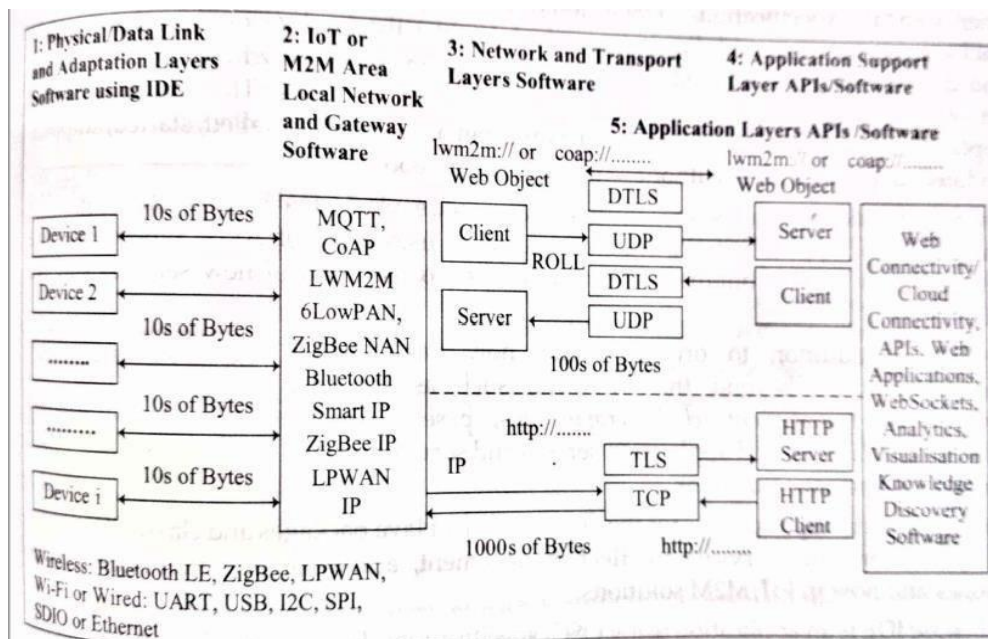


Sub:	IoT&WSN					Sub Code:
Date:	28/12/2021	Duration:	90 Minutes	Max Marks:	50	Sem / Sec:

Answer any FIVE FULL Questions

1	<p>Explain the about vulnerabilities in WSN and also explain the address management in IoT. [10]</p> <p>Insecure web interface Insecure web interface can lead to problems like SQL injection, cross-site scripting, cross-site request forgery, command injection, weak passwords.</p> <p>Insecure network services</p> <ul style="list-style-type: none"> ➤ It includes debugging services, diagnostics sevices, testing services. ➤ In secure network services can lead to problems like insecure storage of sensitive data (location, images, PII, PHI etc). <p>Ineffective authentication/authorization <i>Authentication vulnerabilities includes:</i> User enumeration weak passwords, Brute force attacks, weak session management.</p> <p>An absence of transport layer encryption If your IoT device sends private data over an insecure protocol, it is in cleartext, and as a result, anybody can read it. This only underscores the importance have secure communications protocols with these devices.</p> <p>Privacy issues If the data on the IoT device is not encrypted, and other individuals have access to it, this makes your data vulnerable to covert hijacking and theft.</p> <p>Inadequate security features</p> <ul style="list-style-type: none"> ➤ Many times, IoT device may not have the security features built into them as it is claimed to be. ➤ As a result, there are no encryption options or features to detect and monitor any potential Cyber-attacks. <p>Insecure network traffic (free Wi-Fi (wireless) network)</p> <ul style="list-style-type: none"> ➤ It means there's no special login or screening process to get on the network, which means you and anyone else can use it. ➤ It can lead to weak authentication of the client side, on the server side, Lack of encryption, Replay attacks, relying of “unknown” or “hard to understand protocols” <p>Insecure device firmware</p> <ul style="list-style-type: none"> ➤ Firmware is used in managing interactions between the hardware and the higher-level software used to configure, manage and operate the device e.g. wireless routers, ➤ copiers, printers and cameras. ➤ Insecure device firmware can lead to the data can be stolen or modified i.e. sending data without encryption and devices taken control of for the purpose of attacking other devices <p>Address Management:</p> <ul style="list-style-type: none"> · Name: Denote/refer to “things” <ul style="list-style-type: none"> · Nodes, networks, data, transactions, ... · Often, but not always, unique (globally, network-wide, locally) · Addresses: <u>Information needed to find these things</u> <ul style="list-style-type: none"> · Street address, IP address, MAC address · Often, but not always, unique (globally, network-wide, locally) · Addresses often hierarchical · Services: to <u>map between names and addresses</u> <ul style="list-style-type: none"> · E.g., DNS · IP addresses are prominent examples
2	<p>Explain with neat sketch five levels for software development for application and services for IoT and M2M [10]</p> <p><u>Devices, Gateways, internet and web/cloud services, software-development are five levels of software development required</u> for applications and services in IoT/M2M. Main devices are:</p>

- 1) Physical/data Link and adaptation layers software
- 2) IoT/M2M area local network and gateway software.
- 3) Network and transport layer software
- 4) Application support Layer APIs/Software
- 5) Application layers APIs/Software



3 What is IoT security Tomography? Explain Layered attack model and possible attack at each layer [10]

Tomography: It means producing 3D picture of internal structure of an object by observation and recording.

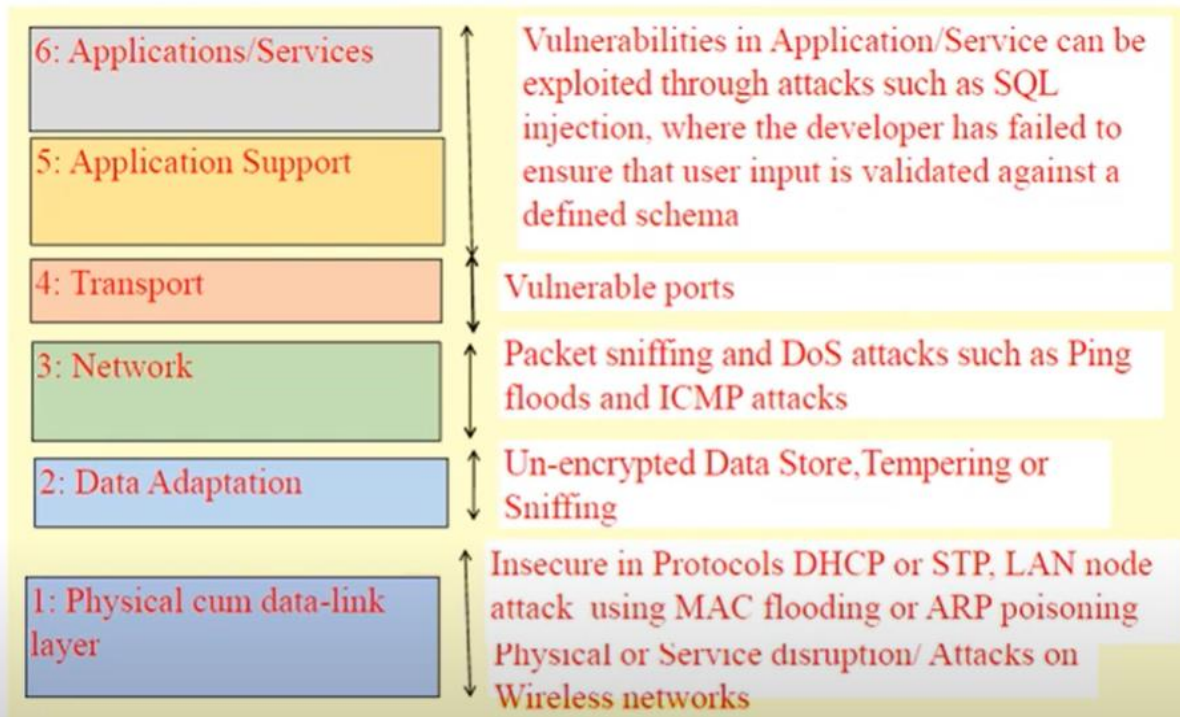
Network tomography

- It refers to the study of vulnerabilities and security aspects for network monitoring in complex system such as RFID, WSN or IoT networks.
- It also helps in observing each network section.

Security Tomography:

It enables finding the attack vulnerable sections/subsections on observation for behaviors using finite number of objects or threats in a complex set of subsystems

LAYERED ATTACKER MODEL:



- 4 Explain security requirements and threat analysis in WSN [10]
 Security functional group contains five sets of functions which are required for ensuring security and privacy. Five functional components of security are defined in IOT are:
- 1) Identity management
 - 2) Authentication
 - 3) Authorization
 - 4) Key exchange and management
 - 5) Trust and reputation

Identity Management:

- An object's identity should always be unique compared to the other objects from its family.
- Unique identity can be called core identity, as an object can also have several temporary identities.
- Devices must establish their identity before they can access gateways and upstream services and apps.
- An object should know the identity of its owner if it exists.

Secure Authentication/Authorization

- IoT devices should be authenticated with strong usernames, IDs and password before being allowed to communicate with other IoT devices on the network.
- Authentication token/session should always be unique to each user along with user id, app id and device id.
- System's credentials, application, device and server should be authenticated as spoofed devices could transmit malicious data to other devices and can implement a denial-of-service attack on the IoT network.

Key exchange and management

- Public key cryptography also known as asymmetric encryption keeps the data safe and secure during transmissions.
- In a public key encryption system, any person can encrypt a message using the receiver's public key. That encrypted message can only be decrypted with the receiver's private key.
- **Certification Authority (CA):** This is effectively done by issuing a digital certificate to confirm the authenticity of the device, firmware / software updates, and facilitate encrypted communications.

Trust and reputation

Trusted IoT Device:

The trusted IoT devices should be able to communicate with the intended hosting services only.

And the firmware / software should be frequently updated.

The Trusted IoT Master:

A trusted master must provide a secure communication with dependent sensor devices, and issue

5 Explain about Arduino platform and write a program for displaying traffic light. [10]

```

int internalLED = 13; // indicating successful running
/* Variables are written using a lower case first character */
int ledR0, ledY0, ledG0, ledR1, ledY1, ledG1, ledR2, ledY2, ledG2, ledR3,
ledY3, ledG3;
Assign the pins to the respectively connected LEDs */
ledR0 = 2; ledY0 = 3; ledG0 = 4; ledR1 = 5; ledY1 = 6; ledG1 = 7; ledR2 = 8;
ledY2 = 9; ledG2 = 10; ledR3 = 11; ledY3 = 12; ledG3 = 14;
/* Declare Functions for sequences of traffic lights ON-OFF as follows: */
void north_south_Green() {
digitalWrite (ledR0, LOW); digitalWrite (ledY0, LOW); digitalWrite (ledG0,
HIGH);
digitalWrite (ledR2, LOW); digitalWrite (ledY2, LOW); digitalWrite (ledG2,
HIGH);
};
/* Function Switch RED ON for East and West pathways*/
void east_west_Red() {

```

```

digitalWrite (ledR1, HIGH); digitalWrite (ledY1, LOW); digitalWrite (ledG1,
LOW);
digitalWrite (ledR3, HIGH); digitalWrite (ledY3, LOW); digitalWrite (ledG3,
LOW);
};
/*****
void setup () {
/* GPIO pins 2 to 12 and 14 are thus assigned port numbers corresponding to 12
external LEDs, R0, Y0, G0, R1, Y1, G1, R2, Y2, G2, R3, Y3, and G3.*/
/* Assign mode of each pin as output */
pinmode (ledR0, OUTPUT); // Constants are written in Upper Cases
pinmode (ledY0, OUTPUT);
pinmode (ledY3, OUTPUT);
pinmode (ledG3, OUTPUT);
/* Let Pin 13 be used for indicating successful running of the developed codes
during testing phases. Initialise internal Port 13 Digital IO Pin LED for
test.*/
pinmode (internalLED, OUTPUT);
/* Initialise start of the Board and Sequences. */
digitalWrite (internalLED, HIGH);

```

```

/* Display the settings of Digital IO pins at serial display-monitor on the
computer where IDE is setup. */
/*Let UART mode baud rate = 9600*/
Serial.begin (9600);
Serial.println ("Arduino project.Program for controlling three traffic signals-
Red, Yellow and Green at four pathways");
Serial.println ("Arudino board LED glows when cycle starts for the sequences of
lights turning high and turns off for brief interval in order to indicate the
successful completion of the cycle");
Serial.println ("Twelve 12 external LEDs, R0, Y0, G0, R1, Y1, G1, R2, Y2, G2,
R3, Y3, and G3 corresponds to 12 traffic lights at north, east, south, west
")
}
/*****
Step: Loop function which endlessly runs
void loop () {
/* Assume no right turn from pathways or left turn from pathways permitted, just
for simplicity and for learning the basics. */
/*Switch Green ON for North and South pathways */
/*Switch RED ON for East and West pathways*/
// Run Functions

```

6 Explain how the data is read from sensors and also explain passive clustering. [10]

- 1) Sensors senses the analog data and send the analog data to 10 bit ADC (Analog to digital converter).
- 2) ADC send the 10 bit parallel data to PISO converter.
- 3) Parallel IN serial out (PISO) converter converts parallel data to serial data.
- 4) This serial output connects to SPI (Serial Peripheral Interface) Pin of Arduino board.
- 5) For example let sensor senses the temperature of 100 degree.
- 6) ADC converts 100 degree to binary 111111111, which is send to PISO then to SPI of arduino

Passive Clustering:

Only the necessary information is exchanged by adding state information about each sender in the packet like "initial", "clusterhead", "gateway", "ordinary node".

For example:

- Whenever a node start a broadcast it is stamped as in "Initial node".
- The first nodes receiving and forwarding the packet is considered as clusterhead.
- Any initial nodes receiving the packets will turn into ordinary/gateway nodes.
- A node that first claims to be a clusterhead rules the rest of nodes in its clustered area.

7 Explain Various aspects of Energy -Efficient unicast

- In ad-hoc routing packets are forwarded to destination nodes by wireless node-to-node communication.
- It is critical to reduce the electric energy consumption of nodes since nodes work by using the electric battery.
- Since the main goal is Energy efficiency, hence various aspects can be considered which creates an energy-efficient route from a source node to a destination node by selecting nodes which consume

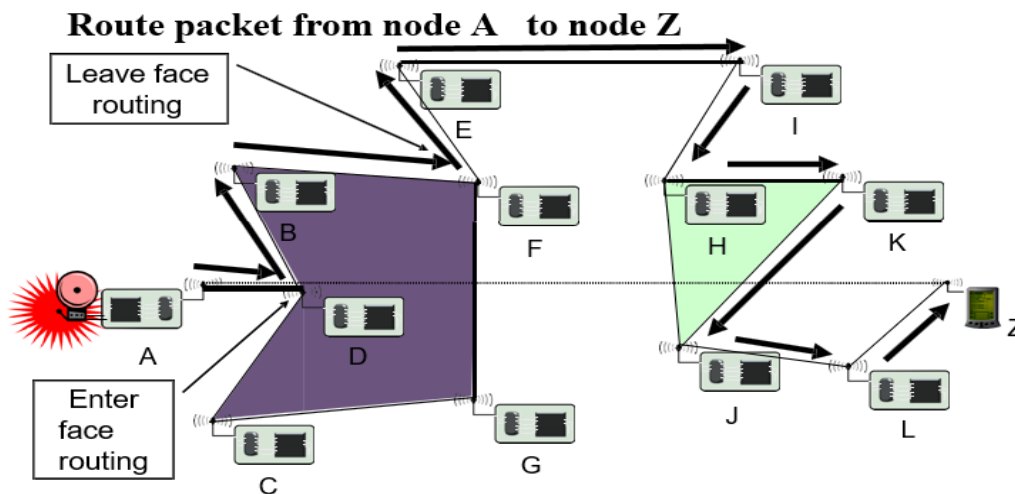
smaller energy.

- Minimize energy per packet (or per bit)
- Maximize network lifetime
- Routing considering available battery energy
 - Maximum total available battery capacity
 - Minimum battery cost routing(MBCR)
 - Min-Max Battery Cost Routing(MMBCR)
 - Conditional Max-Min Battery Capacity Routing(CMMBCR)
 - Minimize variance in power levels.

8. Explain about Right-Hand Rule to recover Greedy Routing (GPSR)

- GPSR forward the packet as long as possible using greedy forwarding with “most forward rule”.
- If no progress possible: Switch to “perimeter” routing
- **Perimeter: Set of nodes defining the face**
- **Face:** it is largest possible region of the plane that is not cut by any edge of the graph; can be exterior or interior.
- Perimeter sends the packet around the face using right-hand rule.
- For this the packet carries information that where it has to enter a given face.
- The node and the connecting line between it and the destination decides whether the packet should leave the face and proceed to the next one.
- Also packet can, switch back to greedy routing

GPSR – Example



- A packet is routed from node A to node Z where node A is the source and node Z is the destination.
- The packet can be greedily forwarded to node D
- But at node D the dead end is there, hence is avoided.
- Hence the packet has to be routed around the perimeter of the interior face defined by BFGCD
- Now the packet is forwarded from node B to F.
- And from F it will be routed around perimeter of exterior face i.e. Via node E to I to H and then to node K to J and from J to L then to destination node Z.
- Faced based procedure is applied to planer graphs.