Computer Networks and Security

(Code : 314451)

Semester VI – Information Technology
(Savitribai Phule Pune University)

Strictly as per the New Choice Based Credit System Syllabus (2019 Course)
Savitribai Phule Pune University w.e.f. academic year 2021-2022

J. S. Katre

M.E. (Electronics and Telecommunication)
Formerly, Assistant Professor
Department of Electronics Engineering
Vishwakarma Institute of Technology (V.I.T.), Pune.
Maharashtra, India

Vaishali S. Joshi

TechKnowledge™ Publications

PE137A Price ₹ 315/-

(Book Code : PE137A)

Computer Networks and Security (Code : 314451)

(Semester VI - Information Technology, Savitribai Phule Pune University)

J. S. Katre, Vaishali S. Joshi

First Printed in India : January 2001

First Edition : January 2022 **(TechKnowledge Publications)**

This edition is for sale in India, Bangladesh, Bhutan, Maldives, Nepal, Pakistan, Sri Lanka and designated countries in South-East Asia. Sale and purchase of this book outside of these countries is unauthorized by the publisher.

ISBN : 978-93-5563-080-3

Published by :

TechKnowledge Publications

Head Office : B/5, First floor, Maniratna Complex, Taware Colony, Aranyeshwar Corner,
Pune - 411 009. Maharashtra State, India

Ph : 91-20-24221234, 91-20-24225678.

Email : info@techknowledgebooks.com,

Website : www.techknowledgebooks.com

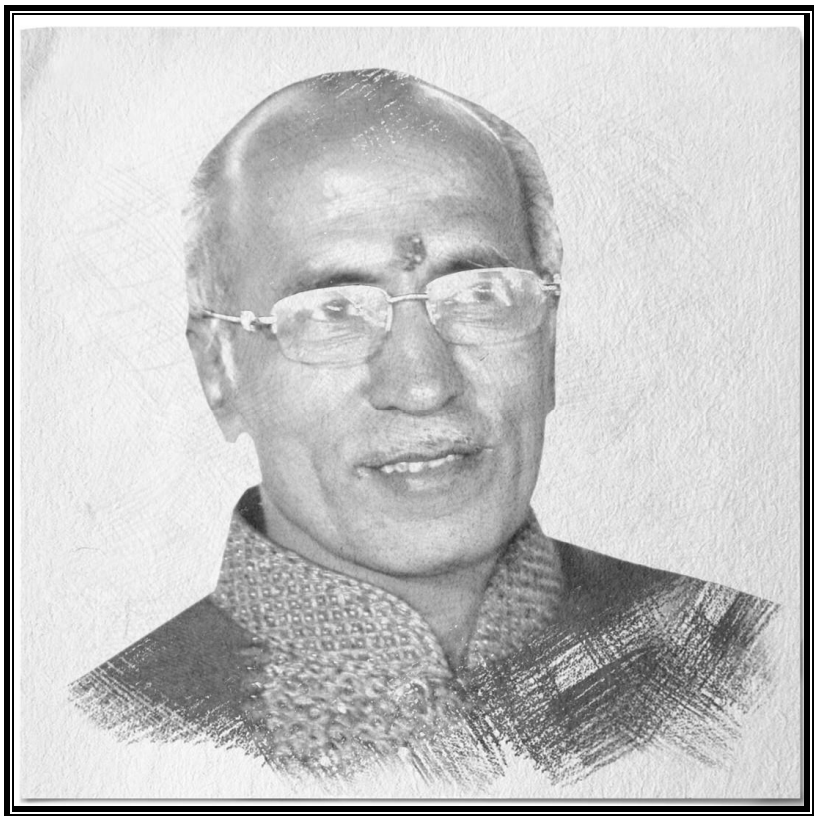
[314451] (FID : PE137) (Book Code : PE137A)

We dedicate this Publication soulfully and wholeheartedly,

in loving memory of our beloved founder director,

Late Shri. Pradeepji Lalchandji Lunawat,

who will always be an inspiration, a positive force and strong support behind us.



"My work is my prayer to God"

- Lt. Shri. Pradeepji L. Lunawat

Soulful Tribute and Gratitude for all Your Sacrifices, Hardwork and 40 years of Strong Vision…

(Book Code : PE137A)

Syllabus…

Computer Networks and Security : Sem. VI, Information Technology (SPPU)

Teaching Scheme	Credits Scheme :	Examination Scheme :
Theory (TH) : 03 hrs/week	**03 Credit**	**Mid_Semester : 30 Marks**
		End_Semester : 70 Marks

Prerequisite Courses :

1. Basic of Computer Network

Companion Course :

1. Cyber Security

Course Objectives :

To familiarize students with-

1. The application layer services, responsibilities and protocol.
2. Fathom wireless network and different wireless standards.
3. Differences in different wireless networks and to learn different mechanism used at layers of wireless network.
4. The concept of network security.
5. Basic cryptographic techniques in application development.
6. Cyber security vulnerabilities & study typical threats to modern digital systems.

Course Outcomes :

On completion of the course, students will be able to-

CO1 : Explain Responsibilities, services offered and protocol used at application layer of network.

CO2 : Apply concepts of wireless network and different wireless standards.

CO3 : Recognize the Adhoc Network's MAC layer, routing protocol and Sensor network architecture.

CO4 : Implement the principal concepts of network security and Understand network security threats, security services, and countermeasures

CO5 : Apply basic cryptographic techniques in application development.

CO6 : Gain a good comprehension of the landscape of cyber security Vulnerabilities & describe typical threats to modern digital systems.

Course Contents

Unit I

Application Layer :

Client Server Paradigm : Communication using TCP and UDP, Peer to peer paradigm, **Application Layer Protocols :** DNS, FTP, TFTP, HTTP, SMTP, POP, IMAP, MIME, DHCP, TELNET. **(Refer Chapter 1)**

Unit II

Wireless Standards :

Wireless LANs : Fundamentals of WLAN, Design goals, Characteristics, Network architecture, **IEEE 802.11 :** components in IEEE 802.11 network, Physical layer, **MAC Sub Layers :** DCF, PCF, Hidden and Exposed station problem, Frame format, Addressing mechanism, **IEEE 802.15.1 Bluetooth :** Architecture layers, Operational states, **IEEE 802.16 WiMax :** Services, Architecture, Layers, Comparison between Bluetooth, IEEE 802.11 and IEEE 802.16. **(Refer Chapter 2)**

Unit III

ADHOC and WSN :

Infrastructure network and Infrastructure-less wireless networks, Issues in Adhoc wireless network, **Adhoc Network MAC Layer :** Design issues, Design goal, Classification, MACAW, **Adhoc Network Routing Layer :** Issues in designing a routing protocol for Ad-hoc wireless networks, Classifications of routing protocols, DSDV, AODV, DSR.

Applications of Sensor Network, Comparison with Ad Hoc wireless network, Sensor node architecture Issues and Challenges in designing a sensor network, Classification of sensor network protocols, **Sensor network architecture :** Layered architecture, Clustered architecture. **(Refer Chapter 3)**

Unit IV

Introduction to Network Security :

Importance and Need for security, Network Attacks : Passive, Active. **Network Security Threats :** Unauthorized access, Distributed Denial of Service (DDoS) attacks, Man in the middle attacks, **Concept of Security Principles :** Confidentiality and Privacy, Authentication, Authorization and Access control, Integrity, Non-repudiation, **Stream Ciphers : Substitution Cipher :** Mono alphabetic cipher, Polyalphabetic substitution cipher. **Transposition Cipher :** Rail-Fence

Block Ciphers modes : Electronic Code Book (ECB) Mode, Cipher Block Chaining (CBC) Mode, Cipher Feedback Mode (CFB), Output Feedback (OFB) Mode. **(Refer Chapter 4)**

Unit V

Cryptographic Algorithm :

Mathematical preliminaries : Groups, Rings, Fields, Prime numbers, **Symmetric key algorithms :** Data encryption standards, Advanced encryption standard, **Public key encryption and Hash function :** RSA Digital signatures, **Digital certificates and Public key infrastructure :** Private key management, Diffie Hellman key exchange, The PKIX model. **(Refer Chapter 5)**

Unit VI

Introduction to Cyber Security :

Introduction to Cyber Security : Basic cyber security concepts, Layers of security, Vulnerability, Threat, Harmful acts-malware, Phishing, MIM attack, DOS attack, SQL Injection, **Internet Governance :** Challenges and Constraints, Computer criminals, Assets and Threat, Motive of attackers, Software attacks, Hardware attacks, **Cyber Threats :** Cyber warfare, Cyber crime, Cyber stalking, Cyber terrorism, Cyber espionage, Comprehensive cyber security policy. **(Refer Chapter 6)**

❑❑❑

Unit I

Syllabus : Client Server Paradigm : Communication using TCP and UDP, Peer to peer paradigm, **Application Layer Protocols :** DNS, FTP, TFTP, HTTP, SMTP, POP, IMAP, MIME, DHCP, TELNET.

Syllabus : Wireless LANs : Fundamentals of WLAN, Design goals, Characteristics, Network architecture, **IEEE 802.11 :** components in IEEE 802.11 network, Physical layer, **MAC Sub Layers :** DCF, PCF, Hidden and Exposed station problem, Frame format, Addressing mechanism, **IEEE 802.15.1 Bluetooth :** Architecture layers, Operational states, **IEEE 802.16 WiMax :** Services, Architecture, Layers, Comparison between Bluetooth, IEEE 802.11 and IEEE 802.16.

Syllabus : Infrastructure network and Infrastructure-less wireless networks, Issues in Adhoc wireless network, **Adhoc Network MAC Layer :** Design issues, Design goal, Classification, MACAW, **Adhoc Network Routing Layer :** Issues in designing a routing protocol for Ad-hoc wireless networks, Classifications of routing protocols, DSDV, AODV, DSR.

Applications of Sensor Network, Comparison with Ad Hoc wireless network, Sensor node architecture Issues and Challenges in designing a sensor network, Classification of sensor network protocols, **Sensor network architecture :** Layered architecture, Clustered architecture.

Unit IV

Syllabus : Importance and Need for security, Network Attacks : Passive, Active. **Network Security Threats :** Unauthorized access, Distributed Denial of Service (DDoS) attacks, Man in the middle attacks, **Concept of Security Principles :** Confidentiality and Privacy, Authentication, Authorization and Access control, Integrity, Non-repudiation, **Stream Ciphers : Substitution Cipher :** Mono alphabetic cipher, Polyalphabetic substitution cipher. **Transposition Cipher :** Rail-Fence.

Block Ciphers modes : Electronic Code Book (ECB) Mode, Cipher Block Chaining (CBC) Mode, Cipher Feedback Mode (CFB), Output Feedback (OFB) Mode.

Syllabus : Mathematical preliminaries : Groups, Rings, Fields, Prime numbers, **Symmetric key algorithms :** Data encryption standards, Advanced encryption standard, **Public key encryption and Hash function :** RSA Digital signatures, **Digital certificates and Public key infrastructure :** Private key management, Diffie Hellman key exchange, The PKIX model.

Unit VI

Syllabus : Introduction to Cyber Security : Basic cyber security concepts, Layers of security, Vulnerability, Threat, Harmful acts-malware, Phishing, MIM attack, DOS attack, SQL Injection, **Internet Governance :** Challenges and constraints, Computer criminals, Assets and Threat, Motive of attackers, Software attacks, Hardware attacks, **Cyber Threats :** Cyber warfare, Cyber crime, Cyber stalking, Cyber terrorism, Cyber espionage, Comprehensive cyber security policy.

❑❑❑