REAL-TIME MONITORING OF THE GREAT BARRIER REEF USING INTERNET OF THINGS WITH BIG DATA ANALYTICS

Marimuthu Palaniswami[1], Aravinda S. Rao[1], Scott Bainbridge[2]
[1]The University of Melbourne, Dept. of Electrical and Electronic Engineering Parkville, VIC - 3010, Australia
[2]Australian Institute of Marine Science PMB #3, Townsville, QLD - 4810, Australia

Abstract –The Great Barrier Reef (GBR) of Australia is the largest size of coral reef system on the planet stretching over 2300 kilometers. Coral reefs are experiencing a range of stresses including climate change, which has resulted in episodes of coral bleaching and ocean acidification where increased levels of carbon dioxide from the burning of fossil fuels are reducing the calcification mechanism of corals. In this article, we present a successful application of big data analytics with Internet of Things (IoT)/wireless sensor networks (WSNs) technology to monitor complex marine environments of the GBR. The paper presents a two-tiered IoT/WSN network architecture used to monitor the GBR and the role of artificial intelligence (AI) algorithms with big data analytics to detect events of interest. The case study presents the deployment of a WSN at Heron Island in the southern GBR in 2009. It is shown that we are able to detect Cyclone Hamish patterns as an anomaly using the sensor time series of temperature, pressure and humidity data. The article also gives a perspective of AI algorithms from the viewpoint to monitor, manage and understand complex marine ecosystems. The knowledge obtained from the large-scale implementation of IoT with big data analytics will continue to act as a feedback mechanism for managing a complex system of systems (SoS) in our marine ecosystem.

Keywords – Artificial intelligence, big data analytics, coral bleaching, Internet of Things, wireless sensor networks, real-time monitoring, event detection

1. INTRODUCTION

The Great Barrier Reef (GBR) of Australia consists of 3200 coral reefs extended over 280 000 square km [1]. The GBR has about 900 islands covering 2600 km that include mangrove forests, coastal wetlands and estuaries, deep shoals, seagrass meadows, continental shelf margin and slope [2]. Both economically and ecologically, Australia significantly gains benefits from this geographically-important marine ecosystem. However, the burning of fossil fuels releases carbon dioxide (CO_2), which in turn is absorbed by oceans, resulting in acidification. This process inhibits corals from secreting calcium carbonate exoskeletons [3], reducing (calcification) the reef-building mechanism and associated organisms. Rise in global temperature is also putting more stress on the marine species. Coral bleaching is the process where the relationship between the coral and its symbiotic algae breaks down during rapid changes in sea-water temperature (hot or cold), making corals vulnerable [4].

Anthropogenic activities are attributed to increased stresses on coral reefs as the prominent reason for coral bleaching. Episodes of bleaching at regional scales have been occurring for many decades (prior to the 1980s), but due to a lack of reporting, documentation and understanding, it is difficult to measure the extent of the bleaching effect prior to the 1980s [5]. In 1911, the first thermal bleaching incident was reported at Bird Key Reef in the Florida Keys, where large numbers of corals were injured during abnormally hot and calm weather conditions, killing many fish, Diadema and molluscs [6]. In 1929, a similar bleaching incident was reported at Low Isles on the GBR, killing many corals [7]. The reports of bleaching incidents have grown significantly since 1971, and this has been linked to climate change [8].

The Australian Institute of Marine Science (AIMS) collects environmental data to analyze and address these challenging questions. It is understood that the catastrophic thermal stress might seriously impact the GBR over the next century [8]. As a result, it is imperative that we understand the temperature patterns and ecological response to mitigate the human-activity-induced stresses [5]. Given the lack of evidence, complex environmental simulation models with detailed characterization are more likely to lead to more uncertainty [9]. The only way to approach this problem is to collect information on the tropical marine environment, assisting to develop more robust models with evidence. However, the challenge here is to collect data at the appropriate spatial and temporal scales [10]. The sensitive environmental dynamics on the GBR necessitates real-time monitoring as a way of managing and understanding anthropogenic stresses effectively.

Internet of Things (IoT)/wireless sensor networks (WSNs) enable real-time, remote sensing at fine spatial and temporal scales of large areas (such as the GBR) [11]. WSNs consist of a network of sensor nodes deployed at multiple, statistically important locations. Sensor nodes are equipped with relevant sensing elements, data processor units, transceiver with antennas, power systems and protective housings [12]. The network of sensor nodes is formed by directing the nodes to communicate with specific nodes in the network. Sensor networks promise to allow data collection at a higher sampling frequency (including finer spatial and temporal scales) while able to keep the cost to a minimum, and provide real-time access to a range of parameters [13]. In addition, visualization of sensor data on a web portal in real time with modeling and simulation results, have clearly changed the approaches to monitoring the GBR.

Artificial intelligence (AI) plays a critical role in analyzing real-time streaming sensor data from such large-scale environments. Given the volume of data received from the sensor nodes, the data needs to be modeled to make a meaningful sense of the data. To extract useful information from the marine system, WSNs/IoT need appropriate network architecture, protocols, communication with AI-based analytics helping to inform end users [14]. Designing such networks requires categorizing sensor networks into different communication models, data delivery models, and network dynamic models. However, technical challenges in implementing such networks include network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security. The role of AI and data analytics, is vital in such situations. AI incorporates several elements of learning, adaptation, evolution and fuzzy logic to intelligently analyze data and create intelligent machines to extract and represent information in a meaningful way [15].

In this article, we present our previous experiences in implementing real-time WSN/IoT for monitoring the GBR. The article focuses on implementation challenges and how AI was used to detect interesting events from the deployed WSN. Clause 2 describes the measures taken to monitor and understand GBR. It also provides the challenges faced in deploying WSN on the GBR. Clause 3 provides the proposed network architecture used in monitoring the GBR using WSN. Clause 4 provides a case study of detecting Cyclone Hamish (that passed through the GBR during March 2009) using a suite of AI algorithms and some of the open challenges in system of systems (SoS) integration with AI. The conclusion of this article is provided in clause 5.

2. THE GREAT BARRIER REEF MONITORING

The GBR is the largest living structure that stretches over 2300 kilometers. It includes 600 types of coral, over 100 jellyfish species, more than 3000 varieties of molluscs, 1625 kinds of fish, 133 types of sharks and rays, and over 30 different types of whales and dolphins. It is also unique as the GBR extends 14 degrees of latitude, including 600 continental islands and about 150 inland mangrove islands [16].

The Great Barrier Reef Ocean Observing System (GBROOS) Project, which is part of the Australian Integrated Marine Observing System (IMOS), has been supported by a special National Collaborative Research Infrastructure Strategy (NCRIS) grant from the Australian Government. GBROOS is an observation system that looks to record the impact of the Coral Sea on the GBR. Specifically, GBROOS aims to provide the observational data to understand the long-term change and impact on the GBR. The GBROOS has five components of monitoring [17]:

1) nine long-term moorings (temperature and salinity profiles, waves and currents)
2) two reference moorings (basic oceanographic parameters)

3) IoT/WSNs on seven islands (reefs) (temperature profiles and weather data)
4) remote sensing using satellites (surface temperature and ocean color data)
5) underway sampling (temperature, salinity, chlorophyll).

WSN/IoT provides real-time sensing of spatially and temporally dense measurements of a range of bio-physical parameters [18]. Without WSN/IoT technology, it is difficult to get such spatially and temporally dense record of bio-physical events, which is what makes the WSN deployment so important. In addition, WSN/IoT significantly improves the access to real-time data covering long time and large-scale geographical areas. WSN/IoT find its use highly important in benthic zones [19], as well as to understand the effect of heat and light on coral bleaching [20]. Furthermore, WSN/IoT data allows us to understand complex ocean processes impacting reefs, and providing detailed environmental information up to the coral bommie (outcrop of coral reef) level [20]. The WSN/IoT data from Lizard Island, Orpheus Island, Rib Reef, Myrmidon Reef, Davies Reef, Heron Island and One Tree Island, coupled with four other complementary sensing components (as listed above), provide a dense environmental information source. The real-time data from the integrated system enables the detection of interesting events and for managers to take immediate action.

Figure 1 shows the IoT/WSN deployment sites at seven locations on the GBR. The harsh marine environments of the GBR poses several challenges in implementing large-scale IoT/WSN and observing the data in real time. The sensor nodes are aware of their spatial locations, providing three dimensional data [spatial position (x,y) and depth (z)] [10]. In the event of unsuccessful transmission by a sensor node, a node could be reconfigured to transmit data to other nodes. The data could then be rerouted to the base station without loss. The implementation challenges include network design, sensor node design with protective casings, floating buoys to house sensor nodes, reliable moorings that can withstand tides, water currents and heavy storms. There is always a chance of sea creatures dismantling the setup either due to curiosity or accidently. The following subclause highlights some of the challenges:

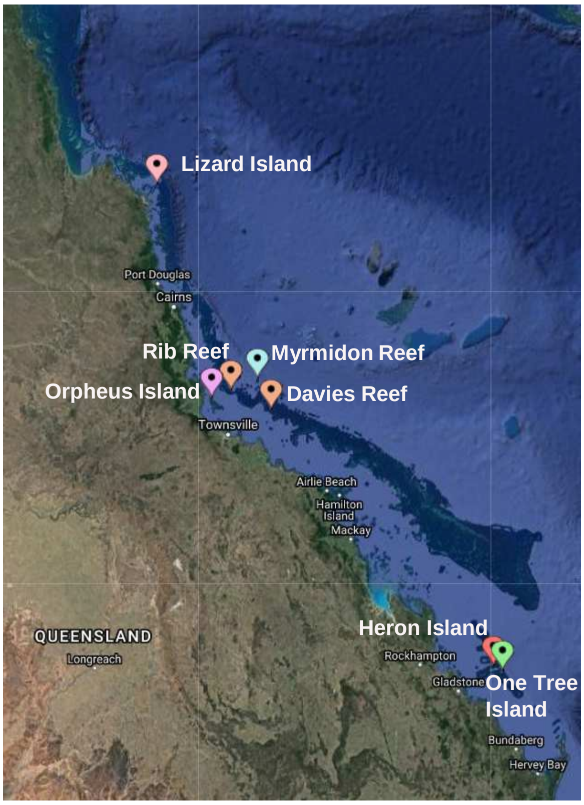

Fig. 1. Map of seven IoT/WSN deployments sites on the GBR. Monitoring of Rib Reef, Myrmidon Reef and Davies Reef have been decommissioned in 2014. Image source: Map Data © 2017 Google Images

2.1. Sensor network and sensing elements

Sensor nodes are resource constrained i.e., they have limited processing power, battery, memory to store and process data. Therefore, the design of sensor networks is application-specific. The architecture design of sensor networks is aimed at maximizing the lifetime of the network at the cost of expending limited resources. These constraints also influence the data sampling times and spatial distribution of sensor nodes. Marine environment is relatively aggressive compared with other environments, requiring specialized sensing elements for continuous monitoring [21]. Marine environment monitoring requires the integration of sensor nodes, such as WSN based iMote2 [22] and IoT-enabled Waspmote [23]. The sensors also need to be calibrated prior to deployment and corrected for drifts in readings from true value over time, as a result of gradually degrading calibration.

2.2. Securing buoys and casing

Sensor nodes need floating buoys to hold the electronics in a secure casing, protection from surrounding environments to avoid water, humidity build-up or condensation. Experience from previous deployments have indicated equipment will foul and corrode [24]. Therefore, utmost care must be taken when deploying sensor nodes in marine environments, given there is a high chance of contact with sea water. The floating buoys are the preferred protective casings for marine environments. However, the buoys introduce several challenges. First, the buoys consisting of sensor nodes need moorings fixed usually to the sea floor using cables. Second, depending on the type of sensing element we may also have to run a long cable with a sensing element, causing deterioration of the measured signal from the sensing element. Third, the buoys drift due to ocean currents and tides, causing radial (vertical) and tangential (horizontal) displacements of sensors nodes. Therefore, these displacements are likely to cause issues with wireless data transmission as the nodes move in a manner that they are unable to be in the communication range of the deployed sensor network.

2.3. Communication and scheduling constraints

Communication in a sensor network can be categorized into two kinds: local coordination and sensor-base communication [25]. Local coordination involves aggregating data among a group of nodes. The sensor-base communication is concerned with communicating the aggregated data to a base station. Both these types of data aggregation could utilize single-hop or multi-hop communication [26]. The data could be logged to a data logger, or collected manually using regular site visits, or using a microwave communication link (such as, the setup at Davies Reef) [27]. Radiocommunication draws most of the battery power. Hence, scheduling of sleep and wake-up cycles to sense environment, store data, and transmit data are critical to prolong the operational time of the network.

2.4. Scalable networking architecture

Marine environments need sensor networks that have flexible architecture to cover spatially small (few meters) as well as large (few kilometer) areas. Therefore, the sensor network architectures need to be scalable. Homogenous sensor networks consist of sensor nodes of the same processing power, radio range, data storage capacity, and networking abilities. These attributes of a homogenous network limit the topology of the sensor network to be flat i.e., it is not scalable in the event of dynamic rerouting or reconfiguration of network nodes. On the other hand, heterogeneous network includes sensor nodes having varied processing, communication, and storage abilities. These attractive features of heterogeneous sensor nodes provide scalable networking solutions through hierarchical architectures. Tenet [28], Tsar [29], SensEye [30], Asap [31], and Citric [32] are some of the examples of heterogeneous networks.

2.5. Detecting interesting events using AI

The network topology of IoT/WSN can be a star, mesh, tree or a combination of all [33]. The way that data moves across the network from one location to another depends on the topology. Thus, event detection can be local or global relative to the network. Local events are specific to the sensor nodes, whereas global events require the sensor data to be gathered at a centralized location. Local event detection requires processing power at the sensor nodes. Often, the computational power, memory and resources are limited in individual nodes. Therefore, simple event detections locally are often relatively easy and will be based on one-dimensional sensor data. For example, detecting changes in temperature level above a certain threshold is an example of a local event. On the other hand, global event detection involves high computational power, memory, sophisticated AI algorithms and network resources. Global events also consider multidimensional sensor data from multiple sensors. For example, detecting an island-wide temperature change is an example of a global event. AI algorithms face challenges due to error in data, data loss, non-generative data models, temporally and spatially incomplete records of physical phenomenon and certain marine artefacts affecting the sensor data. The challenge in IoT/WSN to detect events is to identify anomalous events in a resource-constrained setup.

3. CLOUD-CENTRIC NETWORK ARCHITECTURE FOR REAL-TIME MONITORING

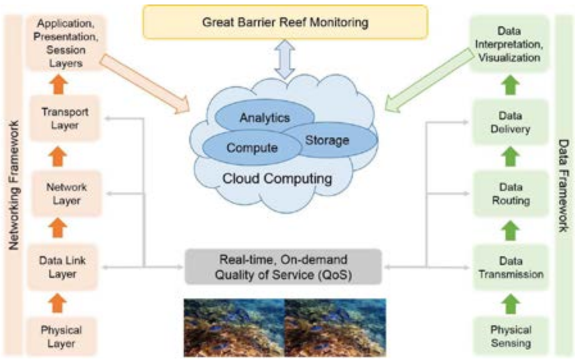

Fig. 2. Proposed IoT/WSN architecture for real-time monitoring, managing and understanding of environment

Figure 2 shows the proposed cloud-centric network architecture for real-time sensing, monitoring and decision-making. The data framework in Fig. 2 illustrates how data is converted when transferring from lower layers of the network architecture to layers above. The data from the end-user applications are managed through a cloud platform. The platform contains computing hardware and software, data storage capacity and AI analytics to service end users on a real-time basis.

3.1. Networking framework

The networking framework shows the networking protocols from physical layer up to the application layer. The layers are conceptually similar to the Open Systems Interconnection (OSI) model. The layers ensure that the control is passed from the layer below to the layer above. The physical layer allows physical transmission of data bits, whereas the data link layer allows transfer of data from one sensor node to another. The network layer determines the path on the network to the correct physical node by managing Internet Protocol (IP) addresses. The transport layer manages end-to-end connections and reliability of network. This is achieved by transferring data across network connections. Transfer Control Protocol (TCP) is an example of a transfer layer protocol.

Figure 2 also shows that the data link layer, network layer and transport layers together are responsible for controlling the quality of service (QoS) demands requested by the users as well as for prioritizing data for real-time applications, such as video [34]. The session layer manages different types of communications between hosts. This operation includes the opening and closing of sessions. The presentation layer manages contexts between applications by handling format conversions, encryption/decryption, independent of application – web content is an example. The application layer is the topmost layer and is used by the end users. It provides services to end-user applications through appropriate networking protocols, such as Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS). Web browser, is an example of application layer that uses HTTP or HTTPS networking protocol for a wide variety of services.

3.2. Data framework

The data framework provides a model of the data flow from physical sensing to data transmission among sensor nodes, routing through different networks, delivery with appropriate encapsulations, interpretation and visualization based on cloud computing and analytics. Sensors attached to the nodes measure physical phenomena and processing boards are programmed to sample at specific sampling rates. Sensor nodes are spatially distributed based on the project plan, cost, application and scientific objectives. The data from the sensors are stored temporarily on board the nodes, before they are transmitted to gateway nodes. The data link layer handles data transmission by sensing the physical medium and channel availability. Once the data is transferred from nodes to gateways, the data will be directed to high-level nodes, such as the cloud servers. Gateways are programmed to direct the data from sensor nodes to cloud databases through IP addresses. The network layer manages the IP addresses and data routing. The delivery of data to a particular database is ensured by the transport layer. Cloud servers manage the storage of received data from sensor nodes and also have high computation compared to sensor nodes. The data is made available to end users through applications from the cloud servers. Servers also manage application sessions among different hosts, as well as allow multiple sessions for the same application from multiple users.

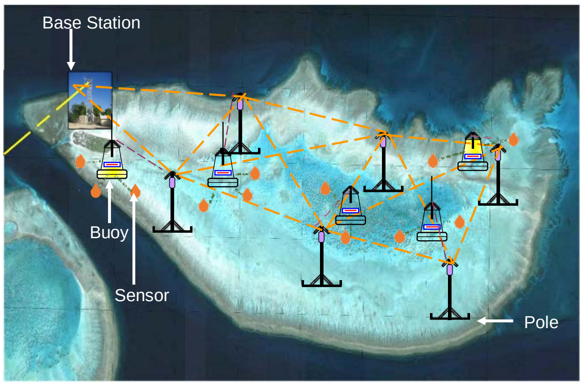

Fig. 3. IoT/WSN deployed at Heron Island of the Great Barrier Reef. Figure shows sensor nodes networked to communicate with buoys, which in turn communicate with poles. Finally, the data from the poles are transmitted to a base station. The base station transmits the data to the mainland that is 75 km away

4. CASE STUDY: DETECTING CYCLONE HAMISH ON HERON ISLAND OF GBR USING AI

In this clause, we provide a case study from the IoT/WSN deployed on Heron Island for real-time monitoring of the GBR and in particular the passage of Tropical Cyclone Hamish in 2009. The Australian Federal Government and Queensland State Government provided funding for the Australian Integrated Marine Observing System (IMOS) [20], which included five components to observe ocean parameters with the IoT/WSN being one of them. By mid-2008 the IoT/WSN had been installed at Heron Island with the other sites completed by 2010.

Figure 3 shows the deployment of heterogeneous sensor nodes with hierarchical network architecture. The network consists of 5 buoys and 6 poles in the lagoon area of the GBR, with a spatial resolution of 2 km. The first tier (top level) consists of poles, followed by floating buoys (as second tier). Sensor nodes are connected to buoys via appropriate cabling. Further, sensor nodes are equipped with temperature probes that measure sea temperatures below the surface. For this case study, we have considered one month of data (collected from 21 February 2009 to 22 March 2009, 9:00am to 3:00pm with 10 minutes sampling frequency) [15, 21, 35].

4.1. WSN network architecture

Figure 4 shows the network architecture of the deployed IoT/WSN on Heron Island. The buoys use single-hop communication to send data to poles, and poles use multi-hop communication to send data to the base station. One of the poles is housed with a weather station, measuring air temperature, pressure, humidity, rain, wind speed and direction. The data from this weather station is collected every 10 minutes. The data received by the main base station is then transmitted to a database that is 75 km away on the Australian mainland using the Telstra 3G network.

4.2. Cyclone Hamish detection using AI

Event detection in the case of Heron Island involved detecting anomalous patterns from the sensor data. The key challenge here is to identify anomalous events in the resource-constrained IoT/WSN setup while achieving high detection accuracy [36]. We approached the problem using our previously established method of detecting elliptical anomalies or Elliptical Summaries Anomaly Detection (ESAD). This is achieved by first modeling the collected data at individual sensor nodes by sample-based ellipsoids and numerically clustering the sets of ellipsoids [36, 37]. Next, a dissimilarity measure of the data is constructed using improved visual assessment of cluster tendency (iVAT) [38]. This step provides us a visual tendency of assessment (VAT) to seek the presence of the number of clusters of ellipsoids in the data. The block within the dissimilarity matrix is reordered using a recursive iVAT algorithm. As a final step, a single linkage algorithm is employed to extract anomalous clusters from the dissimilarity data. Using this AI approach, we were able to clearly identify the pattern of the passage of Tropical Cyclone Hamish appearing as an anomaly before and after the cyclone passed through Heron Island in 2009. The algorithm has since been transformed for real-time applications. Recently, we were able to demonstrate that the Cyclone Hamish event from the WSN data can be detected in real-time IoT settings using our suite of AI algorithms.

4.3. System of systems (SoS) view of integrated AI

Our ecosystem not only consists of environmental applications, but also agriculture, smart city, healthcare, transport, energy and many others. From a global technological ecosystem, we need to have a holistic view of the entire ecosystem to understand and solve the emerging issues. In other words, we need to have an integrated view of the SoS. Figure 5 provides a common operating picture (COP) of a system of systems using cloud-centric AI analytics.

AI algorithms are used to provide application-specific analytics to end users. These are generally provided as a service to end users. The SoS concept goes beyond traditional analytics to provide a complete understanding of the issues to governments, policymakers and decision managers. In this respect, systems are to be integrated in a seamless manner and solve technological issues within and outside the realm of specific solutions.

4.4. Open research challenges

- An estimated 8.4 billion IoT devices are used in 2017 for numerous applications [39]. The challenge lies in SoS integration with AI to process, analyze and generate actionable knowledge. For data originating from billions of devices, it will be nearly impossible to analyze manually. This challenge is attributed to the **big data** challenge. The analysis should include the growth of multidimensional data attributes (i.e. volume, velocity, variety, veracity, variability, and value) to produce actionable knowledge using AI algorithms.

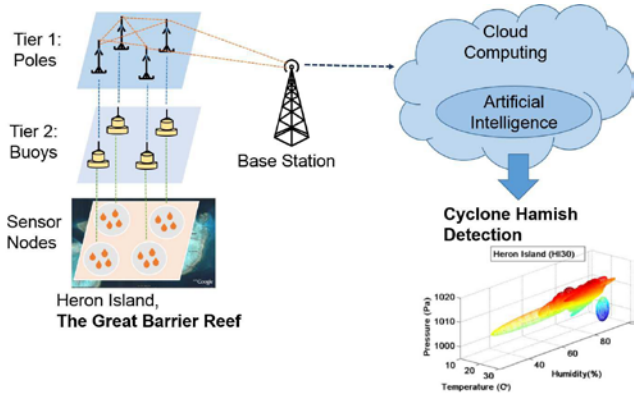

Fig. 4. WSN/IoT system architecture used to monitor Heron Island. The data is collected using a two-tiered (tree) hierarchical network architecture. The data is then transmitted to a central base station, which then transmits it to a mainland server. The cloud server consists of AI analytics that can monitor streaming real-time data and detect events

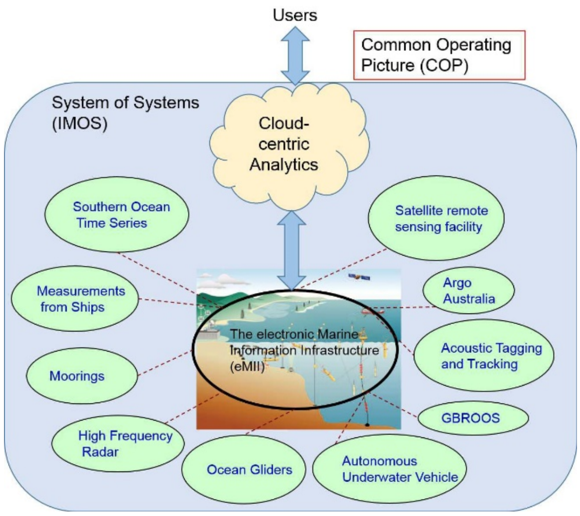

Fig. 5. The illustration depicts the idea of achieving a common operating picture (COP) using system of systems approach. The eMarine Information Infrastructure (eMII) provides a single integrative framework for data and information management that will allow discovery and access of the data by scientists, managers and the public. The data from real-world are then fed to AI-based cloud-centric analytics. The output from the analytics is used to make decisions as well as to provide feedback to the existing systems

- Clustering of data from sensors and IoT devices is an unsupervised task to extract hidden patterns without a priori information. However, with the big data challenges (pointed above), the clustering algorithms need to be **scalable** (algorithms could be used on large volumes of data), **self-tuning** (the AI algorithms should work without any input parameters from end users), **immune to outliers** (eliminate outliers, missing data points, and error points from the sensed data), and **adaptive** (the AI models must adapt the models to newly arrived data points without retraining using all data points).
- The AI algorithms must provide a holistic knowledge of SoS in **real-time**. This requires AI algorithms to be aware of not only the current system where the algorithm resides, but also about dependent and interconnected systems. Currently, most of the AI algorithms are designed to be performed for a specific system, ignoring the implications of data flow and connectedness of dependent systems.
- One of the important challenges in today's IoT/WSN paradigm is the **data security** issue. The algorithms, services and infrastructure face tremendous challenge in maintaining security,

authenticity, trust, privacy and transparency of the data. This also becomes further complicated when citizen-centric data is allowed (such as, the Open Data initiatives from governments) and through crowdsourcing. New methods, such as, block-chain is a possible future solution.

CONCLUSION

The Great Barrier Reef (GBR) of Australia is the largest living structure (coral reef) on the planet and stretches over 2300 kilometers. Anthropogenic stresses on coral reefs are causing coral bleaching. The burning of fossil fuels releases carbon dioxide which in turn is absorbed by the oceans, reducing the efforts of the reef-building mechanism by corals. Therefore, it is necessary to monitor and manage our marine environment as well as to prevent ecosystem collapse. In this article, we presented an overview and a use case of the WSNs/IoT to monitor the complex marine environments, including the GBR. The article presented an architecture used to monitor the GBR as well as the role of AI algorithms to detect events. With a suite of AI algorithms, we were able to detect Cyclone Hamish (which occurred in 2009) patterns using temperature, pressure and humidity sensors using two-tiered IoT/WSN network architecture. The article highlights the role of AI algorithms that could be used to monitor, manage and understand complex marine ecosystems.

ACKNOWLEDGEMENT

Authors acknowledge the support from ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) and SensorMap - Microsoft Research RFP Project grant, the Queensland State Government via the Department of Science, Information Technology and Innovation, the National Collaborative Research Infrastructure Strategy (NCRIS) and the Wireless Sensor Network Facility (FAIMMS) of the Integrated Marine Observing System (IMOS). The project is a collaborative effort between The University of Melbourne (ISSNIP research group) and Australian Institute of Marine Science (AIMS).

REFERENCES

[1] Miles MJ Furnas et al., Catchments and corals: terrestrial runoff to the Great Barrier Reef, Australian Institute of Marine Science & CRC Reef Research Centre, 2003.

[2] Robert C Ferrier and Alan Jenkins, Handbook of catchment management, John Wiley & Sons, 2009.

[3] Marc Lallanilla and Staff Writer, “What are coral reefs?,” https://www.livescience.com/ 40276-coral-reefs.html, October 2013.

[4] National Ocean Service, National Oceanic and Atmospheric Administration, “What is coral bleaching?,” https://oceanservice.noaa.gov/facts/ coral_bleach.html, July 2017.

[5] Ray Berkelmans, Glenn Death, Stuart Kininmonth, and William J Skirving, “A comparison of the 1998 and 2002 coral bleaching events on the great barrier reef: spatial correlation, patterns, and predictions,” Coral reefs, vol. 23, no. 1, pp. 74–83, 2004.

[6] Alfred Goldsborough Mayor, The effects of temperature upon tropical marine animals, Carnegie Institution of Washington, 1914.

[7] Charles Maurice Yonge, A Gr Nicholls, and Martha Jane Yonge, Studies on the physiology of corals, vol. 1, British Museum, 1931.

[8] Ove Hoegh-Guldberg, “Climate change, coral bleaching and the future of the world’s coral reefs,” Marine and freshwater research, vol. 50, no. 8, pp. 839–866, 1999.

[9] Scott Wooldridge and Terry Done, “The use of bayesian belief networks to aid in the understanding and management of large-scale coral bleaching,” MODSIM. Modsim, Townsville, pp. 614–620, 2003.

[10] Stuart Kininmonth, Scott Bainbridge, Ian Atkinson, Eric Gill, Laure Barral, and Romain Vidaud, “Sensor networking the great barrier reef,” Spatial Sciences Qld Journal, pp. 34–38, 2004.

[11] Ron Johnstone, Davide Caputo, Umberto Cella, Alessandro Gandelli, Cesare Alippi, Francesco Grimaccia, N Haritos, and Riccardo E Zich, “Smart environmental measurement & analysis technologies (se-mat): Wireless sensor networks in the marine environment,” Stockholm, Sweden, June 2008.

[12] Jiong Jin, Jayavardhana Gubbi, Slaven Marusic, and Marimuthu Palaniswami, “An information framework for creating a smart city through internet of things,” IEEE Internet of Things Journal, vol. 1, no. 2, pp. 112– 121, 2014.

[13] Stuart Kininmonth, “Considerations in establishing environmental sensor networks,” in 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE, 2007, pp. 687–691.

[14] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[15] James C Bezdek, Sutharshan Rajasegarar, Masud Moshtaghi, Chris Leckie, Marimuthu Palaniswami, and Timothy C Havens, “Anomaly detection in environmental monitoring networks [application notes],” IEEE Computational Intelligence Magazine, vol. 6, no. 2, pp. 52–58, 2011.

[16] Australian Government, Great Barrier Reef Marine Park Authority, “Facts about the great barrier reef,” http: //www.gbrmpa.gov.au/about-the-reef/ facts-about-the-great-barrier-reef, 2017.

[17] Australian Institute of Marine Science (AIMS), “GBROOS Data - Observing the Great Barrier Reef,” http://data.aims.gov.au/gbroos/, 2017.

[18] Aravinda S Rao, Stephen Marshall, Jayavardhana Gubbi, Marimuthu Palaniswami, Richard Sinnott, and Vincent Pettigrovet, “Design of low-cost autonomous water quality monitoring system,” in 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2013, pp. 14–19.

[19] Philip W Rundel, Eric A Graham, Michael F Allen, Jason C Fisher, and Thomas C Harmon, “Environmental sensor networks in ecological research,” New Phytologist, vol. 182, no. 3, pp. 589–607, 2009.Integrated Marine Observing System (IMOS), “Wireless Sensor Networks,” http://imos.org.au/ facilities/wirelesssensornetworks/, 2017.

[20] Sutharshan Rajasegarar, Jayavardhana Gubbi, Olga Bondarenko, Stuart Kininmonth, Slaven Marusic, Scott Bainbridge, Ian Atkinson, and Marimuthu Palaniswami, “Sensor network implementation challenges in the great barrier reef marine environment,” in Conference Proceedings of the ICT-MobileSummit. International Information Management Corporation (IIMC) Ltd, 2008, pp. 1–9.

[21] MEMSIC, Inc, “Wireless sensor networks,”http://www.memsic.com/ wireless-sensor-networks/, 2017, [Online].

[22] Libelium, “Waspmote,” http://www.libelium. com/products/waspmote/, 2017, [Online].

[23] Olga Bondarenko, Stuart Kininmonth, and Michael Kingsford, “Underwater sensor networks, oceanography and plankton assemblages,” in 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE, 2007, pp. 657–662.

[24] Chenyang Lu, Brian M Blum, Tarek F Abdelzaher, John A Stankovic, and Tian He, “Rap: A real-time communication architecture for large-scale wireless sensor networks,” in Eighth IEEE Real-Time and Embedded Technology and Applications Symposium. IEEE, 2002, pp. 55–66.

[25] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A survey on sensor networks,” IEEE Communications magazine, vol. 40, no. 8, pp. 102–114, 2002.

[26] Cameron Huddlestone-Holmes, Gilles Gigan, Graham Woods, Adam Ruxton, Ian Atkinson, and Stuart Kininmonth, "Infrastructure for a sensor network on davies reef, great barrier reef," in 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE, 2007, pp. 675–679.

[27] Omprakash Gnawali, Ki-Young Jang, Jeongyeup Paek, Marcos Vieira, Ramesh Govindan, Ben Greenstein, August Joki, Deborah Estrin, and Eddie Kohler, "The tenet architecture for tiered sensor networks," in Proceedings of the 4th international conference on Embedded networked sensor systems. ACM, 2006, pp. 153–166.

[28] Peter Desnoyers, Deepak Ganesan, and Prashant Shenoy, "Tsar: a two tier sensor storage architecture using interval skip graphs," in Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005, pp. 39–50.

[29] Purushottam Kulkarni, Deepak Ganesan, Prashant Shenoy, and Qifeng Lu, "Senseye: a multi-tier camera sensor network," in Proceedings of the 13th annual ACM international conference on Multimedia. ACM, 2005, pp. 229–238.

[30] Junsuk Shin, Rajnish Kumar, Dushmanta Mohapatra, Umakishore Ramachandran, and Mostafa Ammar, "Asap: A camera sensor network for situation awareness," Principles of Distributed Systems, pp. 31–47, 2007.

[31] Phoebus Chen, Parvez Ahammad, Colby Boyer, ShihI Huang, Leon Lin, Edgar Lobaton, Marci Meingast, Songhwai Oh, Simon Wang, Posu Yan, et al., "Citric: A low-bandwidth wireless camera network platform," in Distributed smart cameras, 2008. ICDSC 2008. Second ACM/IEEE international conference on. IEEE, 2008, pp. 1–10.

[32] Chris Townsend and Steven Arms, "Wireless sensor networks: Principles and applications," in Sensor Technology Handbook, Jon S. Wilson, Ed., chapter 22, pp. 575–589. Newnes, 2005.

[33] Jesu´s Pe´rez, Victor Za´rate, and Christian Cabrera, "A network and data link layer qos model to improve traffic performance," Emerging Directions in Embedded and Ubiquitous Computing, pp. 224–233, 2006.

[34] Scott Bainbridge, Damien Eggeling, and Geoff Page, "Lessons from the fieldtwo years of deploying operational wireless sensor networks on the great barrier reef," Sensors, vol. 11, no. 7, pp. 6842–6855, 2011.

[35] Sutharshan Rajasegarar, James C Bezdek, Christopher Leckie, and Marimuthu Palaniswami, "Elliptical anomalies in wireless sensor networks," ACM Transactions on Sensor Networks (TOSN), vol. 6, no. 1, pp. 7, 2009.

[36] Masud Moshtaghi, Sutharshan Rajasegarar, Christopher Leckie, and Shanika Karunasekera, "Anomaly detection by clustering ellipsoids in wireless sensor networks," in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on. IEEE, 2009, pp. 331–336.

[37] Timothy C Havens and James C Bezdek, "An efficient formulation of the improved visual assessment of cluster tendency (ivat) algorithm," IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 5, pp. 813–822, 2012.

[38] Gartner, Inc, "Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 per- cent from 2016," http://www.gartner.com/newsroom/id/3598917, 2017, [Online].