CGC COLLEGE OF ENGINEERING
Building Careers. Transforming Lives.

CGC College of Engineering
Department of CSE

AWSN (BTCS-716-18)

Assignment-2

Given Date: 13.10.2025 **Submission date: 17.10.2025**

Q. No.	1	2	3	4	5	Total Marks
Mapped CO	CO5	CO4	CO5	CO3	CO4	
Max Marks	2	2	2	2	2	10
Marks Obtained						

Submitted To:

Dr. Pardeep Singh Tiwana

Submitted By:

Student Name :Manpreet Singh

Roll No:2220980

Branch / Section: CSE / V

Q1 -> Assess the effectiveness of different defense mechanisms against flooding Attacks and Justify which Approach provides the Best Protection.

Ans Flooding attacks in adhoc and wireless sensor network are denial-of-services (DoS) attacks where malicious nodes continuously send excessive packets to exhaust network resources such as bandwidth, energy, and memory. These attacks degrade network performance, disrupt routing, and reduce the lifetime of sensor nodes. To counter them, several defense mechanisms have been proposed.

Approach:
- -> Rate-limiting Technique
- -> Authentication-based defense
- -> Trust-based system.
- -> Statistical anomaly detection.

Among these, authentication-based mechanisms provides the most reliable protection, as they ensure that only verified nodes can participate in network communication.

Q2 -> Key issues and challenges involved in meeting security Requirements during Network Provisioning.

Ans Network provisioning in ad hoc and wireless sensor network (WSNs) involves configuring and establishing network resources, routes and security parameters for communication. However, meeting security requirements during this phase represents several challenges due to the unique characteristics of these networks, such as limited energy, dynamic Topology and lack of centralized control.

- -> Authentication
- -> Key management
- -> Confidentiality.

-> data integrity.

Q3-> Define Key Distribution and Management in Network Security

Ans Key distribution->
-> Process of securely sharing cryptographic key among users or devices.
-> methods: Manual -> Physically or verbally shared
Automatic -> Using Protocol, KDCs or PKI for secure delivery.

Key Management ->
-> Handling the life cycle of keys securely
-> Key activities
-> Generation: Strong creating, random key
-> Storage: securely storing key (eg HSMs)
-> Usage: Controlling Purpose-Specific key usage
-> Rotation/Expiration: Regularly updating keys
-> Revocation: Invalidating compromised or unused key
-> Destruction: securely deleting old key.

Q4-> Demonstrate how Transport layer solutions, such as TCP are applied in Ad hoc wireless network to ensure reliable communication?

Ans In Ad-hoc Wireless network reliable communication is challenging due to high error rates, dynamic Topology, variable delays and shared wireless medium. Thus TCP designed for wired network ensure reliability using segmentation, sequence number & acknowledgement. This mechanisms allow the receiver to detect lost or corrupted packet and ensure data is delivered correctly. However in AWNs TCP can misinterpret Packet loss caused by mobility or wireless error as

congestion, reducing performance. To address this, enhanced TCP variants (e.g. TCP-W, TCP-ELFN) and cross layer solution inform TCP about link failures preventing unnecessary congestion control actions.

Q5 -> Analyze the components and working of the SPINS security protocol to explain how it ensure data confidentiality and authentication in sensor Network.

Ans The SPINS security protocol ensures data confidentiality and authentication in sensor network through two main components

SNEP
μTESLA

SNEP provides confidentiality by encrypting communication using symmetric key cryptography and ensures integrity and authentication with message authentication codes (MACs). This protects data from unauthorized access and Tampering

μTESLA is designed for secure broad cast authentication introducing delayed disclosure of symmetric keys to allow lightweight, efficient authentication of broad cast message, which is essential for Sensor Networks, By combining this feature SPINS manges to deliver robust security with low computational and energy required making it ideal for resource constrained environment like sensor network, where both confidentiality and authenticated communication are critical.