REFERENCES:

1. M. J. Osborne," An Introduction to Game Theory", Oxford University Press, 2004.
2. M. Machler, E. Solan, S. Zamir, "Game Theory", Cambridge University Press, 2013
3. N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani (Editors), "Algorithmic Game Theory" Cambridge University Press, 2007.
4. A.Dixit and S. Skeath, "Games of Strategy", Second Edition, W W Norton & Co Inc, 2004.
5. YoavShoham, Kevin Leyton-Brown, "Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations", Cambridge University Press 2008.
6. Zhu Han, Dusit Niyato, Walid Saad, Tamer Basar and Hjorungnes, "Game Theory in Wireless and Communication Networks", Cambridge University Press, 2012.
7. Y.Narahari, "Game Theory and Mechanism Design", IISC Press, World Scientific.

CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√				√	√	
2.	√		√	√			√	√	√
3.	√		√	√			√	√	√
4.	√		√	√			√	√	√
5.	√		√	√			√	√	√

CP5071 ADHOC AND WIRELESS SENSOR NETWORKS L T P C
3 0 0 3

OBJECTIVES:

- To learn about the issues in the design of wireless ad hoc networks.
- To understand the working of protocols in different layers of mobile ad hoc and sensor networks.
- To expose the students to different aspects in sensor networks.
- To understand various traffic generators and models for sensor networks.
- To understand various security issues in ad hoc and sensor networks and solutions to the issues.

UNIT I FUNDAMENTALS AND ROUTING PROTOCOLS OF WIRELESS AD HOC NETWORKS 9

Introduction – Applications of Mobile Ad Hoc Networks (MANETs) – Medium Access Control Layer – Topology Control – Routing Protocols – Broadcasting – Multicasting – Internet Connectivity for MANETs – Security in MANETs - Scenario Based Performance Analysis of Various Routing Protocols in MANETs

UNIT II MOBILITY MODELS AND OVERHEAD CONTROL MECHANISMS IN MANETS 9

Description of Various Mobility Models – Simulation and Analysis of Various Mobility Models – Overhead Analysis in Hierarchical Routing Scheme – Overhead Minimization Techniques – Energy Models

UNIT III WIRELESS SENSOR NETWORKS (WSN) 9

Applications of WSNs – Hardware and Software Issues in WSN – Design Issues of MAC Protocols – Deployment – Localization – Synchronization – Calibration – Network Layer Issues – Classification of Routing Protocols – Transport Layer Issues – Data Aggregation and Dissemination – Database Centric and Querying

UNIT IV PERFORMANCE ANALYSIS AND EVALUATION 9

Overview of IEEE 802.15.4 and its Characteristics – Data Gathering Paradigm – Simulation Environment and Result Analysis of IEEE 802.15.4 - Zigbee Routing Protocols – Traffic Generators – Traffic Model - Simulation Environment and Result Analysis of Zigbee Routing Protocols.

UNIT V SECURITY IN ADHOC AND SENSOR NETWORKS 9

Security Attacks – Key Distribution and Management – Intrusion Detection – Software based Anti-tamper techniques – Water marking techniques – Defence against routing attacks – Secure Ad hoc routing protocols – Broadcast authentication WSN protocols – TESLA – Biba – Sensor Network Security Protocols – SPINS

TOTAL: 45 PERIODS

OUTCOMES:

Upon completion of the course, the student will be able to

- Identifying suitable routing protocols for various scenarios of ad hoc networks.
- To explore various mobility models for MANETs.
- Identify different issues in wireless sensor networks.
- Analyse the performance of IEEE 802.15.4.
- Identify and critique security issues in ad hoc and sensor networks.

REFERENCES:

1. Subir Kumar Sarkar, “Wireless Sensor and Ad Hoc Networks Under Diversified Network Scenarios”, Auerbach Publications, 2012.
2. Holger Karl, Andreas Willig, “Protocols and Architectures for Wireless Sensor Networks”, Wiley India Private Limited, 2011.
3. Erdal Çayirci, Chunming Rong, “Security in Wireless Ad Hoc and Sensor Networks”, John Wiley and Sons, 2009.
4. Carlos De Morais Cordeiro, Dharma Prakash Agrawal, “Ad Hoc and Sensor Networks: Theory and Applications”, World Scientific Publishing, Second Edition, 2011.
5. Waltenegus Dargie, Christian Poellabauer, “Fundamentals of Wireless Sensor Networks Theory and Practice”, Wiley India Private Limited, 2014.
6. Adrian Perrig, J.D. Tygar, “Secure Broadcast Communication: In Wired and Wireless Networks”, Kluwer Academic Publishers, Springer, 2002.

CO	PO						PSO		
	1	2	3	4	5	6	1	2	3
1.	√		√				√	√	
2.	√		√				√	√	
3.	√		√	√			√	√	√
4.	√		√				√	√	
5.	√		√	√			√	√	√

SE5075 **SOFTWARE SECURITY** **L T P C**
3 0 0 3

OBJECTIVES:

- Know the importance and need of software security.
- Know about various attacks.
- Learn about secure software design.
- Understand risk management in secure software development.
- Know the working of tools related to software security.

UNIT I LOW LEVEL ATTACKS 9

Need For Software Security – Memory Based Attacks – Low Level Attacks Against Heap and Stack - Stack Smashing – Format String Attacks – Stale Memory Access Attacks – ROP (Return Oriented Programming) – Malicious Computation Without Code Injection. Defense Against Memory Based Attacks – Stack Canaries – Non-Executable Data - Address Space Layout Randomization (ASLR), Memory-Safety Enforcement, Control-Flow Integrity (CFI) – Randomization

UNIT II SECURE DESIGN 9

Isolating The Effects of Untrusted Executable Content - Stack Inspection – Policy Specification Languages – Vulnerability Trends – Buffer Overflow – Code Injection - Generic Network Fault Injection– Local Fault Injection - SQL Injection - Session Hijacking. Secure Design - Threat Modeling and Security Design Principles - Good and Bad Software Design - Web Security- Browser Security: Cross-Site Scripting (XSS), Cross-Site Forgery (CSRF) – Database Security – File Security

UNIT III SECURITY RISK MANAGEMENT 9

Risk Management Life Cycle – Risk Profiling – Risk Exposure Factors – Risk Evaluation and Mitigation – Risk Assessment Techniques – Threat and Vulnerability Management.

UNIT IV SECURITY TESTING 9

Traditional Software Testing – Comparison - Secure Software Development Life Cycle - Risk Based Security Testing – Prioritizing Security Testing With Threat Modeling – Shades of Analysis: White, Grey and Black Box Testing.