IoT : Mid Sem Short Notes

Module 1

Evolutionary Phases

i) Connectivity	Digitize Access	email, services, web
ii) Networked Economy	" Business	e comm, supply ch
iii) Immersive Experience	" Interaction	cloud, video, social
iv) IoT	" World	ppl, things, process

IoT : things
-> subset of IoE

Digitization (IoE) : Encompasses connectivity of things
-> data generated
-> business insights
-> convert info to digital

Industrial Revolution

4.0	IoT Integration (Today)	Sensors, Interconnectivity
3.0	Electronics & Control (E 1970)	Automated Production
2.0	Mass Production (E 20th)	Labor, Electricity
1.0	Mech Assistance (L 18th)	Water, Steam

Convergence of IT & OT

	OT	IT
operational Focus	24x7	Manage data, communication
Priorities	AIS	SIA
Types of Data	Monitor, Control, Supervise	Voice, Video, Trans, Bulk
Security	Control phy access	Authenticate users to N/W
Implication of failure	Direct impact	Can be business impacting
N/W upgrade	OP maintanence window	often
Security vulnerablity	Low	High

IoT Challenges

- Scale - Security - Privacy - BDA - Interoperability

Architectural Drivers

- Scale - Security - Device & N/W - Volume of data
- Support for legacy device - need for D.A.

IoT Arch

① -> one M2M

By ETSI in 2008 (Launded in 2012)

Accelerate adoption of M2M apps & devices

Goal: Common service layer - readily embedded in devices - allow comm with app servers. (Focus: IoT Services)

Challenge: Heterogeneity of device, S/W, Access Methods

↳ horizontal: interoperability

App Layer	Service Layer	N/W Layer
Auto. Appl. | Home | Energy	Common S.L	Apps talk to API to comm with sensors
→ Smart Energy	Comm. Tech & Ptcl	
→ Asset Track	Comm. N/W	
→ Fleet Manage	Comm. Devices & H/W	
	(support RESTful API)	

② → IoTWF $\boxed{\text{PCEC DDAC}}$

: 2014 by IoTWF Arch Committee = 7 layers ref model

IT	7 : Collab & People	- Involve ppl & business process
Query Rest	6 : App	- Report, Analyse, Control $\boxed{\text{RAC}}$
x Real	5 : Data Abstraction	- Aggregation & Access
↕	4 : Data Accumulation	- Storage
OT Event	3 : Edge Computing	- Data Elmt Analy & Trans $\boxed{\text{DEAT}}$
Motion	2 : Connectivity	- Comm & Processing Unit
Real Time	1 : Phy Dev & Controller	- Things

Achieve

→ Decompose IoT → Define a sys (diff vendors)

→ Diff Tech @ Each layer → Interop (Define interface)

→ Tiered security model

Simplified IoT Arch

Vertical Spe App	Core IoT Func Stack		IoT Data Mng & Compute
Analy	—— Application	Security ↕	Cloud
N/W Mgmt	—— Comm. N/W		Fog
N/W Trans Lay	Things		Edge
Gateway / Backhaul			
Access N/W			

Module 2

Sensor : Sense phy quantity → digital representation

→ Active / Passive → Invasive / Non → Contact / No

→ Absolute / Relative → Area of appl → How sensor measure / What

Actuators : Receives control signal → triggers a physical effect

→ Type of motion → PWR → Binary / Cont → Area of appl

→ Type of energy

Micro Electro Mechanical Sys (MEMS)

→ Integrate & Combine - Mechanical & Electric Elmt

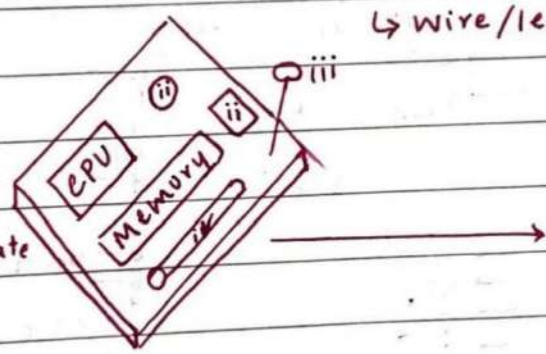
→ microfabrication technique (↑ Production ↓ cost)

Eg : InkJet Printers, SmartPhones, Airbag accelerometers

Smart Object

(i) Processing Unit (ii) Sensor, Actuator (iii) Comm Device (iv) PWR source

↳ microcontroller ↳ wire/less ↳ scavenger src



(WSN)
Low Memory
Lossy Comm
Narrowband Media
Moderate CPU PWR
PWR critical

Trends

Size ↓ Power

Processing ↑ Communicate

Sensor Network

i) **SANET**

→ diverse, heterogeneous, resource constrained Eg: Smart Homes

Adv : i) Greater Deployement Flex ii) Simpler scaling

iii) Low Cost iv) Easy maint. v) Effortless intro of new

vi) Better equipped - dynamic topology change

Disadv : i) ↓ Secure ii) ↓ Speed iii) ↑ impact by environment

ii) **WSN** (Design contraints in diag)

→ motes → no infrastructure

Comm Pattern : Event driven, Periodic

Adv : Self organize, Fault tolerance, reliability, ↑ life, optimise

Comm Ptcl (Consider these while choosing)

→ requirement of specific application, environment of WSN

→ Trade-offs the ptcl offers b/w PWR, speed, range, loss.

→ Overlay of autonomous techniques (self organise, healing, config)

IoT Hardware Platforms :

Building Blocks : Sensing, Actuating, Communication, Analysing

Interfaces : UART : Universal Asynchronous Receiver / Transmitter

SPI : Serial Peripheral Interface

I2C : Serial Clock Pin + Serial Data Pin

CAN : Message based Protocol

Arduino

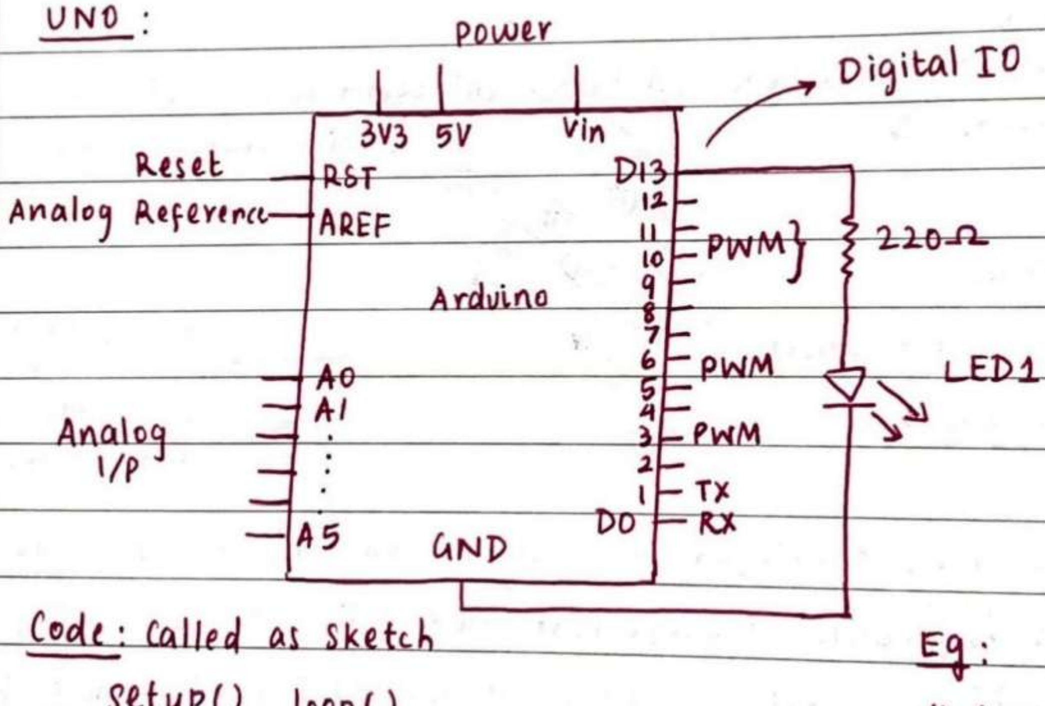
Printed Circuit Board (PCB), microcontroller chip is used → small computer-integrated circuit

To make apps, controls, adaptive env.

8-bit Microcontroller, 32-bit ARM, USB, Analog I/P, GPIO pins

Adv : ↓ cost, cross platform, simple, open src, extensible H/W & S/W

UNO :



Pulse Width Mod → PWM: 11, 10, 9, 6, 5, 3

SPI : 10 11 12 13

Serial : 0 1

Interrupt : 2 3

Code: Called as Sketch

setup(), loop()

Functions :

Digital : pinModel, digitalRead, digitalWrite

Analog: analogRead, analogWrite

Time : delay, millis

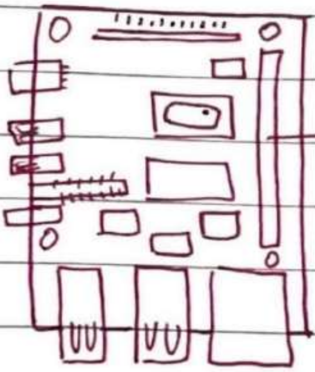
Maths: min, max, random

Eg :

```
#define LED-PIN 13
void setup()
{pinMode(LED-PIN, OUTPUT);}
void loop() {
  digitalWrite(LED-PIN, HIGH);
  delay(1000);        1 second
  (   , LOW);
}
```

Raspberry PI:

Low Cost mini computer, Linux flavours



	1	2	
SDA	3	4	
SCL	5	6	Ground
	7	8	Tx
Ground	9	10	Rx
	11	12	
	13	14	Ground
	15	16	
	17	18	
MOSI	19	20	Ground
MISO	21	22	
SCLK	23	24	CE0
Ground	25	26	CE1
	27	28	
	29	30	Ground
	31	32	
	33	34	Ground
	35	36	
	37	38	DIN
Ground	39	40	DOUT

Interfaces

Serial → Rx Tx

SPI → MISO, MOSI, SCK, CE0, CE0

I2C → SDA - data line, SCL - clock line

Ground : 6 9 14 20 25 30 34 39 (8)

GPIO : 3 5 7 8 10 11 12 13 15 16 18 19 21 22 23 24 26 27 28 29 31 32 33 35 36 37 38 40 (28)

3V3 Power : 1 17 (2)

5V power : 2 4 (2)

Commands :

Raspi-config . StartX, Ifconfig, SSh , Sudo , config.txt

Module 3

Communication Criteria

Range, Freq Band, Pwr, Topology, Constrained Devices, N/W.

class 0, 1, 2

Access Technologies

→ Standardization + Alliances → PHY → MAC

→ Topology → Security → Competitive Tech

IEEE 802.15.4

→ Low cost, Low Data Rate, Easy Install

→ Home Automation, Automotive N/W, WSN, Toys

Disadv : MAC reliability, unbounded latency, interference

↳ CSMA/CA, wait time ↳ freq hopping

Multipath fading : Multiple copies of signal hitting

① Low Rate PHY, MAC layer in WPAN

Eg: ZigBee, 6LoWPAN, ZigBeeIP, Thread

② 2.4 GHz to sub-GHz in ISM based on ~~B~~DSSS

Preamble	Start of Frame Delimiter	Frame len	PHY SDU
← 5 →		← 1 →	← 0-127 →

← 6 → (Preamble to Frame len)

③

Frame ctrl	Seq Num	Dest PAN Num	Dest Addr	Source PAN	Src Addr	Payload	Frame check seq
2	1	← 4 - 20 →					2

④ Star, P2P, Mesh : min one FFD as PAN coordinator

↳ Full Func Device

⑤ Adv Encryp Standard (AES) : Src Add, Aux Security Header, Payload : 128-bit key

$\underbrace{\text{Aux Security Header}}_{0-14\text{ B}}$

⑥ DASH7 - RFID, military, radio waves, 1 mile, AES

IEEE 802.15.4 g/e

MAC PSDU ⇒ 0-2047 B, Mesh, AES

Frame Ctrl	Seq Num	Addr Fields	Aux sec Header	Info Elmt	Frame payload	FCS
2	1	4-20		VAR		2/4

IEEE 1901.2a

NB-PLC : NarrowBand Power Line Communication

→ x reliable, manage, interop. → wireless Tech → MIC

MAC

Sgmt ctrl	Frame ctrl	Seq Num	Addr field	Aux Sec Head	Info Elmt	Frame Payload	FCS
3	2	1	0/20	0/5/6/10/14			2

IEEE 802.11ah

→ unconstrained N/w, be able to connect endpoint

→ ★ topology (2 hops, relay function)

→ supports large no of devices

LoRAWAN

→ Unlicensed LPWA technology

→ low data rate, demod below noise floor

→ LoRa Gateway acts as central hub

→ Spreading Factor

App				
COAP	MQTT	IP V6/ 6LOWPAN	Raw	Others
LoRAWAN MAC				
PHY				
868 MHz	915	Other Bands		

MAC

Header	Payload	Mess. Integrity Code
1		4

→ messages : Join Req, Join Acc, Confirm, Unconfirm, Up, Down

6

→ star of stars topology → AES, ABP, OTAA

Module 4

Advantages of IP

i) Open ii) versatile iii) Ubiquitous iv) Scalable
v) Manageable, Secure vi) Stable, Resilient vii) Adoption
viii) Innovation

Need for optimisation

i) Constrained Nodes
- communicate thro unreliable path
- limited throughput, low convergence
→ Very constrained in RSRC, infreq comm, limited security, mngt
→ Enough pwr & capacities → stripped down IP / Non IP stack
→ |||^{l} to generic PC, constrained N/W capacity

ii) Constrained N/W
- Past: Low Speed Modems but now
- tech with low B/W, distance, pwr, n/w services
→ high latency, high potential for packet loss
Low power & lossy N/W (LLN)
- PDR (Packet Delivery Rate) keeps oscillating

Optimizing IP

Transport : TCP/UDP
N/W : IPv4/IPv6
Adaptation ⟶ RFC : Req For Comments
Data Link : 802.14.4g
Physical : Wire/less

6LoWPAN to 6Lo

Adaptation Layer : Model for packaging IP into lower layer ptcl
6LoWPAN : Optimize transmission of IPv6 packets over C.N/W

HTTP	RTP	
TCP	UDP	ICMP
IP		
MAC		
Ethernet PHY		

APP Ptcl	
UDP	ICMP
IPV6	
LoWPAN	
IEEE 802.15.4 MAC	
PHY	

RFC 4944 - foundational

Header Stacks :

802.15.4 Header   IPV6 Header compression   IPV6 Payload

Frag Header

Mesh Addressing Header

Steps :

i) Header compression : IPV6 40 byte → 6 byte (stateless)

UDP 8 byte

• 1 - 40 - 8 - 53 • ⇒ • 2 - 4 - 108 •

ii) Fragmentation : Datagram size, Tag, Offset (1-2-1)

MTU = 1280 bytes min (Size of largest Ptcl data unit)

iii) Mesh Addressing

Forward Packets over multiple hops.

→ Src Add, Dest Addr, Hop Limit (1-2-2)

Mesh-Under : Routing @ 6LoWPAN Adaptation Layer

Mesh-Over : IP routing

many link layer hops → one IP hop terminated by edge gateway

6Lo

↳ IPv6 over N/W of Resource Const. Nodes

RPL : Routing Ptcl for LLN

was published by

RoLL : Routing over LLN

→ Each node - router - part of mesh N/W

RPL : DAG, DoDAG

Cons. Nodes

configured using DIO

Storing   Non storing

→ upto 3 parents

→ no loop

→ upward

DAG : Directed Acyclic Graph

DODAG : Destination Oriented DAG

DIO : DAG Information Object

OF : objective Function defines how metrics are used to route & establish

Rank : How close node is to the root

RPL Headers : N/W Layer header for datagrams

Leverage Data-Plane packets for loop detection

Metrics : 8

ETX, Hop Count, Latency, Link Quality Level, Link Color,

Node State & Attr, Node Energy, Throughput

Module 5

Transport Layer :

For TCP/IP → TCP, UDP

TCP (Transmission ctrl)	UDP (User Datagram) → IoT
Connection Oriented	Connectionless protocol
Session established before tran.	Quickly send, no guarantee
Like phone call	Like mail, music, VoIP
Large data - small packets	N/W Services like DNS
Correct seq, Flow ctrl → SLOW	Performance, Latency ✗ → Fast
Reliable (3 way handshake)	Not reliable
Header : 20 bytes	8 bytes

Transport methods :

→ App. Layer Ptcl not present : class 0, smart objects

→ SCADA

→ Generic Web Based Ptcl

→ IoT App. Layer Ptcl

Data Broker : Piece of middleware that standardizes sensor O/P into a common format that can then be retrived by authorized applications.

SCADA : Supervisory Control & Data Acquisition

- Automation Control System
- well structured running over physical, data link layers
- High lvl : collect sensor data & telemetry, control them
- Now : Global, Real-time, data driven decisions
- Used : Utilities & Manufacturing/Industrial Vehicles
- Eg : Modbus & variants - Master/slave relationship

Adapting SCADA

DNP3 - master/slave = Port 20000

master → powerful computer

slave → remote device (outstations)

Protocol Stack for Transporting Serial DNP3 SCADA over IP

	Master		Outstation	
App. Layer Fragment	DNP3 App. Layer	<- - logical comm - ->	DNP3 App. Layer	} DNP3 ptcl
Transport Segment	DNP3 Trans. Func.		DNP3 Trans. Func	
Link Frame	DNP3 Data Link Layer		DNP3 Data Link Layer	
	Conn. Mgmt		Conn. Mgmt	IEEE 1815 Section
TCP/UDP	Transport	<- - - - - - - ->	Transport	} IP Layers
IPv4	N/W		N/W	
	Data Link physical		Data Link physical	
	↕	IP N/W	↕	

Dual End pt : Process that can both listen for conn. req, perform active open on the channel if required

Tunneling Legacy SCADA over IP Networks

→ Flexibility needed → ideally IEEE 1815-2012 is used in DNP3

→ else tunnel over raw socket over TCP/UDP

→ or intermediate device to do protocol translation

Protocol Translation

→ alternative to raw socket conn for transporting legacy serial data

SCADA Transport over LLN with MAP-T

↳ Mapping of Addr & Port using Transl. RFC 7599

Generic : HTTP/HTTPS, XMPP

Scenarios in SCADA :

A : Raw Socket b/w Routers

B : " Router & SCADA, IP/Serial Redirector S/W, Ethernet interface

C : " " , SCADA knows to directly comm over " .