# Building Resilience for SDN-enabled IoT Networks in Offshore Renewable Energy Supply

Agrippina Mwangi
*Sustainable Development*
*Utrecht University*
Utrecht, Netherlands
a.w.mwangi@uu.nl

Elena Fumagalli
*Sustainable Development*
*Utrecht University*
Utrecht, Netherlands
e.m.fumagalli@uu.nl

Mikkel Gryning
*Wind SCADA Control*
*Ørsted*
Gentofte, Denmark
migry@orsted.com

Madeleine Gibescu
*Sustainable Development*
*Utrecht University*
Utrecht, Netherlands
m.gibescu@uu.nl

***Abstract*—Resilient software-defined Internet of Things (SD-IoT) networks are critical in offshore renewable energy supply (such as offshore wind farms) for wide-area monitoring, protection, automation, and control (WAMPAC). Offshore wind farms transmit time-sensitive data about the turbine performance, power generation, environmental conditions, and critical equipment status to the wind farm offshore landing point or the remote control room. As such, there is a need to guarantee real-time communication to coordinate protection and control actions that maximize production and minimize inadvertent wind farm downtime. This research designs a deep Q-Network (DQN) resilience model that quickly detects disruptions and applies optimal traffic engineering actions at the software-defined network (SDN) controller to guarantee high performance. This resilience model improves the quality of service of the SDN-enabled IoT networks in offshore wind farm communication networks.**

***Index Terms*—Internet of Things, software-defined networking, resilience, offshore wind farms, performance, QoS**

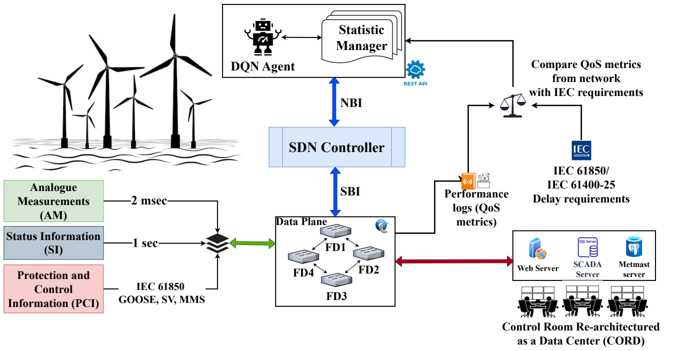

Fig. 1. A co-simulation testbed to evaluate the performance of a software-defined IoT network for an offshore wind farm (analog measurements, status, and protection and control data samples).

## I. Problem Statement and Related Works

The Internet of Things (IoT) is gradually being adopted in offshore renewable energy supply such as offshore wind farms. Considering the adverse weather conditions at sea and limited access to operations and maintenance, IoT devices and digitalized data acquisition devices such as non-conventional instrument transformers are being deployed in most offshore wind farms for wide-area monitoring, protection, automation, and control. These IoT devices acquire highly granular data at high sampling rates [1].

For offshore wind farms, status information (SI), analog measurements (AM), and protection and control information (PCI) are transmitted as illustrated in Figure 1. SI and AM data are exchanged between the wind turbines and the in situ central control room to determine the wind turbine performance, power generation, environmental condition, and critical equipment status.

Further, PCI is exchanged between wind turbines within the wind farm to quickly detect faults and abnormalities in the wind farm in order to have coordinated protection and fault mitigation [2]. Because these data points are critical to the operation and management of offshore wind farms, it is imperative that they are exchanged within the specified IEC 61850 (and 61400-25 TC-88) data delivery requirements.

Like other communication networks, offshore wind farm IoT networks encounter stochastic disruptions caused by equipment failure [2], transient communication network traffic loads [3], and cyber threats [4]. These disruptions have catastrophic effects on the underlying wind farm operations. For instance, (i) packet drops during network congestion or network equipment failure cause data unavailability, (ii) unauthorized access of data either in transit or at the storage locations affects data confidentiality, and (iii) data manipulation by intruders corrupts the data leading to a loss in data integrity.

Modern communication network designs are leveraging software-defined networking (SDN) for dynamic network management to address the highlighted performance concerns. Mhdawi et al. [5] developed a micro cloud-software defined network testbed for onshore wind farm network recovery which provides an immediate fail-over recovery system for faulty sensors to provide continuous sensor reading with no interruptions. Further, Muna et al., [6] designed an SDN-based routing framework to distinguish between two transient network loads namely elephant flows and mice flows using unsupervised machine learning. Dorsch et al. [7] designed a software-defined communication network that orchestrates traffic flows by applying fine-grained prioritization to the SDN controller for multi-agent system-based smart grid power

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 956433.

control. Dake et al. [3] uses multi-agent reinforcement learning to detect and prevent transient network loads that result from malicious bots. While these studies have made significant advancements in the design of software-defined IoT networks, there remains a paucity of resilience model frameworks that:

- Proactively flag the stochastic disruptions that affect the current communication networks
- Apply the most optimal traffic engineering action to improve network performance
- Learn from their immediate past experiences for advanced network optimization and management

## II. Proposed Methodology

A co-simulation testbed (see Figure 1) is developed to represent the wind farm IoT network.

- At the data plane, the wind turbine data acquisition module (for AM, PCI, and SI data samples) and an array of fiber optic cables are designed on the Mininet emulator (running on a virtual machine). The data sample values are generically scripted into the virtual hosts on the Mininet network topology and transmitted at the IEC 61850 sampling rate of 80 samples/cycle.
- At the control plane, the OpenDayLight SDN controller (running on a separate virtual machine) is configured to communicate remotely via an IP address and OpenFlow protocol to the Mininet network topology.
- At the application plane, a Deep Q-Network (DQN) agent reads the network Quality of Service (QoS) metrics from the statistics manager in the SDN controller as log files. These performance logs are based on the standard QoS metrics namely latency, jitter, round trip time (RTT), and packet loss rate.

A performance variable ($P_{network}$) is defined that sums the product of the QoS metric weighted values and the QoS metrics values from the time-stamped performance logs. This performance variable is compared to the threshold performance variable ($P_{threshold}$) defined by IEC 61850 and IEC 61400-25.

Based on the outcome of the two, the network can be in these states:

- Normal state ($P_{network} \geq P_{threshold}$)
- Degraded state ($P_{network} \leq P_{threshold}$)

When the network is in a degraded state, the DQN agent is triggered to determine the optimal state-action pair that updates flows (instructions) in the SDN controller to quickly restore the network to its normal operating state. The DQN agent has a neural network that approximates the Q-values to attain the maximum expected cumulative reward.

## III. Results and Discussion

Having set up the co-simulation testbed, stochastic disruptions were launched by administratively turning links up/down and sending large data samples randomly. To test the efficiency of the DQN agent to re-route traffic and reallocate resources to ensure high performance, several quantitative assessment tools were used:

- Learning curves were used to monitor how best the DQN agent learned to make better decisions based on the data from the statistics manager,
- The DQN agent seeks to maximize the cumulative reward, hence, a cumulative reward plot for the training episodes is used for quantitative evaluation. Further, it converges to show when the Q-values stabilize upon learning an optimal policy to dynamically re-route the traffic,
- The impact of the policy update was measured by comparing the metrics before and after the policy update,
- Lastly, the DQN agent's performance is compared against a baseline, in this case, the Dijkstra algorithm for finding the shortest path (used in traditional networking protocols).

The results of this empirical evidence illustrate the proficiency of the DQN agent in automating the network self-healing process making the offshore wind farm communication network resilient by minimizing the overall latency.

## IV. Conclusion

The proposed resilience model morphs traditional networks into self-healing networks that proactively respond to stochastic disruptions such as equipment failure and cyber threats by rerouting traffic and reallocating resources to ensure continued network uptime. These self-healing networks identify and isolate the disruption or bottleneck in the network based on a quantitative assessment of the QoS metrics using the DQN agent. The DQN agent uses the assessment to proactively add flows to redirect traffic or reallocate resources through the SDN controller ensuring optimal performance. These self-healing networks are set to transform IoT networking in offshore wind farms and other cyber-physical energy system applications that depend heavily on timely data exchange such as electric-vehicle charging networks and virtual power plants.

## References

[1] P. Vizarreta, A. V. Bemten, E. Sakic, K. Abbasi, N. E. Petroulakis, W. Kellerer, and C. M. Machuca, "Incentives for a softwarization of wind park communication networks," *IEEE Communications Magazine*, vol. 57, no. 5, pp. 138–144, 2019.

[2] A. Mwangi, K. Sundsgaard, J. A. Leiva Vilaplana, K. V. Vilerá, and G. Yang, "A system-based framework for optimal sensor placement in smart grids," in *2023 IEEE Belgrade PowerTech*, pp. 1–6, 2023.

[3] D. K. Dake, J. D. Gadze, G. S. Klogo, and H. Nunoo-Mensah, "Multi-agent reinforcement learning framework in sdn-iot for transient load detection and prevention," *Technologies*, vol. 9, no. 3, p. 44, 2021.

[4] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Transactions on Smart Grid*, 2023.

[5] A. K. Al Mhdawi and H. Al-Raweshidy, "$\mu$C-sdn: Micro cloud-software defined network testbed for onshore wind farm network recovery," in *2018 IEEE Global Conference on Internet of Things (GCIoT)*, pp. 1–6, 2018.

[6] M. Al-Saadi, A. Khan, V. Kelefouras, D. J. Walker, and B. Al-Saadi, "Sdn-based routing framework for elephant and mice flows using unsupervised machine learning," *Network*, vol. 3, no. 1, pp. 218–238, 2023.

[7] N. Dorsch, F. Kurtz, S. Dalhues, L. Robitzky, U. Häger, and C. Wietfeld, "Intertwined: Software-defined communication networks for multi-agent system-based smart grid control," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 254–259, 2016.