NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS270ME25
Course Title:	Mobile and Wireless Network Security
Course Type:	Department Elective-II
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
2	0	2	-	-	-	3

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to:

1. relate the fundamental concepts of mobile and wireless network security (BL2)
2. identify security threats in wireless networks and design strategies to manage network security (BL3)
3. analyse security issues in IoT and cellular networks (BL4)
4. design a secured network application considering all possible threats. (BL6)

Unit	Contents	Teaching Hours (Total 30)
Unit-I	**Security in General Wireless/Mobile Networks:** High-Performance Elliptic Curve Cryptographic Co-processor, An Adaptive Encryption Protocol in Mobile Computing	04
Unit-II	**Security in Wireless LANs**: Cross Domain Mobility Adaptive Authentication, AAA Architecture and Authentication for wireless LAN Roaming, Experimental Study on Security Protocols in WLANs	05
Unit-III	**Security in Ad Hoc Networks:** Pre-authentication and authentication models in Ad Hoc Networks, Promoting Identity-based key management, attacks and countermeasures, Secure and resilient data aggregation, Secure routing in MANET, Intrusion Detection System in MANET	06
Unit-IV	**Security in Mobile Cellular Networks**: Security issues in GSM, 3G and 4G networks, Authentication and encryption, Security concerns in 5G networks	06
Unit-V	**Security in Sensor Networks and IoT**: Security Issues, Key Management Schemes, Secure Routing in Sensor Networks, Energy-aware security mechanisms, Security and privacy issues in IoT, Identity and access management, Data Integrity, Best practices for IoT security.	09

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall
2. Y. Xiao, X. Shen, D. Z.Du, Wireless Network Security, Springer International Edition
3. W. Stallings. Cryptography & Network Security: Principles and Practice, Prentice Hall
4. Noureddine Boudriga, Security of Mobile Communications, CRC Press
5. Levente Buttyán and Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks, Cambridge University Press
6. James Kempf, Wireless Internet Security: Architectures and Protocols, Cambridge University Press
7. Stefanos Gritzalis, Tom Karygiannis, Charalabos Skianis, Security and Privacy in Mobile and Wireless Networking (Emerging Communication and Service Technologies), Paperback, Troubador Pub
8. Himanshu Dviwedi, Chris Clark, and David Thiel, Mobile Application Security, McGraw-Hill.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Design and configure a basic wireless network using Wi-Fi technology by setting up a wireless router and configuring network parameters to establish a secure and functional Wireless Local Area Network (WLAN) in Cisco Packet Tracer	02
2	Implement Elliptic Curve Encryption and Decryption for a given input file. Use GF(2^8)	04
3	Design an ad hoc network with various types of ad hoc, sensor and IoT nodes in Cisco Packet Tracer	02
4	Setup a rogue access point using Airbase-ng or Hostapd and capture as well as analyse the received traffic	02
5	Demonstrate methods to bypass MAC filtering in WiFi networks	02
6	Demonstrate how WEP encryption can be cracked in a Wireless LAN	02
7	Demonstrate how WEP encryption can be cracked in a Wireless LAN	02
8	Perform network hardening on a simulated network environment by applying security measures such as disabling unnecessary services, configuring firewalls, implementing access controls, and monitoring network traffic. Evaluate the effectiveness of these hardening techniques through vulnerability scanning, penetration testing, and traffic monitoring	06
9	Implement an encryption scheme for ad hoc networks modifying the network protocols in NS3	06
10	Perform network traffic encryption using Elliptic Curve Cryptography for wireless networks in NS3.	02