

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**TM
Publications



Computer Networks and Security (Code : 314451)

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

J. S. Katre, Vaishali S. Joshi

Copyright © Authors. All rights reserved. No part of this publication may be reproduced, copied, or stored in a retrieval system, distributed or transmitted in any form or by any means, including photocopy, recording, or other electronic or mechanical methods, without the prior written permission of the publisher.

This book is sold subject to the condition that it shall not, by the way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the publisher's prior written consent in any form of binding or cover other than which it is published and without a similar condition including this condition being imposed on the subsequent purchaser and without limiting the rights under copyright reserved above.

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.

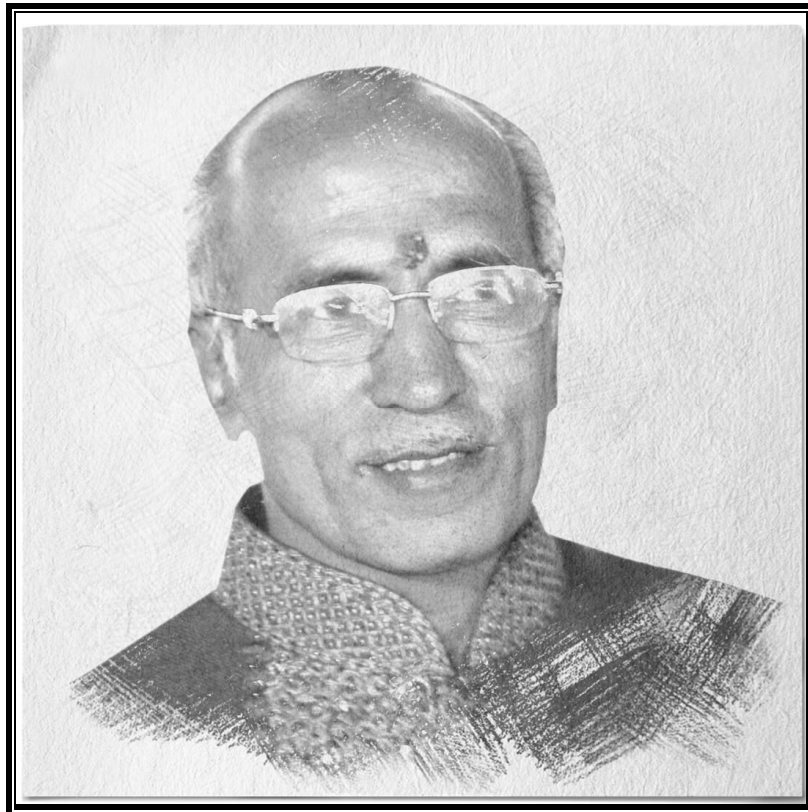
Email : info@techknowledgebooks.com,

Website : www.techknowledgebooks.com

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

(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...*

Syllabus...

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

Teaching Scheme

Theory (TH) : 03 hrs/week

Credits Scheme :

03 Credit

Examination Scheme :

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

Chapter 1 : Application Layer 1-1 to 1-54

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.

<p>1.1 Introduction 1-2</p> <p> 1.1.1 Position of Application Layer 1-2</p> <p>1.2 Providing Services 1-2</p> <p> 1.2.1 Standard and Non-standard Protocols 1-3</p> <p>1.3 Application Layer Paradigms 1-3</p> <p> 1.3.1 Traditional Paradigm Client Server 1-3</p> <p> 1.3.2 New Paradigm : Peer-to-Peer (P2P) 1-4</p> <p> 1.3.3 Mixed Paradigm 1-5</p> <p>1.4 Client Server Paradigm 1-5</p> <p> 1.4.1 Concurrency 1-6</p> <p> 1.4.1.1 Concurrency in Clients 1-6</p> <p> 1.4.1.2 Concurrency in Servers 1-6</p> <p> 1.4.2 Types of Servers 1-6</p> <p> 1.4.2.1 Connectionless Iterative Server 1-7</p> <p> 1.4.2.2 Connection - Oriented Concurrent Server 1-7</p> <p> 1.4.3 Socket Interface 1-7</p> <p> 1.4.4 Types of Interface 1-7</p> <p> 1.4.5 Socket Interface 1-8</p> <p> 1.4.6 Socket 1-8</p> <p> 1.4.7 Communication using UDP 1-9</p> <p> 1.4.8 Server Process 1-9</p> <p> 1.4.9 Client Process 1-10</p> <p>1.5 Communication using TCP 1-10</p> <p> 1.5.1 Server Process 1-10</p> <p> 1.5.2 The Client Process 1-11</p>	<p> 1.5.3 Peer to Peer Paradigm 1-11</p> <p> 1.5.4 P2P File Sharing 1-11</p> <p>1.6 Domain Name System (DNS) 1-12</p> <p> 1.6.1 How does DNS Work ? 1-12</p> <p> 1.6.2 Name Space 1-13</p> <p> 1.6.3 Flat Name Space 1-13</p> <p> 1.6.4 Hierarchical Name Space 1-13</p> <p>1.7 Domain Name Space 1-13</p> <p>1.8 Distribution of Name Space 1-14</p> <p> 1.8.1 Hierarchy of Name Servers 1-15</p> <p>1.9 DNS in the Internet 1-16</p> <p> 1.9.1 Generic Domains 1-16</p> <p> 1.9.2 Country Domain 1-16</p> <p> 1.9.3 Inverse Domain 1-16</p> <p>1.10 Name Address Resolution 1-16</p> <p> 1.10.1 Recursive Resolution 1-17</p> <p> 1.10.2 Iterative Resolution 1-17</p> <p> 1.10.3 The DNS Message Format 1-18</p> <p> 1.10.4 Caching 1-18</p> <p> 1.10.5 DNS Records 1-18</p> <p>1.11 World Wide Web (WWW) 1-20</p> <p> 1.11.1 Web from the Users Side 1-20</p> <p> 1.11.2 Web from the Servers Side 1-21</p> <p> 1.11.3 WWW Architecture 1-22</p> <p> 1.11.4 Browser (Web Client) 1-22</p> <p> 1.11.5 Server 1-22</p> <p> 1.11.6 Uniform Resource Locator (URL) 1-22</p> <p> 1.11.7 Cookies User-Server Interaction 1-23</p> <p>1.12 Web Documents 1-23</p> <p> 1.12.1 Static Documents 1-23</p> <p> 1.12.2 HTML (Hypertext Markup Language) 1-24</p> <p> 1.12.3 Dynamic Document 1-24</p>
---	--



1.12.4	Common Gateway Interface (CGI)	1-24	1.19.2	The Web and HTTP	1-38
1.12.5	Active Documents	1-25	1.19.3	Non-persistent and Persistent Connection	1-39
1.13	Electronic Mail	1-25	1.19.4	HTTP Messages	1-41
1.13.1	E-mail Architecture and Services	1-26	1.19.5	Request Message	1-41
1.13.2	Message Formats	1-27	1.19.6	Methods (Request Type)	1-41
1.14	MIME – Multipurpose Internet Mail Extensions	1-28	1.19.7	Response Message	1-42
1.14.1	Principle of MIME	1-28	1.20	Proxy Server	1-42
1.15	Message Transfer Agent SMTP	1-30	1.20.1	HTTP Security	1-42
1.15.1	Commands and Responses	1-30	1.21	Remote Login TELNET and SSH	1-43
1.15.2	SMTP (Simple Mail Transfer Protocol) ...	1-30	1.21.1	TELNET	1-43
1.15.3	Components of E-mail System	1-31	1.21.2	Network Virtual Terminal (NVT)	1-44
1.15.4	SMTP Commands	1-32	1.21.3	Security Problems of TELNET	1-44
1.15.5	SMTP Operation	1-32	1.22	Secure Shell (SSH)	1-44
1.15.6	Comparison of HTTP and SMTP	1-32	1.22.1	Port Forwarding	1-45
1.16	Message Access Agent POP and IMAP	1-32	1.22.2	SSH Packet Format	1-45
1.16.1	POP 3	1-33	1.22.3	Comparison of TELNET and SSH	1-45
1.16.2	IMAP4	1-33	1.23	Host Configuration DHCP	1-46
1.16.3	Comparison of IMAP and POP 3	1-34	1.23.1	Previously used Protocols	1-46
1.17	File Transfer Protocol (FTP)	1-34	1.23.2	DHCP	1-46
1.17.1	Communication in FTP	1-35	1.23.3	Advantages of DHCP	1-47
1.17.2	File Types	1-36	1.23.4	Components of DHCP	1-47
1.17.3	Data Structure	1-36	1.23.5	DHCP Operation	1-48
1.17.4	Transmission Mode	1-36	1.23.6	DHCP Operation on Different Networks	1-48
1.17.5	File Transfer	1-36	1.23.7	UDP Ports	1-49
1.17.6	FTP Commands	1-36	1.23.8	Using TFTP	1-49
1.18	TFTP	1-37	1.23.9	Error Control	1-49
1.18.1	Applications of TFTP	1-38	1.23.10	Optimizations in DHCP	1-50
1.18.2	Advantages	1-38	1.23.11	Packet Format	1-50
1.18.3	Disadvantages	1-38	1.24	Configuration of DHCP	1-51
1.18.4	Comparison of FTP and TFTP	1-38	1.24.1	Static Address Allocation	1-51
1.19	HTTP (Hypertext Transfer Protocol)	1-38			
1.19.1	Principle of HTTP Operation	1-38			



1.24.2	Dynamic Address Allocation	1-51	2.5.2	Interference	2-8
1.24.3	Transition States	1-51	2.5.3	Multipath Propagation	2-8
1.24.3.1	Address Acquisition States	1-52	2.5.4	Error	2-8
1.24.3.2	Early Lease Termination	1-52	2.6	Technical Issues	2-8
1.24.3.3	Lease Renewal States	1-53	2.6.1	Difference between Wireless and Wired Transmission	2-9
1.25	University Questions and Answers	1-54	2.7	Design Goals for WLANs	2-9
•	Review Questions.....	1-53	2.7.1	Factors Considered to Deploy WLAN	2-10
Unit II			2.8	Medium Access Control	2-10
Chapter 2 : Wireless Standards			2.9	MAC Protocol Issues	2-11
2-1 to 2-52			2.9.1	Hidden Terminal Problem	2-11
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.					
2.1	Introduction to WLAN / Wi-Fi	2-3	2.9.2	Exposed Station Problem	2-12
2.1.1	IEEE Standards	2-3	2.10	IEEE 802.11 Standard for WLAN	2-12
2.1.2	Wi-Fi	2-3	2.10.1	Classification of WLANs	2-13
2.1.3	ISM Band	2-3	2.10.2	The IEEE 802.11 Protocol Stack	2-13
2.2	Fundamentals of WLANs	2-4	2.10.3	802.11 Network Architecture	2-14
2.2.1	Wireless LAN Configuration	2-4	2.10.4	Types of Stations	2-15
2.2.2	Applications of Wireless LAN	2-4	2.11	The Physical Layer	2-15
2.2.3	Wireless LAN - 802.11 (Architecture)	2-4	2.11.1	Various PHY Specifications	2-16
2.3	Architectural Comparison of Wired and Wireless LANs	2-5	2.11.2	IEEE 802.11 FHSS	2-16
2.4	WLAN Equipment	2-7	2.11.3	IEEE 802.11 DSSS	2-17
2.4.1	LAN Adapter	2-7	2.11.4	IEEE 802.11 Infrared	2-17
2.4.2	Access Point (AP)	2-7	2.11.5	IEEE 802.11 a OFDM	2-18
2.4.3	Outdoor LAN Bridges	2-8	2.11.6	IEEE 802.11 b HR-DSSS	2-18
2.5	Characteristics of WLANs	2-8	2.11.7	IEEE 802.11 g OFDM	2-18
2.5.1	Attenuation	2-8	2.11.8	IEEE 802.11 n OFDM	2-18
			2.12	MAC Sublayer	2-18
			2.12.1	RTS and CTS Messages	2-19
			2.12.2	The Retry Counters	2-19
			2.12.3	Distributed Co-ordination Function (DCF)	2-19
			2.12.4	Hidden Station Problem	2-21



2.13	Point Co-ordinate Function (PCF)	2-21	2.23.6	Modulation	2-36
2.13.1	Fragmentation	2-22	2.24	Link Types	2-36
2.13.2	Exposed Station Problem	2-22	2.24.1	SCO Link	2-36
2.14	Framing in WLAN	2-22	2.24.2	ACL Link	2-36
2.15	Addressing Mechanism	2-23	2.25	Packet Transmission in Bluetooth	2-36
2.15.1	Case 1 : 00	2-24	2.26	Operating States of Bluetooth	2-37
2.15.2	Case 2 : 01	2-24	2.26.1	Standby Mode	2-37
2.15.3	Case 3 : 10	2-24	2.26.2	Connection Mode	2-37
2.15.4	Case 4 : 11	2-25	2.26.3	Connection Establishment in BT.....	2-38
2.15.5	Exposed Station Problem	2-25	2.26.4	Interference Handling Techniques in Bluetooth	2-38
2.15.6	Advantages of WLANs	2-25	2.26.5	Advantages of Bluetooth	2-39
2.15.7	Disadvantages of WLAN	2-25	2.26.6	Disadvantages of Bluetooth	2-39
2.15.8	Applications of Wireless LAN	2-26	2.26.7	Security Limitations in Bluetooth	2-40
2.16	PAN (Personal Area Network)	2-26	2.27	Applications of BT	2-40
2.17	Comparison of Wired and Wireless LANs	2-26	2.28	Wireless MAN (WMAN)	2-40
2.18	Wireless PAN (WPAN)	2-26	2.28.1	Wi-MAX	2-41
2.18.1	Need of Wireless PAN	2-27	2.28.2	Wi-Bro (Wireless Broadband)	2-41
2.19	Bluetooth IEEE 802.15.1	2-27	2.28.3	Need of WMAN	2-41
2.20	Principle of Bluetooth	2-28	2.29	IEEE 802.16 (Wi-MAX)	2-42
2.21	Bluetooth Devices	2-28	2.29.1	Wi-Max Standards	2-42
2.21.1	Features of Bluetooth	2-28	2.29.2	Structure of WMAN	2-42
2.21.2	Radio Specifications of BT	2-28	2.29.3	IEEE Project 802.16 (Wi-Max)	2-43
2.22	Bluetooth Architecture	2-29	2.29.4	Spectrum Allocation	2-43
2.22.1	Piconets	2-29	2.29.5	Specifications of IEEE 802.16	2-43
2.22.2	Scatternets	2-30	2.30	Wi-Max Services	2-43
2.22.3	Comparison of Piconet and Scatternet ...	2-31	2.30.1	Fixed Wi-Max Services	2-43
2.23	Bluetooth Protocol Stack	2-31	2.30.2	Mobile Wi-Max Services	2-44
2.23.1	Logical Link Control and Adaptation Protocol (L2CAP)	2-32	2.30.3	Comparison between Fixed and Mobile WiMAX	2-44
2.23.2	Frame Format in Baseband Layer	2-33	2.31	IEEE 802.16 Standards	2-44
2.23.3	TDMA (Time Division Multiple Access) ...	2-34	2.31.1	Comparison of IEEE 802.16 Standards	2-45
2.23.4	Frequency Band	2-36			
2.23.5	FHSS	2-36			



2.32	WMAN (802.16) Network Architecture ...2-46	3.3.3	Transport Layer Protocols3-7
2.32.1	Network Components2-46	3.3.4	Pricing Scheme3-7
2.32.2	Features / Characteristics of WiMAX2-47	3.3.5	Quality of Service3-7
2.32.3	Layers in 802.162-48	3.3.6	Self-organisation3-8
2.32.4	Advantages of IEEE 802.16 (WiMAX)2-50	3.3.7	Security3-8
2.32.5	Disadvantages of Wi-MAX2-51	3.3.8	Service Discovery and Addressing3-8
2.32.6	Uses / Applications of Wi-Max2-51	3.3.9	Management of Energy3-8
2.33	Comparison of Bluetooth, IEEE 802.11 and IEEE 802.162-52	3.3.10	Scalability3-9
•	Review Questions..... 2-52	3.3.11	Deployment Considerations3-9
Unit III		3.4	ADHOC Network MAC Layer3-9
Chapter 3 : ADHOC and WSN 3-1 to 3-52		3.4.1	Issues in Designing a MAC Protocol3-9
<p>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.</p> <p>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.</p>		3.4.2	Design Goals of a MAC Protocol3-11
3.1	Introduction to Wireless Network 3-3	3.5	Classification of MAC Protocols3-11
3.2	Classification of Wireless Networks 3-3	3.5.1	Contention-Based Protocols3-11
3.2.1	Infrastructure Networks 3-3	3.5.2	Contention-Based Protocols with Reservation Mechanisms3-12
3.2.2	Infrastructure-less Networks / Adhoc Networks 3-4	3.5.3	Contention-Based Protocols with Scheduling Mechanisms3-13
3.2.3	Comparison of Infrastructure and Ad hoc Networks 3-5	3.6	Contention-Based Protocols3-13
3.3	Issues and Challenges in Ad hoc Networks 3-5	3.6.1	MACA Protocol3-14
3.3.1	Routing Protocols 3-5	3.6.2	MACAW : A Media Access Protocol for Wireless LANs3-14
3.3.2	Multicasting 3-6	3.7	Other MAC Protocols3-17
		3.8	Routing in Adhoc Network3-17
		3.8.1	Design Issues / Challenges in Routing Protocol3-17
		3.8.2	Characteristics / Goals of Routing Protocols3-19
		3.8.3	Requirements of Routing Protocols3-19
		3.9	Classification of Routing Protocols3-20
		3.9.1	Based on the Routing Information Update Mechanism3-20
		3.9.2	Based on the use of Temporal Information for Routing3-21



3.9.3	Based on the Routing Topology	3-22	3.19.2	Management Planes in the Protocol Stack	3-37
3.9.4	Based on the Utilization of Specific Resources	3-22	3.20	Sensor Network Architecture	3-38
3.10	Table Driven Routing Protocols	3-22	3.20.1	Types of WSN Architectures	3-38
3.10.1	Destination Sequenced Distance Vector Routing Protocol (DSDV)	3-23	3.21	Layered Architecture	3-38
3.11	On-demand Routing Protocol	3-25	3.22	Clustered Architecture	3-39
3.11.1	Dynamic Source Routing Protocol (DSR)	3-25	3.23	Low Energy Adaptive Clustering Hierarchy (LEACH)	3-40
3.11.2	Adhoc on Demand Distance Vector Routing Protocol (AODV)	3-27	3.23.1	Phases of LEACH	3-41
3.11.3	Comparison of DSDV, DSR and AODV	3-29	3.23.2	Advantages of LEACH	3-41
3.12	Advantages of Ad hoc Network	3-29	3.23.3	Disadvantages of LEACH	3-41
3.13	Applications of Ad hoc Network	3-29	3.24	MAC Protocols for WSNs	3-41
3.14	Introduction to Wireless Sensor Networks (WSN)	3-30	3.24.1	Design Issues for Medium Access Protocols	3-42
3.14.1	Applications of Wireless Sensor Networks	3-30	3.25	Classification of WSN MAC Protocols	3-42
3.14.2	Differences between Adhoc and WSNs	3-31	3.25.1	Self Organizing MAC for Sensor Networks (SMACS).....	3-43
3.14.3	Comparison of WSNs and Ad-hoc Networks	3-32	3.25.2	Eavesdrop-and-register (EAR) Algorithm.....	3-44
3.15	Issues and Challenges in Designing a WSN	3-32	3.25.3	Adaptive Transmission Rate Control (ARC)	3-46
3.16	Operating Environment Constraints in WSN	3-33	3.26	Design Issues and Routing Challenges in WSNs	3-46
3.17	WSN Architecture	3-33	3.27	Classification of WSN Routing Protocols	3-46
3.17.1	Characteristics of WSNs	3-33	3.27.1	Flooding	3-47
3.18	Sensor Node Architecture	3-34	3.27.2	Gossiping	3-48
3.18.1	Controller	3-34	3.27.3	Sensor Protocols for Information Via Negotiation (SPIN)	3-48
3.18.2	Memory Unit	3-35	3.27.4	Directed Diffusion	3-49
3.18.3	Sensors and Actuators	3-35	3.27.5	Rumor Routing	3-50
3.18.4	Communication Device	3-35	3.27.6	Comparison of Routing Protocols in WSN	3-51
3.18.5	Power Supply	3-36	3.28	Advantages of WSNs	3-51
3.19	Protocol Stack for WSN	3-37	3.28.1	Disadvantages of WSNs.....	3-52
3.19.1	Layers in the Protocol Stack	3-37		Review Questions	3-52

Unit IV

Chapter 4 : Introduction to Network Security 4-1 to 4-32

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.

<p>4.1 Introduction 4-2</p> <p>4.2 Security Services 4-2</p> <p>4.3 Need for Security 4-2</p> <p>4.4 Key Principles of Security 4-3</p> <p> 4.4.1 Security Goals 4-3</p> <p>4.5 CIA Triad 4-3</p> <p>4.6 Security Attacks 4-4</p> <p> 4.6.1 Attacks on Confidentiality 4-4</p> <p> 4.6.2 Attacks on Integrity 4-4</p> <p> 4.6.3 Attacks on Availability 4-4</p> <p>4.7 ITU-T X-800 Security Architecture for OSI 4-4</p> <p>4.8 Security Policy and Mechanisms 4-5</p> <p> 4.8.1 Specific Security Mechanisms 4-5</p> <p> 4.8.2 Pervasive Security Mechanisms 4-6</p> <p>4.9 Model of Network Security 4-6</p> <p>4.10 Techniques to Achieve Security Goals 4-7</p> <p> 4.10.1 Cryptography 4-7</p> <p> 4.10.2 Steganography 4-8</p> <p>4.11 Cryptographic Attacks 4-8</p> <p> 4.11.1 Passive Attacks 4-8</p> <p> 4.11.2 Active Attacks 4-9</p>	<p> 4.11.3 Comparison of Active and Passive Attacks 4-10</p> <p>4.12 Security Threats 4-10</p> <p>4.13 Unauthorized Access 4-11</p> <p>4.14 Distributed Denial of Service (DDoS) Attacks 4-11</p> <p> 4.14.1 Types of DDoS Attacks 4-11</p> <p> 4.14.2 Simple DDoS Attacks 4-12</p> <p> 4.14.3 Flooding-Based DDoS Attacks 4-13</p> <p>4.15 Man-in-the-middle Attack (MITM) 4-14</p> <p>4.16 Concept of Security Principles 4-14</p> <p> 4.16.1 Confidentiality and Privacy 4-14</p> <p> 4.16.2 Message Integrity 4-14</p> <p> 4.16.3 Message Authentication 4-15</p> <p> 4.16.4 Entity Authentication 4-16</p> <p> 4.16.5 Difference between Entity and Message Authentication 4-17</p> <p> 4.16.6 Message Nonrepudiation 4-17</p> <p> 4.16.7 Access Control 4-17</p> <p> 4.16.8 Availability 4-17</p> <p> 4.16.9 Authorization 4-18</p> <p>4.17 Types of Cryptography Algorithms 4-18</p> <p>4.18 Symmetric Key Cryptography 4-18</p> <p> 4.18.1 Types of Symmetric Key Ciphers 4-19</p> <p>4.19 Traditional Symmetric Key Ciphers 4-19</p> <p> 4.19.1 Substitution Ciphers 4-19</p> <p>4.20 Monoalphabetic Substitution 4-19</p> <p> 4.20.1 Types of Monoalphabetic Ciphers 4-19</p> <p> 4.20.2 Additive (Shift / Caesar) Cipher 4-20</p> <p> 4.20.3 Multiplicative Ciphers 4-21</p> <p> 4.20.4 Affine Cipher 4-22</p> <p>4.21 Polyalphabetic Substitution 4-23</p> <p> 4.21.1 Types of Polyalphabetic Ciphers 4-23</p> <p> 4.21.2 Autokey Cipher 4-23</p>
---	--



4.21.3	Playfair Cipher	4-24	5.1.3	Fields	5-3
4.21.4	Vigenere Cipher	4-25	5.1.4	Summary of Algebraic Structures	5-4
4.21.5	Hill Cipher	4-25	5.2	Prime Numbers	5-4
4.21.6	One Time Pad (Vernam Cipher)	4-26	5.3	Symmetric Key Cryptography	5-5
4.21.7	Comparison of Monoalphabetic and Polyalphabetic Cipher	4-27	5.3.1	Advantages of Symmetric Key Ciphers	5-5
4.22	Transposition Cipher	4-27	5.3.2	Disadvantages of Symmetric Key Ciphers	5-5
4.22.1	Rail-Fence Technique	4-28	5.4	Data Encryption Standard (DES)	5-5
4.23	Stream and Block Ciphers	4-28	5.4.1	Key Generation	5-6
4.23.1	Stream Ciphers	4-29	5.4.2	Strengths of DES	5-7
4.24	Block Ciphers	4-29	5.4.3	Weaknesses of DES	5-7
4.24.1	Modern Symmetric Key Ciphers	4-29	5.5	Double DES	5-7
4.24.2	A Modern Block Cipher	4-29	5.6	Triple DES (3DES)	5-9
4.24.3	Comparison of Stream and Block Cipher	4-29	5.6.1	3-DES with Two Keys	5-9
4.25	Block Cipher Modes	4-30	5.6.2	3-DES with Three Keys	5-9
4.25.1	Electronic Code Book (ECB) Mode	4-30	5.7	Advanced Encryption Standard (AES)	5-9
4.25.2	Cipher Block Chaining (CBC) Mode	4-30	5.7.1	Structure of Encryption Round	5-10
4.25.3	Cipher Feedback (CFB) Mode	4-31	5.8	Public (Asymmetric) Key Cryptography	5-11
4.25.4	Output Feedback (OFB) Mode	4-31	5.8.1	Public (Asymmetric) Key Cryptosystem ..	5-11
4.25.5	Comparison of Block Cipher Modes	4-32	5.8.2	Comparison of Symmetric Key and Asymmetric Key Cryptosystems	5-12
•	Review Questions.....	4-32	5.9	The RSA Cryptosystem	5-12
Unit V			5.9.1	Comparison of DES, AES and RSA	5-14
Chapter 5 : Cryptographic Algorithm			5.10	Hash Function	5-15
5-1 to 5-32			5.10.1	Requirements for a Hash Function	5-15
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.					
5.1	Algebraic Structures	5-2	5.10.2	Simple Hash Function	5-16
5.1.1	Groups	5-2	5.11	Digital Signature	5-16
5.1.2	Rings.....	5-2	5.11.1	Digital Signature Process	5-16
			5.11.2	Signing the Digest	5-17
			5.11.3	Services Provided by Digital Signature ..	5-17
			5.11.4	Entity Authentication	5-18
			5.11.5	Difference between Entity and Message Authentication	5-18



5.12	Diffie-Hellman key Exchange	5-19
5.12.1	Diffie-Hellman Algorithm	5-19
5.12.2	Concept of Diffie-Hellman	5-19
5.12.3	Security of Diffie-Hellman Algorithm	5-20
5.12.4	Advantages of Diffie-Hellman Algorithm	5-21
5.12.5	Disadvantages of Diffie-Hellman Algorithm	5-21
5.13	Key Management	5-22
5.13.1	Symmetric Key Distribution	5-22
5.13.2	Key Distribution Center (KDC)	5-22
5.13.3	Multiple KDCs	5-22
5.13.4	Public Key Distribution	5-23
5.14	Digital Certificates	5-23
5.14.1	Certification Authority (CA)	5-24
5.14.2	Structure of Digital Certificate	5-24
5.14.3	Creation of Digital Certificate	5-25
5.14.4	Types of Digital Certificates	5-26
5.14.5	Advantages of Digital Certificates	5-26
5.14.6	Disadvantages of Digital Certificates	5-27
5.14.7	Comparison of Digital Signature and Digital Certificate	5-27
5.15	Public Key Infrastructure (PKI)	5-27
5.16	Private Key Management	5-28
5.16.1	Mechanisms for Protecting Private Keys	5-28
5.16.2	Multiple Key Pairs	5-29
5.16.3	Key Update	5-29
5.16.4	Key Archival	5-29
5.17	The PKIX Model	5-30
5.17.1	Services Provides by PKIX	5-30
5.17.2	Components of PKIX Model	5-31
5.17.3	PKIX Architectural Model	5-31
•	Review Questions	5-32

Unit VI

Chapter 6 : Introduction to Cyber Security 6-1 to 6-30

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.

6.1	Introduction to Cyber Security.....	6-3
6.2	Challenges to Cyber Security	6-4
6.3	Principles of Cyber Security	6-5
6.4	CIA Triad	6-6
6.5	Layers of Cyber Security	6-6
6.6	Vulnerability	6-7
6.6.1	Categories of Vulnerabilities	6-7
6.6.2	Causes of the Vulnerability	6-8
6.6.3	Types of Vulnerabilities	6-9
6.7	Vulnerability Management	6-10
6.7.1	Vulnerability Detection	6-10
6.7.2	Vulnerability Assessment	6-10
6.7.3	Vulnerability Remediation	6-11
6.8	Threat	6-11
6.8.1	Sources of Cyber security Threats	6-11
6.8.2	Comparison of Treat and Vulnerability	6-12
6.9	Security Attacks	6-12
6.10	Cyber Attacks (Harmful Acts)	6-13
6.11	Types of Cyber Attacks	6-13
6.11.1	Malware	6-14
6.11.2	Man-in-the-middle Attack (MITM)	6-14
6.11.3	Denial-of-service Attack	6-14
6.11.4	SQL Injection	6-14



6.11.5	Zero-day Exploit	6-15	6.20	Cyber Threats	6-24
6.11.6	Phishing	6-15	6.21	Cyber Warfare	6-24
6.11.7	Password Cracking	6-15	6.21.1	Types of Cyber Warfare Attacks	6-24
6.12	Internet Governance	6-15	6.22	Cyber Crime	6-25
6.13	Computer Criminals	6-15	6.23	Cyber Stalking	6-25
6.13.1	Causes of Cybercrimes	6-16	6.23.1	Examples of Cyber Stalking	6-26
6.13.2	Types of Cybercrimes	6-16	6.23.2	Types of Cyber Stalking	6-26
6.14	Assets and Threat	6-17	6.23.3	Protective Measures for Cyber Stalking	6-27
6.15	Categories of Cyber Attackers	6-17	6.24	Cyber Terrorism	6-27
6.16	Motive of Attackers	6-19	6.24.1	Categories of Cyber Terrorism	6-27
6.17	Types of Attacks	6-19	6.24.1	Examples of Cyber Terrorism	6-27
6.17.1	Passive Attacks	6-19	6.25	Cyber Espionage	6-27
6.17.2	Active Attacks	6-20	6.25.1	Cyber Espionage Tactics	6-28
6.17.3	Comparison of Active and Passive Attacks	6-22	6.25.2	Preventing Measures for Cyber Espionage	6-28
6.18	Software Attacks	6-22	6.26	Comprehensive Cyber Security Policy	6-28
6.19	Hardware Attacks	6-23	6.26.1	Cyber Security Policies.....	6-29
6.19.1	Devices Affected by Hardware Attacks	6-23	• Review Questions	6-30	
6.19.2	Motive of Hardware Attacks	6-24			

□□□


Tech Knowledge
 Publications