A Geolocation and Smart Alert System for Nearby First Responders on Roll-on/Roll-off Vessels

by Paschalis Mpeis (University of Cyprus), Jaime Bleye Vicario (Centro Jovellanos, Spain), and Demetrios Zeinalipour-Yazti (University of Cyprus)

A4IoT is an innovative localisation architecture that supports a smart alert system to provide monitoring, navigation and guidance to first responders during fire outbreaks on roll-on/roll-off (Ro/Ro) vessels.

With global trade increasing over the last decade, the maritime industry has grown significantly. Each month, more than 10,000 vessels pass through the Strait of Dover, including cargo ships, tanker ships, roll-on/roll-off ships (Ro/Ro), passenger ships and others. Globalisation and the recent advent of low-cost manufacturing facilities has fuelled an interest in innovative systems to tackle existing issues to lower the costs, improve safety standards and comply with international and regional regulations.

Vessel-owners and passengers have the expectation that, just like other smart spaces (e.g., factories and hospitals), marine vessels will benefit from the latest Internet of Things (IoT) technology. One obvious application of this technology is localisation – obtaining the geographic location of an object by means of digital information processed via a network. Although satellite-based localisation, e.g., GPS, is globally available, it works only in outdoor spaces and is obstructed by the bulky steel structures of vessels. Additionally, vessels lack onboard hardware infrastructure that facilitates indoor localisation, e.g., dense networks of Wi-Fi or UWB, due to the high installation and maintenance costs. On the other hand, there is a growing expectation and a need to localise assets on vessels and to have efficient solutions that work even in the harshest conditions.

The technology that performs accurate on-vessel localisation carries out a variety of important tasks, including: asset tracking, monitoring, analytics, navigation and safety. The localisation literature is very broad and diverse as it exploits several technologies. GPS is ubiquitously available but is energetically expensive and cannot operate in indoor environments. Alternative solutions include: infrared, bluetooth low-energy (BLE), visual or acoustic analysis, RFID, ultra-wide-band (UWB), wireless LANs, or a combination of these into hybrid systems.

In the context of the funded EU Horizon 2020 LASH-FIRE project (nº 814975), which aims to integrate new and

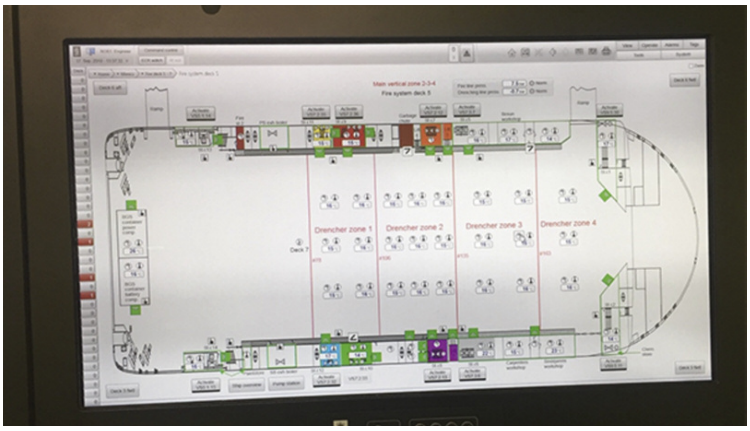

Figure 1: The Fire Resource Management Centre (FRMC) of the Stena Jutlandica Ro/Ro vessel will be augmented with A4IoT to enable real-time tracking of fire hazards and to guide trained personnel in controlling them.

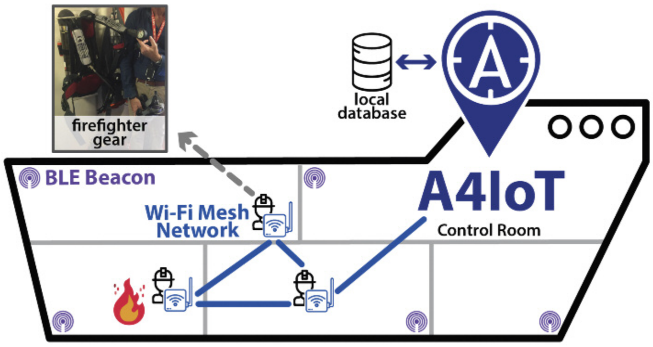

Figure 2: Architectural diagram of A4IoT in a vessel that uses statically attached BLE beacons, and portable IoT devices attached to firefighters' gear, with Wi-Fi mesh-capable routers, BLE receivers, and cameras. Localisation relies on a 2-layer network: a) the Wi-Fi mesh-topology network, that enables connectivity between A4IoT and the firefighters for exchanging text, audio, or video, and b) a BLE beacon sensor broadcast network that will provide accurate localisation within the vessel through RSSI measurements.

advancing technologies to improve safety and security, environmental and personnel impacts and facilitate international trade, we are focusing on effective fire management operations on ro/ro vessels. We are developing a smart alerting system in the form of a vessel indoor information system (see Figure 1) for nearby first responders. The system provides indoor fire intelligence: data collection, data alignment of measurements, activity recognition and orientation, heatmap and crowdsourcing. Our platform will enable messages to be sent (text, audio, video or images) to the crew around the activated fire detector with important safety information about tackling the fire.

Our proposed architecture comprises data, localisation and network layers, as shown in Figure 2. In the control panel of a vessel, an A4IoT backend is automatically deployed using docker [1]. The data layer is kept locally in a document database, the RM data. For the localisation layer we use a long-range beacon-based BLE fingerprint localisation algorithm that provides deck-level accuracy. We are also investigating the use of a computer vision- (CV) based, infrastructure-less localisation algorithm using YOLO [L1] and OpenCV. For the BLE system, we are installing a set of beacons across the vessel's indoor spaces. For the CV technology, we will attach IoT devices with cameras, as well as portable network devices, onto firefighters' gear. This will create a mesh-topology network on-the-fly and give a secure connection between firefighters and the backend, enabling text, audio, video, and localisation data exchange.

To provide localisation, A4IoT [L2] uses a hybrid indoor radio map (RM) that uses the concept of fingerprinting and works seamlessly on the edge/IoT devices. It can operate without connection to the internet with radio signals from different sensors, e.g., Wi-Fi, BLE, or CV. In an offline phase, a logging application records the "fingerprints", which consist of received signal strength indicators (RSSI) of these sensors at certain coordinates (x,y) pinpointed on a vessel's deck map (e.g., every few metres). In the case of CV, it uses extracted textual information from captured images in the place of the RSSI values. Subsequently, in a second offline phase the sensor fingerprints are joined into several N x M matrices, termed the "RM" (i.e., one RM per sensor type), where N is the number of unique (x,y) fingerprints and M the total number of beacons. Finally, an IoT device attached to a firefighter can compare its currently observed fingerprint against the respective sensor-type RM to find the best match, using known algorithms such as KNN or WKNN [2]. Our solution can be infrastructure-free, as it performs best-effort operation with whatever sensor type is available. This information can then be used to guide the firefighters.

Links:
[L1] http://pjreddie.com/darknet/yolo/
[L2] https://anyplace.cs.ucy.ac.cy

References:

[1] P. Mpeis et al.: "The Anyplace 4.0 IoT Localization Architecture", in 2020 21st IEEE International Conference on Mobile Data Management (MDM), pp. 218-225, IEEE, 2020.
[2] C. Rizos et al.: "Indoor positioning techniques based on wireless LAN," in 1st IEEE Intl. Conf. on Wireless Broadband and Ultra Wideband Communications. IEEE, 2007, pp. 13–16.

Please contact:

Demetrios Zeinalipour-Yazti
Data Management Systems Laboratory (DMSL), University of Cyprus
+357 22 892755, dzeina@cs.ucy.ac.cy

Understanding Complex Attacks on a Maritime Port

by Sandra König (AIT Austrian Institute of Technology)

Attacks on maritime ports have become more sophisticated since modern ports turned into cyber-physical systems. Simulation models can help with the vital task of detecting such attacks and understanding their impacts.

Digitalisation introduces new challenges to the protection of modern critical infrastructures, such as maritime ports. While control systems ensure smooth physical operations, they are also accompanied by new threats. Complex attacks such as advanced persistent threats (APTs) or drug smuggling [L1] make explicit use of the interconnection between cyber and physical systems of a port. Their stealth makes them difficult to detect and their potential impacts can only be estimated. Impact estimations in this context should be based on a formal analysis of the system. During the course of the European Commissions project SAURON [L2] a model has been developed that simulates the aftermath of a security incident in a port in order to understand the impact on the port as well as the local population.

The simulation model represents the maritime port as a graph where nodes describe relevant assets, and edges describe a dependency between two assets. Assets can be physical (crane, gate, truck or camera), cyber (server, working laptop or a database), but also represent processes (identification of employees, registration of a container). Once the dependency graph is known, the internal dynamics of each asset are modelled. Its functionality is described on a three-tier scale, where states can be interpreted as "working properly" (state 1), "partially affected" (state 2) or "not working" (state 3). The state of the asset changes depending on notifications about events that have happened. Due to the complexity of the considered attacks, the state changes are assumed to happen with a certain likelihood. Once these likelihoods are determined, it is possible to mimic how an attack spreads through the entire system. A formal description of the model is given in [1] and the idea is illustrated in Figure 1.

A practical application of the formal model to a concrete problem follows these steps [2]: