Dr. Deepthi N. Ratnayake FHEA, MBCS, CITP, MCS(SL), SLAF (Rtd.)
Senior Lecturer in Computer Science (Cyber Security & Networks)
School of Physics, Engineering and Computer Science (SPECS)
Email: d.ratnayake@herts.ac.uk
https://www.linkedin.com/in/deepthiratnayake/

Intelligent Intruder Detection Systems

I would like to invite PhD research students who are interested in developing multidisciplinary skills that are highly demanding of today's research, corporate/business world, and exploring into following areas to further develop the research to the next levels of novel methods and strategies.

1. Network-based Intruder Detection Systems (NIDS).
2. Host Based Intruder Detection Systems (HIDS).
3. Application of Big Data Analytics Technologies for Intruder Detection.
4. Cyber-Physical-system (CPS) based intrusion detection systems (includes robots and unmanned/self-driving vehicles).

The research may require a combination of knowledge and skills of Operating Systems, Wireless/Wired/Cloud based networks, IOT and their security landscape depending on the topic you are investigating. Applicants are required to have a strong first degree or Master's degree in Computer Science, or an area relevant to the project. Skills in scripting, programming, AI and/or Data Science and a simulator such as MATLAB is desirable or should be keen to learn. The ideal candidate will be self-motivated with good writing and communication skills. School of Physics, Engineering and Computer Science (SPECS) is equipped with state-of-the-art laboratories and research profile to support above collaborative multidisciplinary research. PhD student will be supervised by Dr. Deepthi Ratnayake (d.ratnayake@herts.ac.uk), whom interested candidates are invited to contact via email in the first instance.

The current ongoing research of Dr. Deepthi Ratnayake is as follows;

1. Wireless Intruder Detection System (WIDS) for SOHO WLANs

Probing is the first communication that an active intruder performs on an Access Point (AP). Early detection of unauthorised probing is crucial, as probing attacks can be the basis of other attacks in a Small Office/Home office (SOHO) Network. In Ratnayake et al. (2014) a prototype of an anomaly based WIDS is designed, employing a supervised feedforward Neural Network (NN) classifier that classifies genuine frames from rogue frames, to detect a probe request attacks in

SOHO WLANs. The overall simulation results showed that the probe request attack classifier performs 96.5% accurately, when it is applied to real-world WLAN data. WPA3 protocol (2018) comes with four major features: a new, more secure handshake for establishing connections, an easy method to securely add new devices to a network, some basic protection when using open hotspots, and finally increased key sizes. However, probing vulnerabilities still remain the same.

Depending on your interest, abilities and experience, the project may be orientated more, either towards development of an IDPS (one option would be developing the existing IDPS to a self-contained, self-learning IDPS), or improving the security architecture of the WLAN.

2. **Application of Big Data Analytics Technologies for Intruder Detection in NOCs**

   Network Operation Centres (NOC) collect a vast amount of network traffic on a continuous manner; however, they are usually being used for individual threat detection applications. The Cyber Security Centre has been collecting data of its REDNET (student's pen testing rig) since 2013. This research aims to explore Application of Big Data Analytics Technologies for Intruder Detection.

3. **Integrated intelligent threat detection and prevention system for Pepper Social Robot (collaborated research with the Adaptive Systems Research Group).**

   a. This research aims to develop an integrated host-based intelligent threat detection and prevention system for NAOqi operating system.

   b. This research aims to develop an integrated intelligent threat detection and prevention system for a Robotics Apartment environment.

4. **Cyber-Physical system (CPS) based intrusion detection system and prevention system for self-driving vehicles**

   This research aims to develop an integrated intelligent threat detection and prevention system for self-driving cars.

These projects are also ideal for students who are experienced in Networks and Operating systems or AI and Data Science research and keen to apply their skills in developing solutions for Cyber Security problems.