9

9-1

**Title：**

Deep Learning for IoT Streaming Data Processing in Edge

**Supervisors:**

Elvis Liu (SUSTech) and Dr Gengfa Fang (UTS)

**Abstract:**

In recent years, deep learning has become an important methodology in many informatics fields such as vision recognition, natural language processing and bioinformatics. Deep learning has been introduced into many tasks related to IoT and mobile applications with encouraging early results. For example, deep learning can precisely predict the home electricity power consumption with the data collected by smart meters, which can improve the electricity supply of the smart grid. Edge computing is another important technology for IoT services. Due to data transferring with limited network performance, the centralized cloud computing structure is becoming inefficient for processing and analyzing huge amounts of data collected from IoT devices.

One open problem is how to reliably mine real-world IoT data from a noisy and complex environment where deep learning is considered as the most promising approach. Multilayer structured deep learning is very appropriate for the edge-to-cloud computing environment where edge computing part can offload parts of learning layers in the edge and then transfer the reduced intermediate data to the centralized cloud server for further processing.

In this project, we study the deep learning for IoT into the edge computing environment to improve learning performance as well as to reduce network traffic. A deep learning network usually has multiple layers. The input data will be processed in these layers. Each layer processes the intermediate features generated by the previous layer and then generates new features. The extracted features generated by the last deep learning network layer will be processed by a classifier and recognized as the output. In deep learning networks, we consider the layers near input data to be lower layers; others are higher layers.

we will study the edge computing structure for IoT deep learning tasks, and deploy the part with lower layers into edge servers and the part with higher layers into the cloud for offloading processing. The challenge is how to divide each deep learning network. Since the size of the intermediate data generated by the higher layers is smaller than that generated by the lower layers, deploying more layers into edge servers can reduce more network traffic. However, the computing capacity of edge devices is limited compared to cloud servers. We can only deploy part of the deep learning network into edge servers. As different deep learning networks and tasks have different sizes of intermediate data and computational overhead, and the network connectivity between edge and cloud is dynamic as well, we will also study efficient scheduling schemes which are needed to optimize deep learning for IoT in the edge computing structure dynamically and on-demand.

In this project, we will also study the vertical applications such as the smart grid and distributed energy resources(DER) by designing and developing the deep learning algorithms and training schemes to solve the real and big problems in energy and utilities together with our industry partners such as Cisco, SAS and government sectors as part of UTS-SAS-Cisco IoT Innovation Lab at UTS.

9-2

**Title：**

Modeling of vulnerability levels of an electric power network equipped with PMUs to cyber-attacks

**Supervisors:**

Elvis Liu (SUSTech) and Haiyan (Helen) Lu (UTS)

**Abstract:**

Electric power networks play crucial roles in every economy around the globe. The increasing complexity of modern electric power networks with phase measurement units (PMUs) pose significant challenges to power system safety and availability. A cause of particular great concern among governments, organisations and businesses is the increasing sophistication and evolving nature of cyber-attacks to power networks. This project will address the research problem of “how to accurately model the level of vulnerability of an electric power network equipped with PMUs to cyber-attack?” This project will take a simulation approach to investigate the vulnerability of an electric power network coupled with physical sensor network of PMUs and develop a classifier using machine learning, especially deep learning techniques to estimate the vulnerability level of a given electric power network. The expected outcomes are a working prototype of simulation model and a suite of features to model vulnerability levels regarding cyber-attacks.

9-3

**Title：**

Autonomic computing model for enhancing resilience of an electric power network to cyber-attacks

**Supervisors:**

Elvis Liu (SUSTech) and Haiyan (Helen) Lu (UTS)

**Abstract:**

Electric power networks play crucial roles in every economy around the globe. The increasing complexity of modern electric power networks with phase measurement units (PMUs) poses significant challenges to power system safety and availability. A cause of particular great concern among governments, organisations and businesses is the increasing sophistication and evolving nature of cyber-attacks to power networks. This project will address the research problem of “how to make an electric power network equipped with PMUs be resilient to cyber-attacks?” This project will take a simulation approach based on the concept of info-symbiotic system to develop an autonomic computing model which will allow an electric power network to achieve self-diagnose and self-protection to enhance the resilience of electric power networks against cyber-attacks. The expected outcomes are a prototype system that implements the autonomic computing model for a regional electric power network.