MALAVIYA MISSION TEACHER TRAINING CENTRE

Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram

Network Security and Network Science: Mathematical Foundations, Practice, Research Trends

About MMTTC:

The Malaviya Mission Teacher Training Center (MMTTC) at IIITDM Kancheepuram is funded by the Ministry of Education (MoE) under the Malaviya Mission Teacher Training Programme. The mission aims to transform higher education by integrating Indian values and ethos into teaching, research, publications, patents, and institutional development. Established as one among the 116 centers in the country, the MMTTC at IIITDM Kancheepuram focuses on design and manufacturing education. It develops e-learning materials, low-cost laboratory instruction modules, and innovative projects for students and teachers.

Date: 10th July to 23rd July 2025
Mode: Online

About the programme:

This refresher course is designed to provide an interdisciplinary introduction to the fields of network science and network security, catering to faculty members, researchers, and professionals from computer science, mathematics, electronics, and related disciplines. It offers participants a mathematical foundation, practical exposure, and awareness of ongoing research trends in each of these domains. The course will be enriched with lectures, hands-on sessions, case studies, and discussions on current research trends, equipping participants with both conceptual knowledge and technical skills applicable to academia, research, and industry. The course will foster participants' interdisciplinary thinking and promote collaborative research opportunities in emerging areas of network science and security.

In the area of network security, the course focuses on the growing challenges associated with securing computer systems, networks, and cloud infrastructures. This component highlights real-world threats and defense mechanisms relevant to today's computing environments. Topics to be covered are system-level security, such as endpoint protection, malware analysis, and operating system vulnerabilities. Security issues arising from virtualization, multi-tenancy, and data privacy in cloud computing will also be covered. Network-related concerns, including intrusion detection and prevention, denial-of-service attacks, spoofing, firewalls, and traffic monitoring, will also be discussed. The Network Science component of the course introduces participants to the theoretical and practical aspects of analyzing complex networks, which are central to understanding systems in communication, social interactions, biology, and infrastructure. Participants will learn about different network models, including small-world and scale-free networks, and explore dynamic processes such as the spread of information or disease, influence propagation, and failure cascades. For practical exposure, participants will be guided through hands-on demonstrations of tools and software relevant to network security as well as network science platforms.

TOPICS TO BE COVERED:

NETWORK SECURITY:

- Elementary Mathematics for Security.
- Foundations of Cryptography.
- Introduction to Network Security-Concepts, Models, and Threat Landscape.
- Intrusion Detection and Prevention Systems (IDS/IPS).
- Virtual Private Networks (VPNs) and Secure Tunneling.
- Man-in-the-Middle, Spoofing, and Sniffing Attacks.
- Secure Coding Practices.
- Cloud Computing Security: Risks, Controls, and Best Practices.
- IoT Security: Device, Network, and Data Protection.
- AI in Security.
- Hands-on Sessions: Wireshark, NMap, OpenSSL, VPN Tunnel, IAM in Cloud, etc.
- Case Studies on Recent Cyber Attacks and Mitigation Strategies.

NETWORK SCIENCE:

- Introduction to Complex Systems and Networked Dynamical Systems.
- Spectral Graph Theory.
- Network Partition and Clustering.
- Network Robustness: Percolation Theory.
- Network visualization and analysis.
- Simulation of spreading processes on networks.
- Empirical data modeling of complex systems.
- Dynamics on multilayer and temporal networks.
- Network Controllability and Optimization.
- Machine Learning for Network Data.
- Biological and Ecological Modeling on Networks.
- Communication and Social Networks.

REGISTRATION:

1. Register and login as a participant in www.mmc.ugc.ac.in
2. In the dashboard click on "Apply for Other programmes".
3. Select Apply for "Refresher Course" and from the dropdown select the Programme Name and Center Name as "Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram (10/07/2025-23/07/2025)"
4. Choose the title from the dropdown menu and enter the remaining personal information including year of joining, total years of experience etc.
5. Upload the NOC on Institute/College/University letterhead. Click here to download the template.
6. Click on Submit to complete the registration process.

RESOURCE PERSONS:

The course content will be delivered from a pool of resource persons from leading prestigious academic institutions, research labs and industry.

ELIGIBILITY:

- Faculty members working in universities and colleges that are included under Section 2(f) of the UGC Act are eligible to attend RC.For the Refresher course, participation in any FIP is a prerequisite for admission.
- This programme shall be taken into consideration for fulfillment of the requirements as laid down in Career Advancement Scheme as per UGC Regulations.

COORDINATORS:

Dr. Nachiketa Mishra
Assistant Professor
School of S&H (Mathematics Stream),
nmishra@iiitdm.ac.in +91 9108682466

Dr. Jagannath Bhanja
Assistant Professor
School of S&H (Mathematics Stream),
jagannath@iiitdm.ac.in +91 94388 56415

Dr. Sanjeet Kumar Nayak
Assistant Professor
Department of Computer Science and Engineering,
sanjeetn@iiitdm.ac.in +91 94734 80414

Dr. Sarbendu Rakshit
Assistant Professor
School of S&H (Mathematics Stream),
sarbendu@iiitdm.ac.in +9190461 92342

IIITDM Kancheepuram
Chennai - 6000127, TamilNadu.