



Biennial since 1998

CSNDSP

2020

Special Session on

Emerging trends and approaches to Cyber security

Prof. Krishna Busawon, Northumbria University,
Newcastle Upon Tyne, UK

krishna.busawon@northumbria.ac.uk

<http://www.northumbria.ac.uk/sd/academic/ee/>



Professor Krishna Busawon is the Head of Control research group in the Faculty of Engineering and Environment. His research interests are in the areas of mathematical modelling, nonlinear control and observer design, fault detection and isolation with applications to various engineering fields such as communication, electrical power and mechanical systems. He has published more than 180 papers in his area of research. Additionally, he has co-authored two books on the “control of under-actuated systems” and “Robotic Manipulators and Vehicles Control, Estimation and Filtering”. He is a Senior Member of the IEEE and the Chair of the IEEE Control Systems Chapter for UK and Ireland. He is also a Fellow of the IET.

Dr. Rupak Kharel, Manchester Metropolitan University,
Manchester, UK

r.kharel@mmu.ac.uk

<https://www2.mmu.ac.uk/computing-and-maths/staff/profile/index.php?id=2352>



Dr Rupak Kharel is a Reader (Associate Professor) in Cyber Security at the Department of Computing and Mathematics in Manchester Metropolitan University. He is also the Principal Investigator and Academic Lead of the ERDF funded £6 million Greater Manchester Cyber Foundry project. His research interest is in the area of cyber physical systems and IoT, cyber security, smart infrastructure systems and Industry 4.0. He has co-authored 50+ papers in his area of research and has attracted numerous funded projects. He is a Senior Member of the IEEE and the treasurer of the IEEE Control Systems Chapter for UK and Ireland. He is also a Fellow of the IET and Higher Education Academy (HEA).

Scope of the session

Cyber security in general has attracted massive interest from academia, government and industry in recent years, because of the advent of future internet, pervasive connection of devices and high-profile cyber-attacks. The threat landscape is ever increasing with cyber attackers being proactive every day and utilizing the latest technologies such as AI and Machine Learning together with the intrinsic vulnerabilities that exists in the current hyper-connected world and Internet of Things/Everything. This provides opportunities for the research communities to keep acquainted with the latest, ever increasing and emerging threat landscapes for a securer, safer and more resilient digital system and digital infrastructure. Moreover, the threat landscape spans multilayer in the infrastructure from physical, network and to the application layer thus making this an interdisciplinary research area.

The aim of this session is to disseminate recent research results in the broad area of cyber security and include all aspects of the modeling, design, implementation, deployment, and management of security algorithms, protocols, architectures, and system, from physical-layer technology to the application layer. With the increasing interest visible light communications and application, research results related to optics and chaos are particularly welcomed. Particular emphasis of this session is also laid on the encryption side of chaotic communication for secure communication. Ultimately, this session aims to bring about new paradigms for secure communication that is fit for purpose for future applications such as the IoT,

driverless cars, smart manufacturing, remote control and diagnosis and much more.

Prospective authors are invited to submit original and unpublished work on the following research topics plus others that are not explicitly listed but are closely related to this Special Session:

- Use case of blockchain and distributed ledger in the cyber physical world
- Physical layer security on 5G and beyond 5G technology
- Nonlinear dynamics and chaos for physical layer security
- Synchronization and control of dynamical systems
- Optics and Chaos for security
- Autonomous vehicle security
- IoT security and privacy
- Resilient IoT framework based on AI/Machine Learning
- Lightweight cryptographic algorithm
- Biometric and emerging authentication technologies
- Malware detection
- Security and privacy in fog/edge computing