NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	MTech CSE (Cyber Security)
Course Code:	6CS270
Course Title:	Mobile and Wireless Network Security
Course Type:	(□ Core/ □ Value Added Course / √ **Department Elective** / □ Institute Elective/ □ University Elective/ □ Open Elective / □ Any other)
Year of Introduction:	2022-23

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

Course Learning Outcomes (CLOs):

At the end of the course, the student will be able to –

1. explain the fundamental concepts of mobile and wireless network security (BL2)
2. examine security threats in wireless networks and design strategies to manage network security (BL4)
3. design a wireless network with all required configurations (BL6)
4. design secured network application considering all possible threats (BL6)

Syllabus: **Total Teaching hours: 30**

Unit	**Syllabus**	**Teaching hours**
Unit-I	**Security concerns in Wireless/Mobile Networks:** High Performance Elliptic Curve Cryptographic Co-processor, An Adaptive Encryption Protocol in Mobile Computing	04
Unit-II	**Security in Wireless LANs:** Authentication methods, 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 semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Y. Xiao, X. Shen, D. Z.Du, Wireless Network Security, Springer International Edition.
2. Lei Chen, JiahuangJi, Zihong Zhang, Wireless Network Security, Springer Science & Business Media
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. Patrick Traynor, Patrick McDaniel, and Thomas La Porta, Security for Telecommunications Networks, Springer
8. Frank Adelstein, Sandeep K.S. Gupta, Golden G. Richard III, and Loren Schwiebert, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill Professional

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Implementing a simple wireless network with required configurations using Wi-Fi	02
2	Developing an ad hoc network with various types of ad hoc, sensor and IoT nodes	06
3	Setting up a rogue access point	02
4	Hacking MAC filtering	02
5	Cracking the WEP encryption	02
6	Breaking WPA2-Personal Passwords	02
7	Performing network hardening.	06
8	Implement an encryption scheme for ad hoc network modifying the network protocols.	06
9	Perform network traffic encryption for wireless network.	02