols do not work properly in dense areas, since they generate a high volume of packet copies and generate an unnecessary burden on the precious VHF link. Therefore, since the marine environment can be characterized as a mix between dense and sparse areas together, an alternative routing approach is needed that can fit the described scenarios. The authors of this paper have shown in previous work [4] [5] that sensory data from ships and vessels at sea can be collected and sent back to onshore sinks collocated with 5G base stations as part of a cartography IoMaT application. A marine Mobile Ad-hoc/Delay Tolerant hybrid routing protocol (MADNET) was proposed to switch automatically between MANET and DTN routing according to the network connectivity. In this paper, we extend the proposed MADNET protocol to include security features such as packet authentication and integrity support. The new ***S-MADNET*** protocol ensures that the packets received at sink nodes are authentic and not sent from malicious sources. It

Corresponding author: Mohammed Al-Khalidi, email: khalidim@edgehill.ac.uk.

This work was supported in part by the Edge Hill Research Investment Fund (RIF).

further ensures the integrity of the data being received and that it has not been altered in any way during transmission. Hence, increasing the network robustness towards a number of known security attacks such as denial of service, spoofing, packet replay, and packet modification. Evaluation results show that the proposed S-MADNET routing protocol outperforms its counterparts in terms of packet delivery rates and packet duplication rates, while maintaining data security.

The rest of this paper is structured as follows. Section II provides a background of the investigated domain and summary of related work, while Section III explains the proposed routing protocol and security solution. Section IV describes the proposed system prototype and IoMaT software components and Section V presents the simulation environment and obtained results. Finally, the conclusions are drawn in Section VI.

II. Background & Related Work

Marine Networks are considered Unstructured Mobile Networks (UMNs) in which there is little or no pre-installed infrastructure (access points, antennas), and as such message forwarding is performed among the mobile nodes or within the wireless infrastructure. UMNs are suitable to a wide range of applications, from environmental monitoring to vehicular networks, mesh networks, among others [6]. Routing in UMNs can be classified into two categories: MANET [7] and DTN [8] routing. In MANETs, end-to-end transmissions can be achieved using different routing protocols, once the network topology has been decided. Therefore, a MANET is highly reliable in areas with high density and low mobility. However, in low density and/or high mobility areas, frequent disruption can cause instability of transmission paths, and therefore decrease the networks reliability. In such an environment, Delay Tolerant Networks (DTNs) perform more effectively. DTN does not depend on route information and provides interoperable communication between a wide range of networks which may have exceptionally poor transmission and be disparate. It has the capability of storing the message whose destination is another node. If a message cannot be delivered immediately due to network partition, the best carriers for a message are those that have the highest delivery probabilities [9].

A large number of research efforts have focused on MANET and DTN routing protocols and optimizing their performance. MANET routing protocols are usually classified into proactive protocols that maintain routing information proactively, such as the *Destination Sequenced Distance Vector Protocol (DSDV)* [10]; or reactive protocols that initiate route establishment on demand, such as the *Ad-hoc On-Demand Distance Vector Protocol (AODV)* [11] and the *Ad-hoc On-Demand Multipath Distance Vector Protocol (AOMDV)* [12]. DTN protocols on the other hand perform hop-by-hop forwarding instead of the end-to-end forwarding used by MANETs. Two of the most popular DTN routing protocols are the *Epidemic* and *Spray and Wait* protocols [13] [14].

Although substantial progress has been made on UMN establishment, addressing UMN security issues is still a major target. Security is difficult to achieve in a network without persistent connectivity, which is an essential requirement for security features such as key exchange. In addition, the lack of a fixed infrastructure and central authority, makes it hard to facilitate trust establishment, i.e., authentication, and membership control. Integrity solutions suffer similar challenges, since strong integrity solutions are also based on cryptographic keys. Inherently, all the MANET and DTN routing protocols discussed previously share these limitations, and therefore, lack the capability to provide effective security. Attempts to improve UMN security exist such as the Security-Aware Ad hoc Routing Protocol (SAR) [15] that addresses the security issue by including security quality metrics in the route discovery process, thereby, allowing data senders to make informed decisions on the quality of protection available to their data packets. The Privacy-Preserving Location-Based On-Demand Routing Protocol (PRISM) [16] build on the AODV protocol by proposing a a group signature scheme which can be verified by anyone who has a copy of a constant-length group public key. While the solutions above maybe considerable in dense node scenarios, they can't be applied in sparse scenarios such as vast seas and oceans, where connectivity is more opportunistic. Security proposals for opportunistic and delay tolerant networks such as the Cryptography-Based Misbehavior Detection and Trust Control Mechanism [17] use infrastructure nodes for monitoring participative nodes in the network. The infrastructure nodes look for suspicious misbehaving nodes that may perform attacks. The Provenance-Based Trust Model for Delay Tolerant Networks (PROVEST) [18] proposes the use of group keys for authentication managed by distributed trusted authorities (TAs). These proposals such as others that rely on the existence of infrastructure nodes are instantly ruled out when considering the spacious seas and oceans.

III. S-MADNET Routing Protocol

As ships can be very dense in certain busy locations across main shipping channels and very sparse in others such as deep ocean and shallows, a new secure hybrid routing protocol is proposed that switches automatically between Ad-hoc On-Demand Distance Vector (AOMDV) routing protocol (the best performing routing protocol in dense locations as found in [19] [20]) and Binary Spray and Wait (SW) DTN (the best performing routing protocol in sparse situations [21] [22]). The routing process at each ship always starts with AOMDV route discovery, where a Route Request message (RREQ) is propagated towards the destination. Any intermediate node (ship) receiving the RREQ packet sets up a reverse path to the source using the previous hop that sent the RREQ as a next hop for the reverse path. If the same route request is received through more than one neighbour, two reverse paths are created accordingly. Also if the intermediate node has a route to the destination, it immediately generates and sends a route reply message (RREP) back through every neighbour that sent a RREQ for the identified destination. Else, the RREQ message is re-broadcast and the same process is repeated until the RREQ reaches a ship with a route to the destination or the

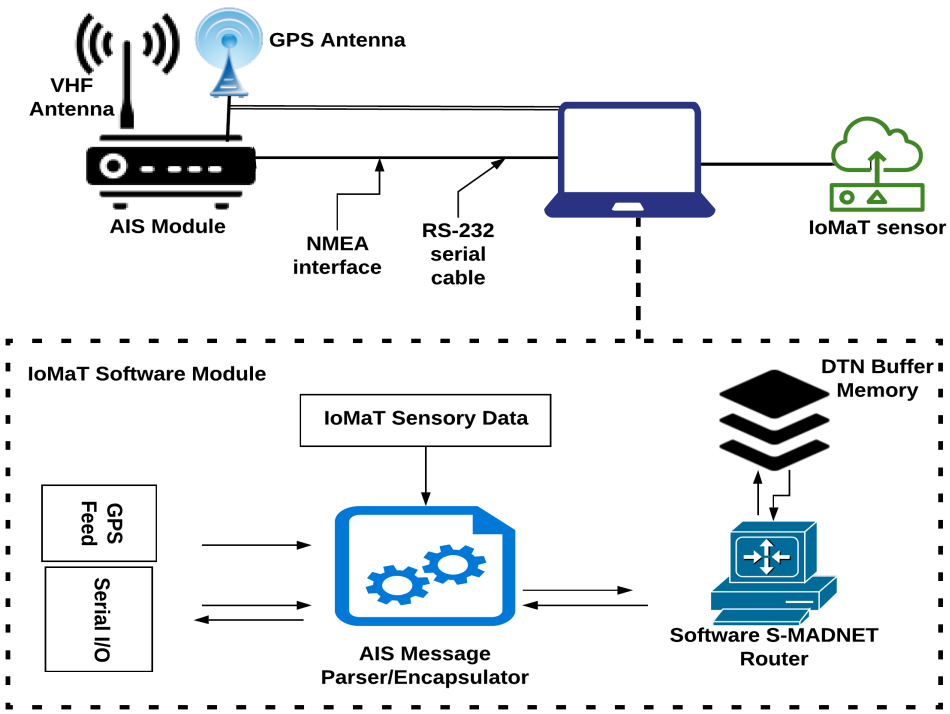

Fig. 1: AIS with IoMaT Software Module

destination itself. Thereafter, a RREP message is forwarded back to the source via the reverse path(s). As the RREP message proceeds towards the source, the forward path(s) are set up towards the destination.

In case no route exists towards the destination and the timeout for receiving a RREP expires, the source node does not regenerate a RREQ packet as would happen in normal AOMDV operation. Instead, the source node initiates Binary (SW) DTN routing that does not rely on end-to-end communication. The DTN bundles are transmitted hop-by-hop and have a certain lifetime, which is known as the time-to-live (TTL). After the TTL expires, the bundle is dropped at intermediate nodes. Re-transmitting bundles can happen either at the originating node or an intermediate one that has obtained the bundles custody by a process named custody transfer. Several DTN protocols exist and differ in the way they propagate DTN bundles throughout the network. In this work, we use Binary (SW) routing that caps the number of bundle copies at a specific value. Basically in Binary (SW), any node x that possesses more than one bundle token, and encounters any other node y that has no tokens, hands over half of its tokens. When node x or y is left with one token only, then the bundle can be forwarded to the destination node only using AOMDV routing and no more copies are sent to any relay nodes.

S-MADNET routing protocol provides an optimum routing solution for the marine environment and achieves the performance trade-off between ship density, sparsity and low available data bandwidth. In sparse areas, the S-MADNET initially jump-starts spreading message copies, in a manner similar to epidemic routing. When enough copies have been spread to guarantee that at least one of them will find the destination through end-to-end AOMDV routing, it stops generating copies. Otherwise, if a direct AOMDV routing path exists from the beginning, then DTN routing will not be triggered for the specified message. This approach limits the propagation of DTN message copies to sparse areas only, since dense areas that are more exposed to link congestion, usually encounter AOMDV routing.

A. Hash Chaining for Secure Data Delivery

To ensure secure delivery of the cartography sensory information, we propose the use of hash chaining, where the sensory data payload is hashed recursively (using an appropriate hashing function) a number of times equal to the sequence number of the packet as shown in equation 1 below:

$$D = H^S(P), \tag{1}$$

where H represents the hash function, S is the packet sequence number and also the length of the hash chain, P is the data payload, and D is the resulting hash digest. The hash digest is sent along with the data payload all the way to the sink node on shore where the process is reversed. The sink uses the same hashing function and chaining concept to recursively hash the data payload a number of times equal to the sequence number of the received packet. The resulting hash digest should be identical to the hash digest that was sent by the source as part

of the packet. Otherwise, the sink ignores the received packet and all further packets received from the same source. This ensures authentication, integrity, and non repudiation of the received packet. The proposed solution is totally distributed, and does not require any central authority, pre-existing infrastructure, or the exchange of control messages.

IV. Proposed System Prototype and IoMaT Software Components

The Automatic Identification System (AIS) is an automatic positioning system that works by fitting small transponders onto ships that transmit a signal continuously. This helps to alerts other ships and shore stations equipped with AIS receivers to the presence of that ship along with other useful information. The signals and the information they carry, can be received by any ship, onshore station, or satellite fitted with an AIS receiver. It is then usually displayed on a screen using interactive chart-plotting software [23].

Designed to prevent marine collisions, AIS is essentially a VHF marine band data network that operates primarily on two dedicated VHF channels (AIS1 - 161,975 MHz and AIS2 - 162,025 MHz). Where these channels are not available regionally, the AIS is capable of automatically switching to alternate designated channels [24]. The AIS system needs power, two inputs, and one output to provide basic functionality. The first input is a GPS feed, for positioning, and the second is a VHF feed, which enables the system to receive incoming AIS signals from other ships. The output on the other hand is a VHF connection, that transmits the ships position and vessel information. Additional information from on board sensors can be input through a data feed as required [25]. AIS link layer communication is based on a self organizing TDMA access protocol. This means that a time period is divided into a number of time slots. When an AIS system switches on, it looks for a vacant time slot and reserves it. Other systems in range will avoid this slot and select another one. Precise timing is needed to ensure that all vessels are synchronised and this is derived from GPS; hence why an AIS system has its own GPS receiver [24].

A. AIS System Level Considerations and IoMaT Integration

The AIS system in Figure 1 shows the principal parts of a ship borne mobile AIS station and the required components to support IoMaT integration. The AIS transceiver transmits and receives radio signals that form the VHF Data Link and interconnect the AIS stations to each other. The GPS receiver supplies the coordinated universal time (UTC) to the AIS station to correct its own clock in order to synchronize all transmissions such that there are no collisions or overlaps which would degrade the information being transmitted [25]. Most AIS models have a 9-pin NMEA port which can be connected to a computer serial port using a standard RS 232 serial cable [26] [27]. In our proposed system, this port is used for relaying the IoMaT sensory data captured on each ship. Therefore, the existing VHF infrastructure is completely utilized for data transmission and no additional equipment is needed. Although only one radio channel is necessary for communication, each AIS station transmits and receives over two radio channels to avoid interference problems, and to allow channels to be shifted without communications loss from other ships. Therefore, in the proposed system, one channel can be used for voice while the other can be used for data communication simultaneously. However, in emergency situations or when channel shifting is needed, both channels can be utilized for voice usage.

Figure 1 also shows the proposed IoMaT software module hosted on a laptop/PC that is connected to the AIS system through an RS 232 serial interface. The module consists of the IoMaT message parser/encapsulator, the S-MADNET software router and the DTN buffer memory. The IoMaT message parser/encapsulator is responsible for parsing and processing the IoMaT input signals, processing messages into suitable transmission packets and sending the IoMaT output signals through the appropriate interface. The S-MADNET software router is responsible for routing the IoMaT messages through the marine network and making routing decisions based on IoMaT control messages. The DTN buffer memory provides a temporary storage unit for IoMaT DTN messages until a suitable target ship is available to receive the message or until the message is dropped on time-out. When a received IoMaT message is first detected at the IoMaT message parser/encapsulator, the message is processed and either sent to the AIS module for re-transmission using S-MADNET routing if a target ship is available and suitable, or else, sent to the DTN buffer memory. On the other hand, if the message is received locally through one of the IoMaT sensory units, the IoMaT message parser/encapsulator encapsulates the sensory information into a suitable AIS IoMaT message format, and proceeds to the routing phase where the message is either buffered at the DTN buffer memory or sent directly through the AIS module using AOMDV or DTN routing whichever suitable.

B. AIS IoMaT Message Format

AIS messages follow a specific format defined by the AIVDM/AIVDO protocol [28]. AIS receivers report ASCII data packets as a byte stream over serial or USB lines, using the NMEA 0183 or NMEA 2000 data formats. AIS packets typically have two introducers, either "!AIVDM" or "!AIVDO"; AIVDM packets are known to be reports from other ships while AIVDO packets are reports from the same ship. To incorporate IoMaT messages, we propose the use of two more introducers that uniquely identify IoMaT packets in an AIS system, namely "!AIVDN" and "!AIVDP". In the same sense, AIVDN identifies IoMaT packets from other ships and AIVDP identifies IoMaT packets from your own ship. Figure 2 shows an example of a standard AIS packet Figure 2(a) and IoMaT packet Figure 2(b) in an AIS system.

Every field in the packet has a specific meaning and is translated according to the AIVDM/AIVDO protocol as follows. Field 1 identifies the packet type, i.e., in Fig. 2(a),

!AIVDM	1	1	1	B	AIS Payload	0*5C

(a) AIS Standard Packet

!AIVDN	1	1	1	B	IoMaT Payload	0*5C

(b) AIS IoMaT Packet

Fig. 2: AIS ASCII Packet Format.

TABLE I: S-MADNET Simulation Parameters

Parameter	Sparse Area (North Sea)	Moderate Area(Clacton (UK)-Middleburg (Netherlands))	Dense Area (English Channel)
Simulation Time(s)	43200	43200	43200
Simulation Area	350 x 400 (km)	175 x 255 (km)	200 x 200 (km)
Average Number of nodes	53	79	100
Routing Protocol	AOMDV,Epidemic, Binary(SW),S-MADNET	AOMDV,Epidemic, Binary(SW),S-MADNET	AOMDV, Epidemic, Binary(SW),S-MADNET
Transmission Range	30(km) - 40(km)	30(km) - 40(km)	30(km) - 40(km)
TTL (s)	14400	14400	14400
Buffer size (MB)	25	25	25
Message size (bits)	1500	1500	1500
Movement Model	Real mobility from live AIS website	Real mobility from live AIS website	Real mobility from live AIS website

AIVDM indicates an AIS packet received from another ship and in Figure 2(b), AIVDN indicates an IoMaT packet also received from another ship. Field 2 identifies the number of fragments in an accumulating message, where in the examples of Figure 2 it is 1, i.e., the message consists of one fragment. Field 3 identifies the sequence number of the current fragment, which is 1, meaning that this is the first fragment. And since the previous field is also 1, therefore the example packet is complete on its own. Field 4 is a sequential message ID for multi-sentence messages. Field 5 is a radio channel code, where AIS Channel A is 161.975Mhz and AIS Channel B is 162.025Mhz. Field 6 is the data payload, where in the case of standard AIS packet Figure 2(a), every character of the ASCII code sequence, is interpreted into a specific message according to the AIVDM/AIVDO protocol (interested readers are referred to [28] for a complete mapping guide). While in the case of IoMaT packet (Fig. 2(b)), the payload consists of a complete S-MADNET packet. Finally, Field 7 represents the number of bits required to pad the data payload to a 6 bit boundary. In this example, its 0 bits. The *-separated suffix (*5C) is the NMEA 0183 data integrity checksum for the sentence.

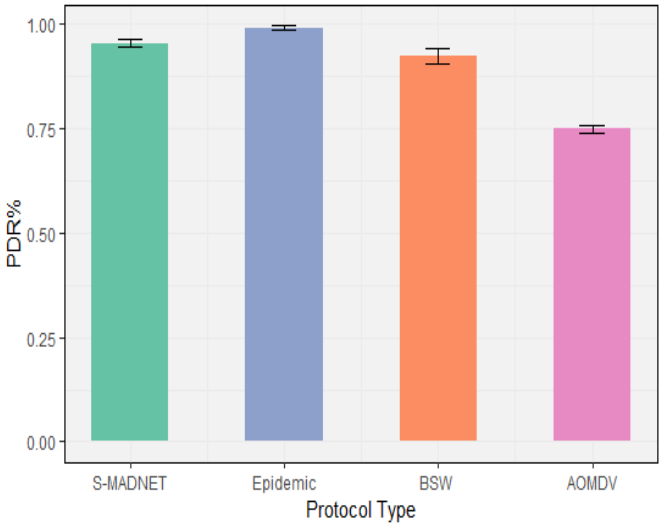

Fig. 3: Packet Delivery Ratio vs. Protocol Type (Dense Area)

V. Simulation and Performance Evaluation

To evaluate the performance of the proposed marine network, we use a model of the VHF radio that complies with

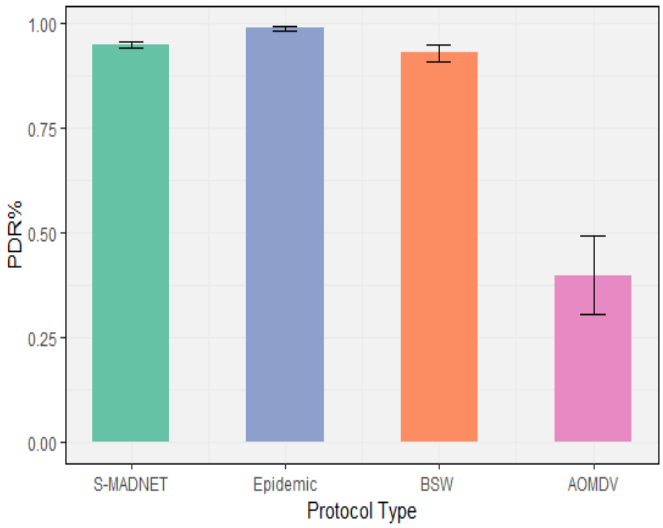

Fig. 4: Packet Delivery Ratio vs. Protocol Type (Moderate Area)

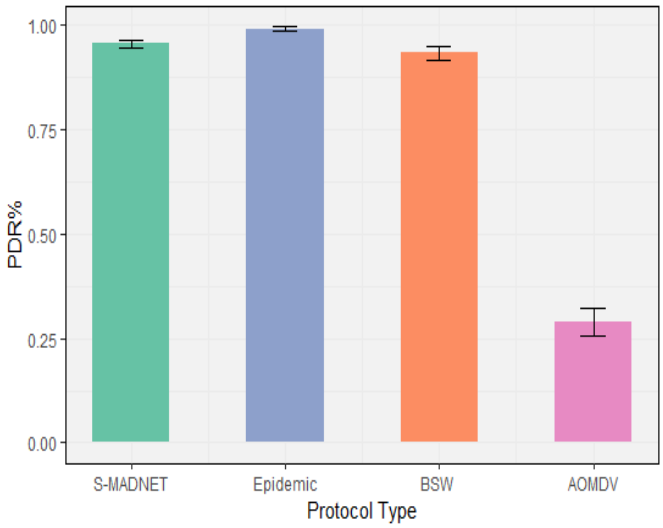

Fig. 5: Packet Delivery Ratio vs. Protocol Type (Sparse Area)

the International Telecommunication Union (ITU) standards to setup a Physical layer in the Network Simulator Version 2 (NS2). VHF transmission ranges were calculated using the Free Space Propagation model.

The simulation was performed using four routing protocols: Epidemic, Binary (SW), AOMDV and S-MADNET. The traffic source type used in the simulation is CBR (Constant Bit Rate) traffic with every ship generating 1500 bits/minute. The hash function SHA-1 is used to generate the hash chains producing a hash dogest of 160 bits. We have chosen to use 25 MB bundle buffer space, which does not become a bottleneck in the simulations. Bundle lifetime is set to 14400 seconds, after which all copies of the bundle will be deleted.

Total simulation time was set to 43200 seconds and three simulation scenarios were evaluated. The first is a sparse scenario in the North Sea with simulation area of 350 x

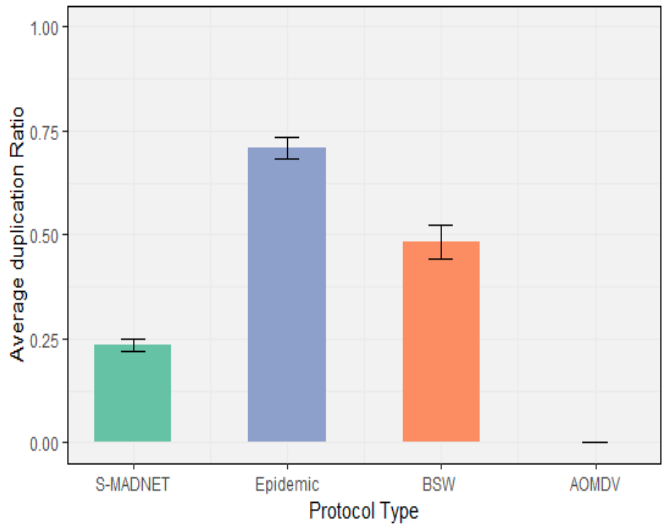

Fig. 6: Average duplication Ratio vs. Protocol Type (Dense Area)

400 km, and the second is a dense scenario in the English Channel with simulation area of 200 x 200 km and the third is a moderate scenario between Clacton (UK) and Middleburg (Netherlands) with simulation area of 175 x 255 km. Each scenario was simulated 6 times corresponding to 6 consecutive days from 9:00 am to 9:00 pm in order to show the variation in performance. We have used real ship trajectories and speed extracted from the real AIS data website in [29]. Table I shows a summary of the simulation parameters used in our simulation.

The performance of S-MADNET routing is evaluated in terms of Packet Delivery Ratio, Packet Duplication Rate, and Total Traffic Cost.

A. Packet Delivery Ratio (PDR)

PDR is the ratio of data packets that are received at the destination successfully. Figures 3, 4 and 5 compare the PDR rates of the simulated routing protocols in three scenarios, namely, dense, moderate and sparse scenarios respectively. It can be seen from the figures that the S-MADNET routing protocol achieves approximately 97% PDR rate in all three evaluated scenarios, which is very close to the Epidemic routing protocol that achieves 99% PDR rate. On the other hand, Binary (SW) and AOMDV achieved 94% and 75% respectively in the dense scenario vs. 95% and 40% respectively in the moderate scenario and 95% and 30% respectively in the sparse scenario. The difference in performance is obviously due to the frequent dis-connectivity in the sparse scenario as compared to the dense scenario which mostly impacts the AOMDV protocol that depends on end to end route establishment.

B. Packet Duplication Rate

The packet duplication rate is defined as the number of nodes in the network that hold a copy of a given packet over the total number of nodes in the network. Figures 6, 7 and 8 show the average packet duplication ratio per routing

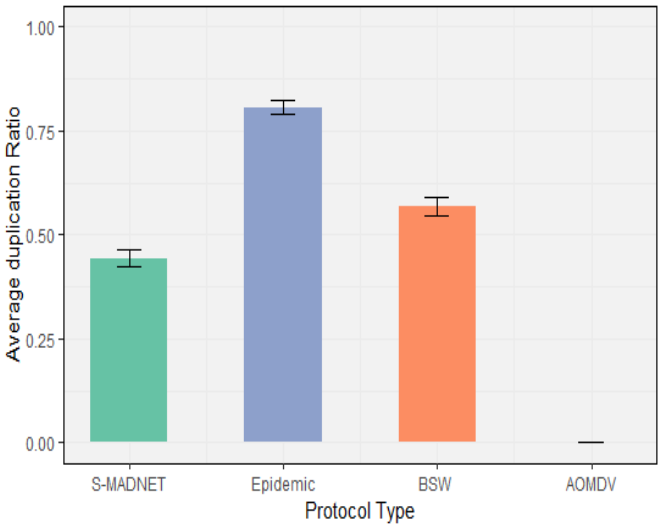

Fig. 7: Average duplication Ratio vs. Protocol Type (Moderate Area)

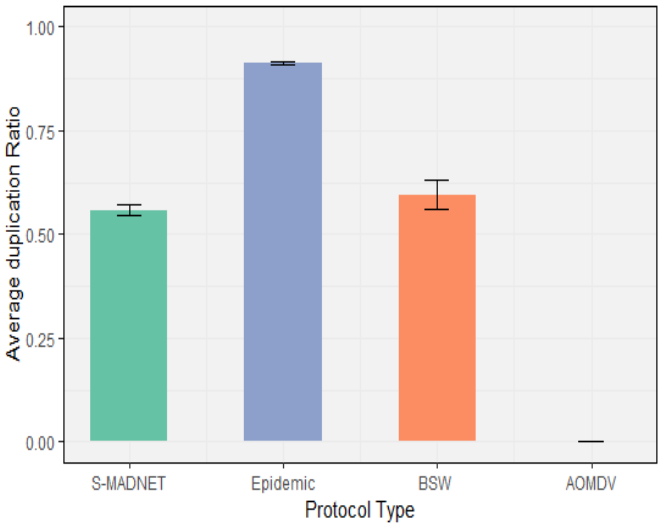

Fig. 8: Average duplication Ratio vs. Protocol Type (Sparse Area)

protocol in dense, moderate and sparse scenarios respectively. It can be seen from the figures that Epidemic routing protocol has the highest duplication ratio in all scenarios due to its stochastic nature, where the packet is always duplicated to all nodes within range until it reaches the destination. However, variations in the protocols performance can be seen from the three scenarios where the duplication ratio increases from 70% in the dense scenario, to about 80% in the moderate scenario and all the way to 90% in the sparse scenario. This is due to the network dis-connectivity rate that increases in sparse scenarios and decreases the possibility of packet delivery to the sink and also the possibility that an anti vaccine packet would spread back through the network nodes and stop the duplication in case the packet has been successfully delivered. It can also be observed from the figures that although the packet duplication rate for S-MADNET routing protocol increases

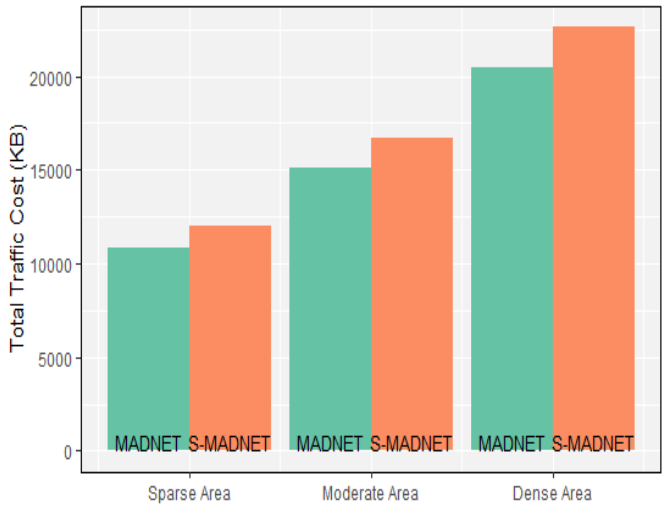

Fig. 9: Total Traffic Cost in MADNET vs. S-MADNET Routing Protocol

in a similar trend to Epidemic and Binary (SW) in the three evaluated scenarios; it outperforms both protocols substantially with duplication rates of 24%, 44% , and 57% in dense, moderate and sparse scenarios respectively. This is because of its efficient switching between AOMDV and Binary (SW) routing according to the route paths available. Finally, it can be seen that AOMDV routing protocol has 0% duplication rate in all three scenarios, as it does not duplicate packets under any circumstances.

C. Total Traffic Cost

The total traffic cost represents the cumulative packet delivery cost over the simulation run time in Kilobytes. Figure 9 shows the total traffic cost for MADNET and S-MADNET (two versions of the routing protocol proposed in this paper: with and without security support) in sparse, moderate, and dense areas respectively. It can be seen from the figure that S-MADNET imposes a marginally higher total traffic cost than MADNET in order to support the proposed security features. However, it is also clear that the difference does not exceed 1.5% in any of the simulated scenarios. This small overhead is introduced due to the inclusion of the hash digest in the packets sent from the ships towards the sink nodes at shore in order to facilitate data security.

VI. Conclusion

This paper has proposed a secure Mobile Ad-hoc/Delay Tolerant hybrid routing protocol (S-MADNET) for the IoMaT environment that switches automatically between MANET and DTN routing according to the network connectivity. An IoMaT routing module that forwards marine sensory data using the proposed secure protocol has also been presented, taking the AIS system level considerations into account. The paper has also shown that S-MADNET protocol outperforms all the evaluated counterpart protocols in its overall performance with the

objective of maximizing the packet delivery ratio and minimizing the packet duplication rate while maintaining data security. Therefore, S-MADNET routing protocol is considered the best option for the marine environment considering the latter's specific characteristics of low transmission bandwidth, random topology, no underlying infrastructure and mixed dense/sparse scenarios.

REFERENCES

[1] F. Weng, X. Zou, and Z. Qin, "Uncertainty of amsu-a derived temperature trends in relationship with clouds and precipitation over ocean," *Climate dynamics*, vol. 43, no. 5-6, pp. 1439–1448, 2014.

[2] Ofcom, "More radio spectrum for the internet of things." [Online]. Available: http://stakeholders.ofcom.org.uk/consultations/radio-spectrum-internet-of-things/

[3] Z. Zhang, "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 1, pp. 24–37, 2006.

[4] R. Al-Zaidi, J. C. Woods, M. Al-Khalidi, and H. Hu, "Building novel vhf-based wireless sensor networks for the internet of marine things," *IEEE Sensors Journal*, vol. 18, no. 5, pp. 2131–2144, 2018.

[5] R. Al-Zaidi, J. Woods, M. Al-Khalidi, and H. Hu, "An iot-enabled system for marine data acquisition and cartography," *Transactions on networks and Communications*, vol. 5, no. 1, 2017.

[6] V. Del Duca Almeida, A. B. Oliveira, D. F. Macedo, and J. Nogueira, "Performance evaluation of manet and dtn routing protocols," in *Wireless Days (WD), 2012 IFIP*. IEEE, 2012, pp. 1–6.

[7] M. Patil and R. C. Biradar, "A survey on routing protocols in wireless sensor networks," in *Networks (ICON), 2012 18th IEEE International Conference on*. IEEE, 2012, pp. 86–91.

[8] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2003, pp. 27–34.

[9] A. Boukerche, *Algorithms and protocols for wireless, mobile Ad Hoc networks*. John Wiley & Sons, 2008, vol. 77.

[10] P. Parvathi, "Comparative analysis of cbrp, aodv, dsdv routing protocols in mobile ad-hoc networks," in *Computing, Communication and Applications (ICCCA), 2012 International Conference on*. IEEE, 2012, pp. 1–4.

[11] A. Moravejosharieh, H. Modares, R. Salleh, and E. Mostajeran, "Performance analysis of aodv, aomdv, dsr, dsdv routing protocols in vehicular ad hoc network," *Research Journal of Recent Sciences ISSN*, vol. 2277, p. 2502, 2013.

[12] S. Biradar, K. Majumder, S. K. Sarkar, and C. Puttamadappa, "Performance evaluation and comparison of aodv and aomdv." *International Journal on Computer Science & Engineering*, vol. 2, no. 2, 2010.

[13] L. Wan, F. Liu, J. Zhang, and H. Zhang, "Performance evaluation of routing protocols for delay tolerant networks," *Computer Science & Information Technology*, vol. 5, no. 11, 2015.

[14] T. Abdelkader, K. Naik, A. Nayak, N. Goel, and V. Srivastava, "A performance comparison of delay-tolerant network routing protocols," *IEEE Network*, vol. 30, no. 2, pp. 46–53, 2016.

[15] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2001, pp. 299–302.

[16] K. El Defrawy and G. Tsudik, "Privacy-preserving location-based on-demand routing in manets," *IEEE journal on selected areas in communications*, vol. 29, no. 10, pp. 1926–1934, 2011.

[17] S. K. Dhurandher, A. Kumar, and M. S. Obaidat, "Cryptography-based misbehavior detection and trust control mechanism for opportunistic network systems," *IEEE Systems Journal*, no. 99, pp. 1–12, 2017.

[18] J.-H. Cho and R. Chen, "Provest: provenance-based trust model for delay tolerant networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 151–165, 2018.

[19] R. Mohsin and J. Woods, "Performance evaluation of manet routing protocols in a maritime environment," in *Computer Science and Electronic Engineering Conference (CEEC), 2014 6th*. IEEE, 2014, pp. 1–5.

[20] R. J. Mohsin, J. Woods, and M. Q. Shawkat, "Density and mobility impact on manet routing protocols in a maritime environment," in *Science and Information Conference (SAI), 2015*. IEEE, 2015, pp. 1046–1051.

[21] R. Mangrulkar and M. Atique, "Routing protocol for delay tolerant network: A survey and comparison," in *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on*. IEEE, 2010, pp. 210–215.

[22] K. K. Sevimli and M. Soyturk, "Lifetime determination for delay tolerant communications in sparse vehicular networks," in *Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on*. IEEE, 2010, pp. 250–255.

[23] B. O. Data, "The definitive ais handbook." [Online]. Available: https://www.marineinsight.com/wp-content/uploads/2016/11/AiS-Whitepaper.pdf

[24] F. E. P. Development, "Ais: A guide to system development." [Online]. Available: https://fidus.com/wp-content/uploads/Guide_to_System_Development_March_2009.pdf

[25] R. Essaadali, C. Jebali, K. Grati, and A. Kouki, "Ais data exchange protocol study and embedded software development for maritime navigation," in *Electrical and Computer Engineering (CCECE), 2015 IEEE 28th Canadian Conference on*. IEEE, 2015, pp. 1594–1599.

[26] J. Deng, "Real-time navigation monitoring system research for lng-fuelled ship in inland water," *Journal of Maritime Research*, vol. 12, no. 2, pp. 87–94, 2017.

[27] E. Alincourt, C. Ray, P.-M. Ricordel, D. Dare-Emzivat, and A. Boudraa, "Methodology for ais signature identification through magnitude and temporal characterization," in *OCEANS 2016-Shanghai*. IEEE, 2016, pp. 1–6.

[28] E. S. Raymond, "Aivdm/aivdo protocol decoding," *GPSD documentation Version*, vol. 1, 2014.

[29] F. Inc., "Live marine traffic." [Online]. Available: https://www.marinetraffic.com/en/