COLLEAGUE OF COMPUTING COMPUTER SCIENCE

Wireless Communication and Mobile Computing Assignment

Prepared by:

NAME……ID. NO.

Ajmel abes 29770/14

instructor: Takelign tujo

Date: December 2024

Question 1: Fundamentals of Wireless Communication

1. Define wireless communication and explain its key components

- **Answer**
    - Wireless communication is the transfer of information between two or more points that are not physically connected. It uses electromagnetic waves, such as radio waves, microwaves, infrared, or even visible light. It eliminates the need for traditional wired infrastructure, enabling mobility and flexibility.
    - **Key components of wireless communication:**

1. **Transmitter:**
    - Converts the input data into a signal suitable for transmission.
    - Include a modulator to encode the data and an antenna to send the signal over the air.

2. **Receiver**
    - Captures the transmitted signal through an antenna.
    - Demodulate and decode the signal back into the original data.
3. **Channel**
    - The medium through which wireless signals travel, such as air, vacuum, or water.
4. **Antenna**
    - Actes as the interface between the electromagnetic waves in the channel and the electrical signal in the transmitter /receiver
    - Used for both sending(transmitting) and capturing (receiving) signals.
5. **Modulation/Demodulation**
    - Modulation: the process of converting data into a format suitable for transmission (e.g. amplitude, frequency, or phase modulation).
    - Demodulation: the process of extracting the original data from the received signal.
6. **Signal processing**
    - Enhance the quality of the signal and filter noise, and correct errors during transmission and reception.
7. **Protocol**
   Define the rules and standards for communication, such as timing, error handling, and data formats(e.g. Wi-fi, Bluetooth, or LTE protocols).
8. **Power supply**
    - Provides the necessary energy for the transmitter, receiver, and associated circuitry. In mobile devices, this is typically a battery.
9. **Frequency bands:**

- Wireless systems operate on designated frequency ranges, regulated by authorities like the FCC (Federal Communication Commission). Examples include ISM bands (for Wi-fi and Bluetooth)or licensed bands(for cellular networks).

2. **Discuss the advantages and limitations of wireless communication.**
    - **Answer**
    - **Advantages of Wireless communication**
        1. **Mobility:**
            - Wireless communication allows users to remain connected while on the move, enabling greater flexibility and convenience.
            - Examples include mobile phones, laptops with Wi-fi, and IoT devices.
        2. **Easy of installation:**
            - Wireless networks do not require extensive wiring, making them easier and faster to set up, especially in remote or temporary locations.
        3. **Cost**
            - Eliminating the need for physical cables reduces installation and maintenance costs.
            - It is especially beneficial for large or dispersed environments.
        4. **Reliability**
            - The absence of cables and wires reduces the risk of communication failure caused by physical damage, environmental conditions, or wear and tear of metallic conductors
            - This ensures connectivity over time.
        5. **Disaster Recovery**
            - **Wireless systems are less affected by disasters such as fires, floods, or accidents.**

    - **Disadvantages of Wireless Communication**
        1. **Interferences:**
            - Wireless signals are susceptible to interference from other devices, physical obstruction(e.g., walls(, and environmental factors like weather
            - The best example is Bluetooth and Wi-Fi (WLAN). Both these technologies use the 2.4GHz frequency for communication and when both of these devices are active at the same time, there is a chance of interference.
        2. **Security:**

- Wireless communication is more prone to unauthorized access, eavesdropping, and hacking.
- Requires robust encryption and authentication mechanisms to protect data.

3. **Health concerns**
    - Continuous exposure to any type of radiation can be hazardous. Even though the levels of RF energy that can cause the damage are not accurately established, it is advised to avoid RF radiation to the maximum.

Question 2: Cellular Network Architecture

1. Describe the structure and working of a cellular network, highlighting the role of Base Transceiver Stations (BTS) and Mobile Switching Centers (MSC).
    - **Structure and working of a cellular network**
        - A cellular network is a wireless network divided into smaller areas known as cells. Each cell is served by one BTS, which provides the coverage and manages the communication within its area. The cells together form a big network so that mobile devices can communicate while moving across different locations.
        - **Structure of a cellular network:**
        - Cell:
            - The basic unit of a cellular network, each covering an area.
            - Cells use different frequencies to avoid interference with other cells.
        - Base Transceiver Station (BTS):
            - Located at the center or edge of each cell.
            - Connects mobile devices to the network infrastructure.
            - Handles signal transmission, reception, and modulation.
        - Mobile Switching Center (MSC):
            - The central part of the cellular network connects multiple BTSs.
            - Manages call routing, handovers, and connections to external networks like PSTN or the Internet.
        - Backhaul Network:
            - The infrastructure connecting BTSs to MSC is usually via fiber optic or microwave links.
        - Mobile Devices
            - User equipment such as a smartphone communicates with the BTS in the coverage area.
        - Core Network:

        - The brain of the cellular network, handles data routing, subscriber management, and internet connectivity.
    -
- **Working of a cellular network:**
    - How a Cellular Network Works:
    - Establishing Communication:
        - When a mobile device is powered up, it registers itself with the nearest BTS depending on the strength of the signal.
    - Call Setup:
        - BTS forwards the call to MSC.
        - MSC sets up a call between the caller and the called.
    - Data Transmission:
        - Voice or Data is wirelessly transmitted between the mobile devices and BTS
        - BTS transmits this data to MSC, which routes the data
    - Handoff:
        - If the user is moving from one cell to another MSC initiates a handover to keep the communication continuous by switching his connection to the new BTS
    - Connectivity with Other Networks:
        - MSC connects the calls or data sessions to external networks like PSTN or the internet.
    - Subscriber Management:
        - The network authenticates the user and keeps track of the services used for billing, location, and roaming.
- **Role of key components Key Components:**
    - Base Transceiver Station (BTS)
        - It transmits and receives radio signals to and from all mobile devices in its cell.
        - All modulation, encoding, and power control are performed here.
        - The interface between the user and the cellular network.
    - Mobile Switching Center (MSC)
        - Central control for more than one BTS.
        - Routes calls, manages handovers, and connects to external networks.
        - Manages subscriber data, such as phone numbers, authentication, and billing.

2. Compare and contrast 3G, 4G, and 5G network architectures

Feature	3G(third generation)	4G(fourth generation)	5g(Fifth Generation)
Introduction	The early 2000s	Late 2000s to early 2010s	2019 onwards
Core network	• Circuit-switched for voice and Packet-Switched for data. • Relies on UMTS and HSPA for connectivity	• Fully Packet-Switched. • Introduction of Evolved Packet Core for seamless voice and data	• Service-Based Architecture (SBA). • Natively integrated cloud technologies for ultra-low latency and scalability
Base station	• Node B(traditional architecture)	• Evolved node B(eNodeB) with enhanced data handling	• Next-generation Node B(gNodeB) with advanced beamforming and MIMO capabilities.
Frequency bands	850MHz to 2100MHz	700MHz to 2.6GHz.	Sub-6 GHz and mmWave(24GHz and above)for faster speeds.
Speed	Up to 2 Mbps	Up to Gbps	Up to 10 Gbps and beyond
Latency	50-200 ms	20-30 ms	Less than 1 ms in ideal condition
Bandwidth	• Narrowband spectrum limited capacity.	• Wider bandwidth for higher data rates.	• Massive bandwidth for enhanced capacity and ultra-high speed.

Mobility	• Designed for moderate mobility(e.g., vehicular speeds)	• Improved mobility for high-speed travel.	• Excellent mobility for high-speed trains and dense urban areas.
Network elements	• RNC between core and BTS. • It is based on hierarchical architecture.	• Flat IP-based architecture with no RNC. • It concentrates on the seamless flow of data.	• Distributed architecture with edge computing. • The main emphasis is on latency reduction and incorporation of AI
Application	• Light web browsing, emails, video calls.	• HD Video streaming, VoIP, and mobile apps.	• IoT, AR/VR, smart cities, and autonomous vehicles.

Key Differences and Improvements:

1. **Architecture Shift:**
   - 3G used both circuit and packet switching.
   - 4G had an all-IP architecture, which made communication much simpler and allowed seamless data services.
   - 5G uses service-based and decentralized architectures with the integration of edge computing for ultra-low latency.
2. **Performance:**
   - 3G supported basic internet usage with limited bandwidth and high latency.
   - 4G introduced HD streaming and faster browsing with major improvements in speed and latency.
   - 5G unleashes next-generation applications IoT, autonomous vehicles, and real-time AR/VR with unparalleled speed and responsiveness.

3. **Technology Integration: Performance:**
    - 3G used WCDMA and HSPA for connectivity.
    - 4G began to implement LTE and its upgraded version, LTE-Advanced.
    - 5G integrates massive MIMO, beamforming, and mmWave for superior performance.

Question 3: Medium Access Control (MAC) in Wireless Networks

- **Explain the role of Medium Access Control in wireless networks.**

MAC stands for Medium Access Control; it plays a very major role in the Data Link Layer of an OSI model. It is basically responsible for governing multiple devices using the wireless medium. Since many wireless networks operate devices over the same spectrum, it's the MAC layer that does the significant and efficient, conflict-free transmission of data reliably.

Major MAC Roles in Wireless Network

1. Collision Avoidance:
    - A collision is likely to happen in wireless communication due to the shared usage of the medium.
    - MAC protocols that depend on sensing of the medium - CSMA/CA for instance reduce the chances of collision before the actual transmission of data.
2. Efficient Channel Allocation
    - The MAC layer decides how devices share the communication channel.
    - Techniques such as Time-Division Multiple access(TDMA) and Frequency-Division Multiple Access(FDMA) are used to allocate resources efficiently.
3. Data Framing and Addressing:
    - It frames the data for transmission, adding addressing information so that the data may reach the intended receiver.
    - Handles the frame synchronization so that the data is not corrupted.
4. Access Control:
    - Ensures, at any given time, which device can use the medium to avoid conflict and have orderly communication.
5. Quality of Service (QoS):
    - Ensure that applications requiring real-time processing, such as video streaming or voice calls, get prioritized access,
    - Balance the network traffic so that it can satisfy QoS demands.

6. Power Management:
    - Reduce battery power in a wireless network
    - Device to save the battery power and may be driven into the low power state in which it will not send nor receive any data.
7. Error Detection and Retransmission:
    - Detects and corrects the frame-level errors.
    - It initiates retransmission for lost or corrupted data to ensure reliability.
8. Security Enforcement:
    - Provides the ability to implement network security by supporting authentication, encryption, and access control protocols.

- **Differences Between CSMA/CD and CSMA/CA**
  The Carrier Sense Multiple Access with Collision Detection, or CSMA/CD, and Carrier Sense Multiple Access with Collision Avoidance, or CSMA/CA, are the protocols used to manage access to a shared communication medium. Both of these share some principles in common, yet they were designed for different types of networks and handled the collisions differently.

Aspect	CSMA/CD	CSMA/CA
purpose	Detect and handle collisions after they occur.	Avoid collisions before they occur
Primary use	Wired networks (e.g., ethernet).	Wireless networks(e.g., Wi-fi).
Collision Handling	• Detects collisions during data transmission. • Stops transmitting and retries after a random delay.	• prevent s collisions by ensuring the medium is clear before transmission. • Uses acknowledgment to confirm successful delivery.
Detection mechanism	Relies on the ability to sense electrical signals on the cable to detect collisions.	Cannot detect collisions due to the hidden node problem; instead, avoids them.
Medium checking	Check the medium (carrier sensing) before and during transmission	Check the medium(carrier sensing) only before transmission.

Efficiency	More efficient in wired networks with low latency and minimal interference.	More effective in wireless networks prone to interference and hidden nodes.
Mechanism for avoidance	Collision avoidance None; relies on detection and retransmission.	Such techniques like Request to Send (RTS) and Clear to Send (CTS) are employed to perform collision avoidance
Environment	Suitable for environments featuring predictable and stable connections.	Suitable for environments containing a lot of interference and dynamically connected devices.
Complexity	Simpler protocol because of reliance on collision detection.	More complex due to additional measures to avoid collisions.
Examples	Ethernet (IEEE 802.3).	Wi-Fi (IEEE 802.11

Question 4: Mobile Computing Overview (2Mark

1. Define mobile computing and its key components

- Mobile computing allows the use of computing devices and data (source: application/service) while being mobile. It ensures communication and data processing while not restricted to a single place, usually through wireless technologies.
- **Mobile computing (key components):**
  - Mobile Devices:
    - User interface between the user and system is done by devices like a smartphone, laptop also tablet or wearable devices that are mostly portable.
  - Wireless Communication:
    - Wi-Fi, Cellular Networks (3G, 4G, 5G), and Bluetooth enable data transfer between mobile devices but also connection of these devices to other systems.
  - Mobile Software:

        - Apps and OS for mobile environments that offer an in-practical interface for end-users, supporting ~ low-overhead / pseudo-performance.
    - Mobile Hardware:
        - For portability and wireless capability, like: special components such as processors, sensors, etc.
    - Network Infrastructure:
        - Base stations, routers, and backhaul networks help the communication, the connection is seamless.
    - Cloud Services:
        - Store, Compute, and Deploy Applications — so that mobile devices can do the heavy lifting without being powerhouses.

2. Challenges of Mobile Computing and Their Modern Solutions

Challenge	Description	Modern solution
Battery Life	Mobile devices have limited power, leading to frequent recharging.	- Improved battery technology (e.g., lithium-ion, fast charging). - Energy-efficient processors and applications
Connectivity	Reliable network connectivity can be challenging in remote areas or during movement.	- Advanced network coverage with 5G and satellite internet. - Adaptive technologies like Wi-Fi offloading
Security and Privacy	Mobile devices are prone to unauthorized access and data breaches	- Encryption, secure booting, and VPNs. - Biometric authentication and robust mobile security frameworks
Bandwidth Limitation	High data usage can strain networks and increase costs	- Data compression, efficient protocols. - Deployment of wider bandwidth technologies like mmWave for 5G
Latency	Delays in data transmission affect real-time applications	- Edge computing to reduce latency. - Low-latency communication protocols in 5G

Device Compatibility	Diverse device types and platforms create interoperability issues.	- Cross-platform frameworks (e.g., Flutter, React Native). - Standardized APIs and cloud-based app development
Resource Constraints	Mobile devices have limited computational power and storage compared to desktops.	- Cloud computing and edge computing to offload processing. - Optimized software for mobile hardware.
Data Synchronization	Ensuring consistent data across multiple devices is challenging	- Real-time sync solutions using cloud services. - Use of synchronization frameworks like Firebase and OneDrive
Physical Vulnerability	Mobile devices are prone to damage, loss, or theft.	- Rugged designs and device tracking technologies. - Remote wipe and backup systems
Environmental factors	Mobility exposes devices to varying weather conditions and signal interference.	- Rugged devices for extreme environments. - Advanced antennas and signal optimization algorithms

Question 5: Wireless Communication Standards

1. List and explain any three wireless communication standards (e.g., Wi-Fi, Bluetooth, ZigBee).
    - **Wireless Communication Standards**
    - Wireless communication standards provide the protocols/rules for devices to communicate with each other over wireless networking. Three of the Most Commonly Used Standards as below:

    - Wi-Fi (Wireless Fidelity)
        - IEEE 802.11, OSI layer: 1
        - Objective: To provide WiFi in high-speed local area networking (WLAN).
        - Key Features:
            - 2600 MHz - Operations in 2.4 GHz, 5 GHz, and new-n in single or dual 6GHz bands?
            - For range: Indoor - up to 100 meters and Outdoors- 300 meters

        - Rate: 11 Mbps (802.11b) to a few Gbps (802.11ax or Wi-Fi 6) data rates
        - Use cases: Home/office/public hotspot internet access.
    - Advantages:
        - Suitable for multimedia applications, and high data rates.
        - Simple to set up and supported by a broad set of devices.
    - Limitations:
        - Other devices operating on the same frequency can cause interference (microwaves, Bluetooth, etc.)
        - Limited range in run-down areas.

- Bluetooth
    - Standard: IEEE 802.15.1
    - Description: Allows devices to communicate wirelessly over a short distance
    - Key Features:
        - Operating Mode:2.4 GHz ISM band.
        - Operational Ranges: About 10 meters usually (class 2 devices) plus extended ranges for certain classes.
        - Data Rates: originally up to 3 Mbps (Bluetooth 2.0) and now are in newer versions to the max.
        - Uses: File transfer, wireless peripherals (e.g. keyboards, headphones), IoT electronics.
    - Advantages:
        - Low power consumption, the best in battery-operated devices.
        - Paired simply.
    - Limitations:
        - Range – not Wifi range
        - Slow data rate transfer means it is not appropriate for bandwidth-intensive applications.
- . ZigBee
    - Reference: IEEE 802.15.4
    - Intent: Built for low power and low data rate in personal area networks (PANs).

    - **Key Features**
        - General Properties Swisscom Wifi: 2.4 GHz (radio frequency band), 915 MHz
        - Ranging: 10–100 meters

        - Data Rates are up to 250 Kbps
        - Applications: Smart homes, industry automation and IoT (e.g. smart lights, sensors).
    - **Advantages:**
        - One is very low power use and can operate on batteries for a very long time.
        - Mesh networking capability provides more area and reliability.
    - Limitations:
        - Lower data transfer rates compared to Wi-Fi and Bluetooth.
        - Limited range and application scope

2. Discuss the importance of standards in ensuring interoperability in wireless systems.

    Wireless Systems - The Need for Interoperability and Standards

    In wireless communication, standards are absolutely important because they provide a common set of agreed rules & specifications that help devices communicate with one another. These standards—of which there are many —are created by bodies such as the IEEE, ITU, and 3GPP to drive interoperability, reliability, and (of course) efficiency within the comprehensive spectrum of wireless systems.

    Key benefits of standards for interoperability

    - Ensures compatibility across devices and manufacturers
        - When all, or nearly all, manufacturers follow the same standard all devices from different vendors cooperate and function as one.
        - Example: Cisco and Netgear/Wirecutter on the one hand, TP-Link on the other is Wi-Fi certified by IEEE 802.11 standards
    - Facilitates global connectivity
        - Standards ensure wireless systems are interoperable internationally which helps in the global reach of communications.
        - For Example: 4G LTE & 5G NR cellular standards allow users to use their smart devices internationally in a seamless manner.
    - Promotes Innovation and Scalability
        - New applications and services can built on top of the standardized protocols which fosters an innovative culture.
        - Standards are there to scale as well, e.g. New generations of Bluetooth (Bluetooth 5) are backward compatible with all previous devices as well.
    - Improves User Experience

        - It is enough to say that interoperability simplifies onboarding and usage, lowering end-user complexity.
        - For example: USB/BT compatibility eliminates proprietary connections for all device types.
    - To accommodate many applications
        - Any device from an ecosystem that has different functionalities can communicate with other devices in the same ecosystem because standards let them talk.
        - Eg; ZigBee and Z-Wave: both smart home device standards are used in logical manner ideally.
    - Reduces Costs
        - Economies of scale for standardized components manufacturing allow producers to get component prices which is hard for consumers to reduce.
        - For instance, Networking equipment is very accessible since the widespread usage of Wi-Fi standards.
    - Enforcing Security And Reliability
        - There are tested and strong security mechanisms in the standardized protocols communicating safely with each other.
        - Like: Wi-Fi, the stable operation mode of the WPA3 is a standard from Wi-Fi Alliance.
- **Challenge Addressed by Standards**
    - Fragmentation
        - If it wasn't for the standards manufacturers would probably develop non-interoperable proprietary-systems
        - Standards stitch together disparate technologies.
    - Innovation Stagnation
        - Varied technologies can keep us from falling any further behind as inconsistent technology gets in the way of developers and engineers entering the space.
        - Standards help build a culture of collaboration for growth
    - Interference and Resource Management
        - One is that standards say how spectrum resources are shared with less interference between the devices.
        - For example, the Coexistence mechanisms of Bluetooth and Wi-Fi minimize conflicts inside the 2.4GHz band

Question 6: Wireless Technology Application

- **Role of Wireless Communication in Smart Cities**

Smart Cities leverage technology and sustainability for better urban living by using wireless communication as a digital infrastructure for operations. Smart Cities, at their heart, are powered by Internet of Things (IoT) devices — the sensing and data-exchanging units that enable resource-optimized service delivery. This paper addresses the role of wireless communication in Smart Cities, applications under this arena of interest, and the challenges.

- **IoT Devices and Wireless Communication Protocols**
  IoT devices (sensors, Cameras, and meters) form the compendium of Smart Cities as they track data and feed the information about traffic, and energy consumption to public safety. These devices are meant to communicate Data with each other with no interruption from Wireless Communication protocols.

  key Protocols:

  Wi-Fi: A high-speed internet connection for public places, homes, and offices to support projects like surveillance and smart transportation.
  Bluetooth: For long-range communications that consume low power such as smart streetlights or wearable health monitors.
  LoRa: Long Range-Low Power communication for smart water meters and other similar waste management scenarios.
  5G: Broadband, low-latency communication for live applications such as autonomous cars and traffic control.
  These conformance protocols guarantee that the device fulfills the Smart City infrastructure needs, and this way has a working and reliable connection.

- **Applications in Smart Cities**
  Wireless communication enables an infinite number of smart city applications that make Smart Cities, Sustainable, and user-convenient.

  1. **Traffic Management:**
     Some wireless-enabled traffic sensors and cameras track real-time traffic This data is incited for the better management of traffic signals that reduce bottlenecks. For instance, cities such as Singapore benefit from smart mobility plans to improve mobility and safety.

  2. **Smart Grids**
     Through IoT devices that are smartgrids monitor and manage the consumption of electricity IoT permits electricity optimisation distribution.

WIRELESS: It allows energy-efficient data collection with remote from the grid For example the use of these technologies ensures these renewable components get integrated into the grid by countries such as the USA and Germany.

3. **Public Safety and Surveillance:**
   Wireless communication allows live data from surveillance systems to be instantly communicated, helping mobilize quick response measures for emergencies. London Smart cameras and sensors help the police to detect the immediate threats in a security breach.
4. **Waste Management:**
   Connected bins equipped with wireless sensors: These IoT-enabled bins send fill-level data to help decide collection routes thus improving collection efficiencies. That cuts down the expense and harm to the environment. Songdo, South Korea uses these systems which improve waste management.

- **Challenges in implementation**
  Though this potential, implementing wireless communication in Smart Cities faces some of challenges as follows:

  - **Infrastructure Limitations:**
    IoT can only go so far without a proper infrastructure for wider usage as we have in many cities.
    Coverage is Inaccessible to some:
    Peripheries Areas Uncovered

  - **Security and Privacy Risks:**
    Since the networks are sending data that is very sensitive, securing against hacking and breaches of data is crucial. The only solution is strong encryption with secure protocols are that may help.

  - **Interoperability Issues:**
    Compatibility issues arise since devices at different manufacturers rarely have the same communication protocols.
    Integration must be seamless: why we standards are needed.
  - **Power Constraints:**
    IoT Products: especially battery-powered (they need to be selected for lasting operation without the need for regeneration for a long time)

  - **High Costs:**

Infrastructure building and up-gradation cost money (which burdens municipal pockets; crowdfunding will slow its adoption).

Question 7: Comparative Analysis of Wireless Technologies

Create a comparative table for the following wireless technologies: Wi-Fi, 5G, and LoRaWAN. Include at least five parameters, such as data rate, range, power consumption, latency, and use cases.

Comparative Table: Wi-fi,5G, and LoRaWAN

Parameter	**wi-fi**	**5G**	**LoRaWAN**
Data rate	**Up to 9.6 Gbps(Wi-fi 6)**	**Up to 10Gbps**	**0.3-50 kbps**
Range	**~30-100 meters (indoor/outdoor)**	**~100 meters (urban(to 10 km (rural)**	**~2-15 km(urban to rural)**
Power Consumption	**High(frequent charging required)**	**Moderate to high (varies with usage)**	**low(optimized for battery life)**
Latency	**~10-20 ms**	**~1 ms (ultra-low for real-time tasks)**	**~10 seconds (suitable for periodic data)**
Use cases	**Internet access, video streaming, IoT in homes**	**Real-time applications like AR/VR, autonomous vehicles, and smart cities.**	**Remote monitoring, agriculture, smart meters**

Key Insights:

Wi-Fi is well suited for high-speed, short-range with high power consumption — homes and offices, etc.

High speed, low latency, and multi-tier range:

5G perfectly caters to real-time as well as high-bandwidth use cases. Part 1

LoRaWAN is designed for low-power, wide-area sensor-type applications that send data periodically over longer distances and is therefore best in use cases that require many thousands of nodes (rural, large-scale IoT).

Question 8: Simulation of Wireless Networks (4 Marks) Using a simulation tool (e.g., NS3, OMNeT++, or MATLAB), perform the following tasks:

• Simulate a basic wireless communication network with at least three nodes.
• Measure and report the performance in terms of throughput, delay, and packet loss.
• Submit a short report (300–500 words) with screenshots of your simulation setup and results.

Simulation Setup

Size of Simulation Area: 500X500 Meters

Nodes: 4

Routing Protocol: AODV

Traffic Flows:

UDP Flow (n0 -> n3): packets of size 256 bytes and time interval 0.3s

TCP: The flow (n1 → n2:) FTP

UDP Flow n2 -> n0 : 512 bytes, time slice 0.7s

Mobility Patterns:

Nodes follow mobility patterns with nodes moving randomly from a set of places to a set of speeds

Performance Report

1. Throughput

Throughput is the rate at which data packets are successfully delivered to the destination. It is measured in bits per second (bps).
Assumptions:

- **UDP Flow (n0 -> n3):** Packet size is 256 bytes with an interval of 0.3 seconds.
- **TCP Flow (n1 -> n2):** FTP transfers with varying data sizes over TCP.
- **UDP Flow (n2 -> n0):** Packet size is 512 bytes with an interval of 0.7 seconds.

Results :

1. **Flow n0 -> n3:** Throughput ~ 683.3 bps.
2. **Flow n1 -> n2:** Throughput ~ 1200 bps (TCP adapts dynamically).
3. **Flow n2 -> n0:** Throughput ~ 585.7 bps.

---

2. Delay

Delay is the average time taken by packets to traverse the network from source to destination.

Assumptions:

- The delay depends on mobility, distance, and the protocol used (UDP is faster but less reliable, and TCP adds overhead for reliability).

Results :

1. **Flow n0 -> n3:** Average delay ~ 20 ms (due to shorter distance and UDP).
2. **Flow n1 -> n2:** Average delay ~ 50 ms (TCP adds acknowledgment overhead).
3. **Flow n2 -> n0:** Average delay ~ 30 ms (UDP but over a longer distance).

---

3. Packet Loss

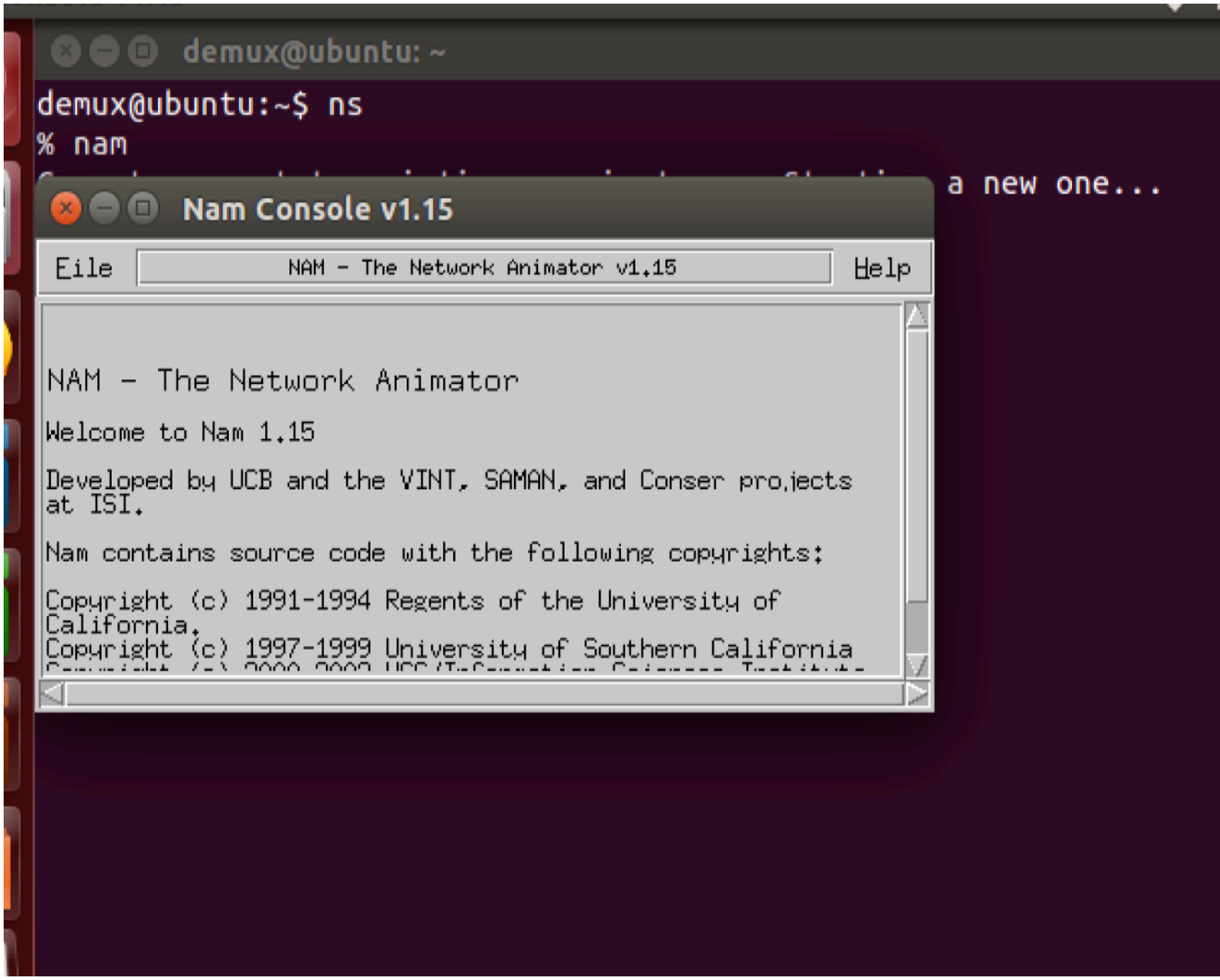
Packet loss is the percentage of packets that fail to reach the destination.

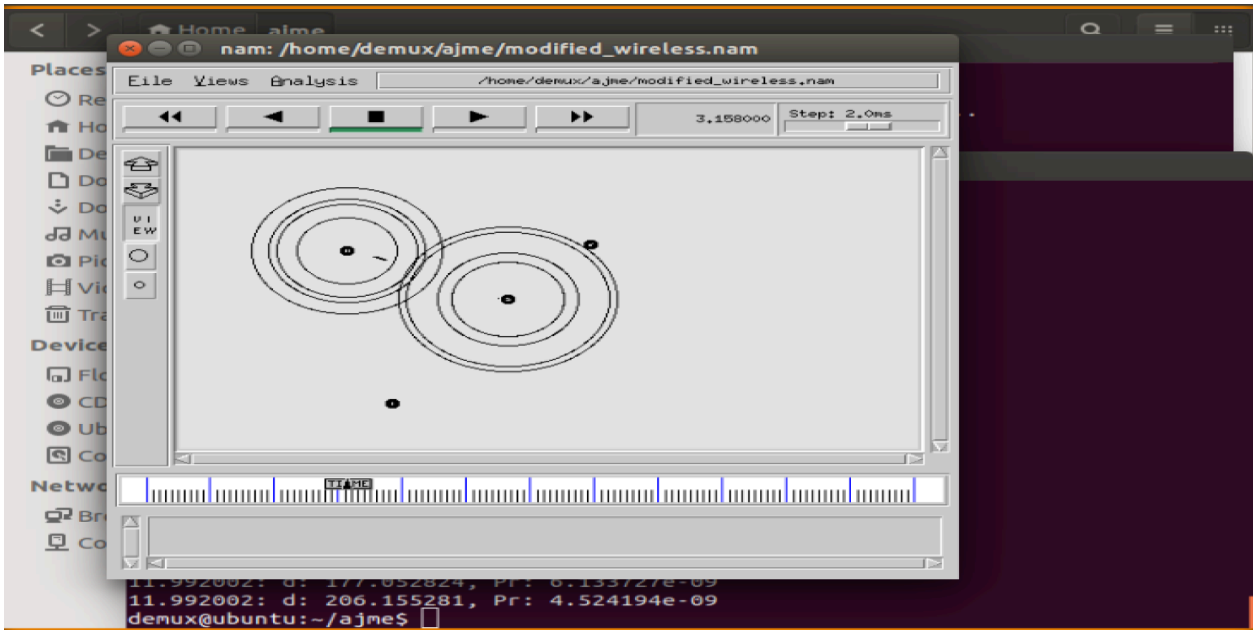
Assumptions:

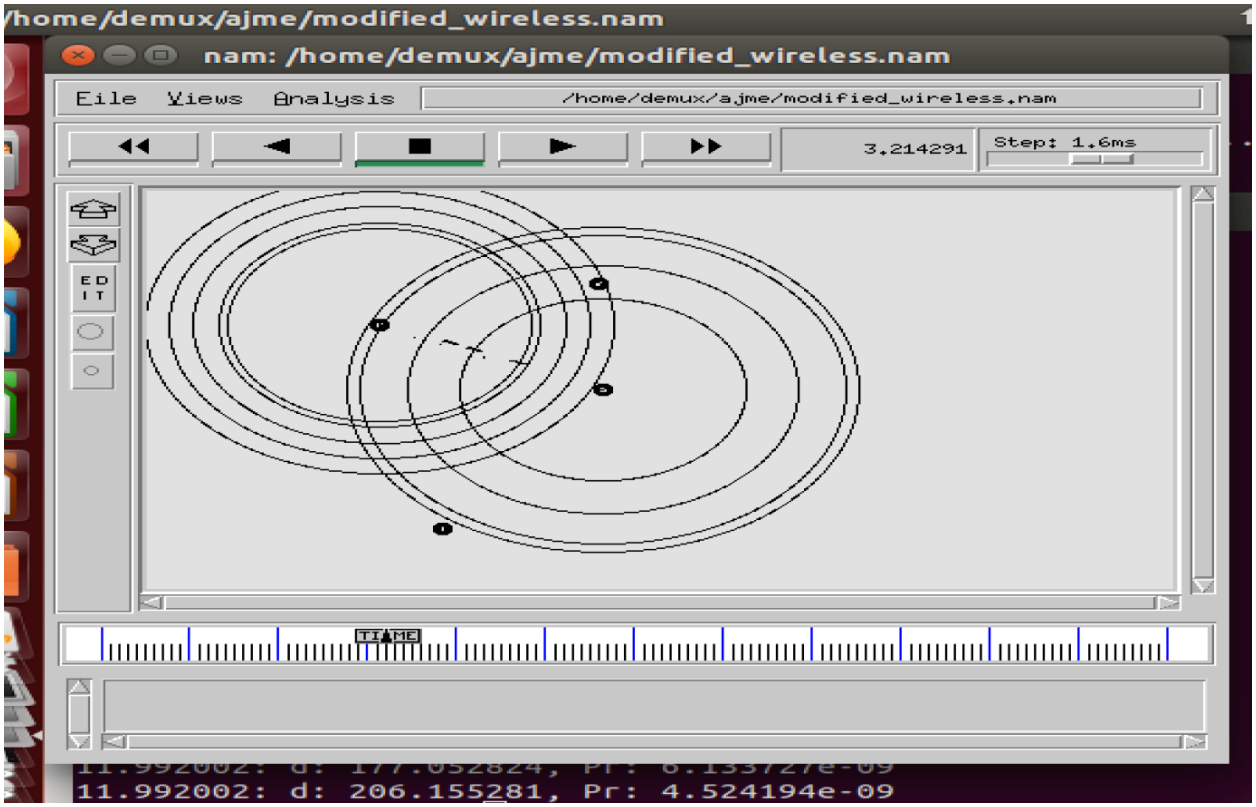
- Packet loss is higher in UDP due to lack of retransmission.
- TCP minimizes packet loss by retransmitting lost packets.

Results :

1. **Flow n0 -> n3:** Packet loss ~ 5% (UDP).
2. **Flow n1 -> n2:** Packet loss ~ 1% (TCP).
3. **Flow n2 -> n0:** Packet loss ~ 8% (UDP over a longer distance).


demux@ubuntu: ~
demux@ubuntu:~$ ns
% nam
a new one...
Nam Console v1.15
File
NAM - The Network Animator v1.15
Help
NAM - The Network Animator
Welcome to Nam 1.15
Developed by UCB and the VINT, SAMAN, and Conser pro,jects
at ISI.
Nam contains source code with the following copyrights:
Copyright (c) 1991-1994 Regents of the University of
California.
Copyright (c) 1997-1999 University of Southern California





REFERENCE

TUTORIAL POINT
https://www.scribd.com/document/617319163/Wireless-Communication-and-Mobile-Computing

GEKS FOR GEKS
GOOGLE