UMONS activities

CyberExcellence-CyberWal

Funded by RW under contract n°2110186

Outline

Electromagnetism and Telecommunication Lab

TELE lab is mainly involved in PHY and DL layers

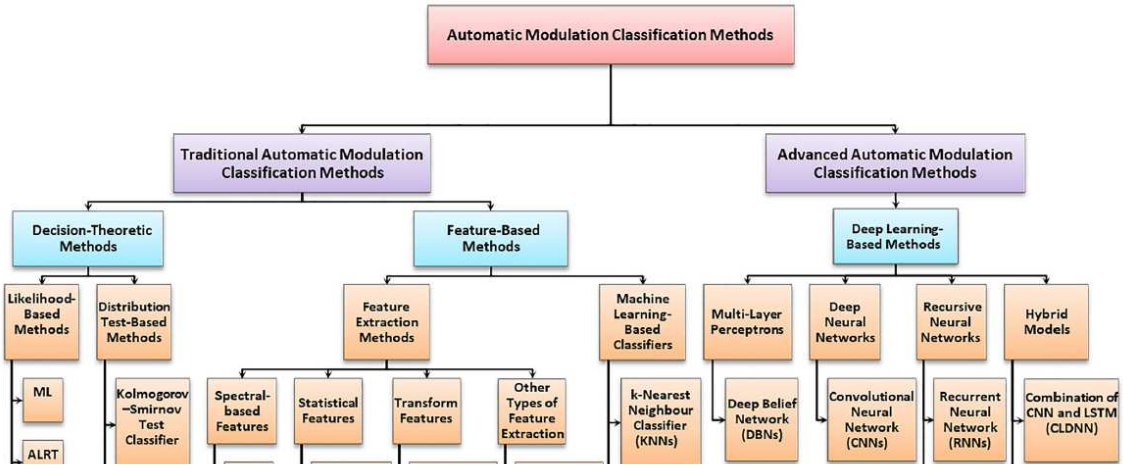
- **TELE lab**
  - Electrical Dept., Faculty of Engineering
  - Head of lab: Prof. Patrice MÉGRET
  - 11 PhD students, 10 senior scientists, 4 academic, 2.5 technicians
- **Main research interests**
  - Optical fiber communications and sensing
  - Powerline communications (G3-PLC)
  - Multimedia networks
  - Sensor design and network
  - Internet of Things technologies
- **Methodology**
  - Simulation of communication systems
  - Performance monitoring of communication systems
  - Optical fiber metrology and fabrication of some optical components

Projects tackle different telecommunication technologies

- **Fab-IoT-Lab**
  - Support for creative hubs in university cities and towns with more than 50,000 inhabitants
  - 3 people with prototyping facilities
- **M&SSCoT**
  - Matrix & Single Switch Converter Technology Network: use of telecommunication systems to control power electronics
  - Alstom, Thales Alenia Space, Deltatec, Alpha Innovations, CETIC, ULiege
- **SWITCH**
  - Smart wireless intelligent tunnel connectivity hub
  - UNamur, UCLouvain, SEE, Icoms Detections SA, EURA NOVA SA
- **Wal-E-Cities**
  - Development of LiFi communications
  - Multitel

Automatic modulation recognition has many potential for identification and monitoring

- Alexander GROS
  - Automatic Modulation Recognition in the context of RF spectrum monitoring and cognitive radios



  - Many possibilities, here Empirical Mode Decomposition (EMD) is used.
  - EMD does not need an a priori defined basis
  - Extension to detection intrusion from performance monitoring

Computer Networking Lab

Networking lab is mainly involved in network and transport layers

- **Computer Networking Lab**
  - Computer Science Dept., Faculty of Science
  - Head of lab: Prof. Bruno QUOITIN
  - 4 PhD students, 1 senior scientist, 2 academic
- **Main research interests**
  - Low-Power and Lossy Networks (LLN) (many interconnected embedded devices with limited power, memory, and processing resources for industrial monitoring, building automation, ...)
  - Indoor Positioning Systems (IPS)
  - Internet of Things technologies and protocols
  - Energy-efficient data-link and routing protocols
- **Methodology**
  - Design of protocols, simulation/testbed evaluation
  - LLN and IPS testbed of approximately 40 nodes
  - Technologies: Internet Protocol (IP), IEEE 802.15.4, LoRa(WAN), RPL, 6LoWPAN/6TiSCH, CoAP, ...

Ongoing research projects tackle network efficiency

- **Centimeter-level Indoor Positioning System**
  - Relies on IEEE 802.15.4 UltraWide Band (UWB) PHY
  - Focus on networking architecture
  - Channel access : time, frequency and code multiplexing
  - Scheduling of communications, with frequency re-use
  - Objective: maximize positioning rate
- **Monitoring of herds in pasture**
  - Partners: Gembloux Agro-Bio-Tech, Polytech UMONS
  - Autonomous gantry deployed in pasture: sense multiple health parameters (T°C, watering frequency, body condition score, weight)
  - Report measurements on cloud portal
  - Evaluate different long-range radio technologies (LoRaWAN, SigFox, NB-IoT/LTE-M, 3G/4G, ...)

Some theses are dedicated to IoT

- Ali HAJ-HASSAN (joint PhD with UPHF, Valenciennes)
  - Industrial IoT : reliable, deterministic communications
  - IPv6 over IEEE 802.15.4 TSCH (IETF 6TiSCH)
  - Security currently relies on pre-shared keys (PSK)
  - Design of **zero-touch** authentication mechanisms
- Phithak THAENKAEW (joint PhD with IMT Nord Europe, Lille)
  - Enhance IoT security through cross-layer mechanisms
  - Combine existing security protocols with use of *Physical Unclonable Functions* (PUF), RF fingerprinting, ...
  - Focus is on LoRaWAN, but likely applicable to other technologies

AI lab has cross-layer activities

- **Artificial Intelligence Lab**
  - Computer Science Dept., Faculty of Science
  - Head of lab: Prof. Stéphane DUPONT
  - 2 PhD students, 1 academic
- **Main research interests**
  - Long experience in multimodal deep learning and robustness
  - Deep learning for audio, language and sequences, and Bayesian models
- **PhD theses**
  - Ahmad HAMMOUDEH: geometric and non-geometric deep learning robustness
  - Bastien VANDERPLAETSE: multi-agent coordination using language

AI has many potential

- Deep learning to improve computer networks security. Deep learning captures security threats better than traditional methods when trained with appropriate data
- Newly developed versions of Graph neural networks, have shown superiority in Intrusion Detection IDS and handling DDoS attacks
- Deep learning could be a potential security threat given that deep neural networks are fooled by slight alterations in the input signals (Adversarial attacks). This may lead to false classification of IDS and delayed response. Adversarial attacks on IDS based on Deep Learning should be studied.
- Neural architectures with more robustness to adversarial as well as other forms of disturbances will be developed and utilized in computer networks and their security. Deep learning architectures (RotConV and REB) were developed and shown increased resilience against noise.
- Mutli-agent systems are becoming more popular due to successful results on different complex tasks. **But several security issues:** identification, authentication, detection of fake message, etc.

BDML lab has cross-layer activities

- **Big Data and Machine Learning Lab**
  - Computer Science Dept., Faculty of Science
  - Head of lab: Prof. Souhaib BEN TAIEB
  - 2 PhD students, 1 academic
- **Main research interests**
  - Machine learning / Artificial intelligence
  - Analysis of sequential data (time series, event sequences)
  - Uncertainty quantification and predictive modeling with deep neural networks
  - Anomaly detection in large-scale online sequential data
- **PhD theses**
  - 3 ongoing PhD thses

Big data and machine learning techniques are useful for cybersecurity research

- Victor DHEUR
  - Uncertainty quantification in AI models
  - AI models will impact decision making for high-consequence cybersecurity applications
  - AI models can provide highly confident but incorrect predictions.
  - Essential to improve the reliability of AI models through appropriate uncertainty quantification methods
- Tanguy BOSSER
  - AI models for event analysis and prediction
  - Many cybersecurity applications often involve processing a large stream of event data in order to detect attacks or predict critical events
  - AI sequence models have been shown to be effective in modeling heterogenous sequences of events.
  - Such models allow to predict the time and type of future events from historical observations

Big data and machine learning techniques are useful for cybersecurity research

- Sukanya PATRA
  - Federated learning for anomaly detection
  - The identification of rare events or suspicious activities from data is an important problem in many cybersecurity applications.
  - Flexible unsupervised or semi-supervised AI models are essential when it is hard to label anomalous data
  - Federated learning allows to train a global AI model from multiple data sources while preserving data confidentiality

Contributions to CyberExcellence

Four labs contribute to CyberExcellence

- 1 lab on PHY and DL layer, 1 lab on Network and Transport layer, and 2 labs on AI, ML, big data tools
- 3 PhD students and 1 post-doc would be specifically engaged
- Participation to WP1, WP2, WP4 and WP6
- Verification of IoT security protocols using e.g., Cryptographic protocol verifier (Proverif)
- Monitor behavior of IoT networks through analysis of network traffic and radio signal
- Intrusion detection in IoT and industrial networks by coupling performance monitoring and AI
- Go beyond pre-shared key (PSK) while remaining compatible with low-resource/low-power embedded systems, e.g. make use of Elliptic Curve Cryptography
- Security of powerline communications (G3-PLC)
- Member of INFORTECH Institute (14 dept., around 120 staff): Data transfer, Big data and Cloud computing, IA, ML, deep learning, algorithms and software, signal processing