Name: Abhishek Guleri
Roll. No: 185509
Lab: Mobile Computing
Assignment No.: 3
Branch: CSE DD

Objective -> Study the hidden and exposed terminal problems, write a program to demonstrate these problems.

Hidden Terminal Problem:

Hidden Terminal Problem occurs when a node is not in range of the sender of data but is in the range of the receiver. When two such unaware nodes start to transmit data to the common receiver data collision occurs. To avoid this problem one can use RTS/CTS control packets.

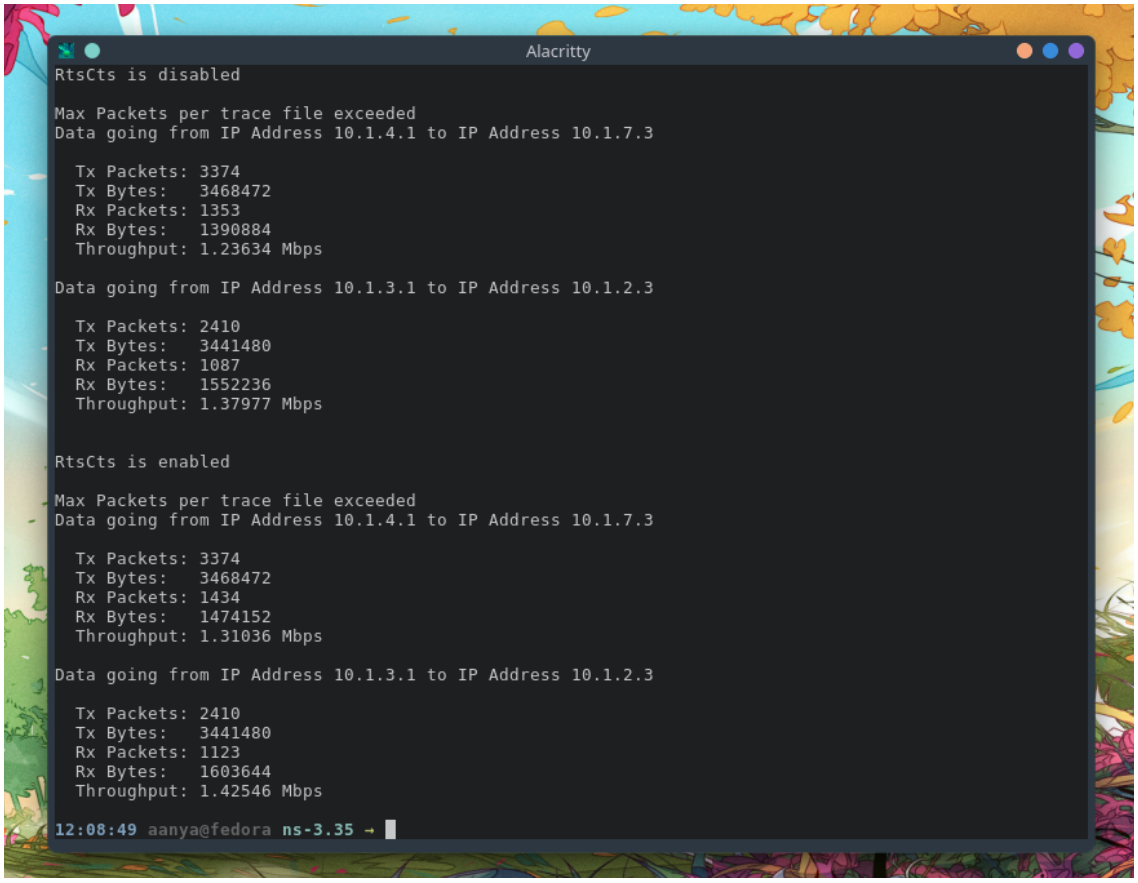
- **Network Topology**

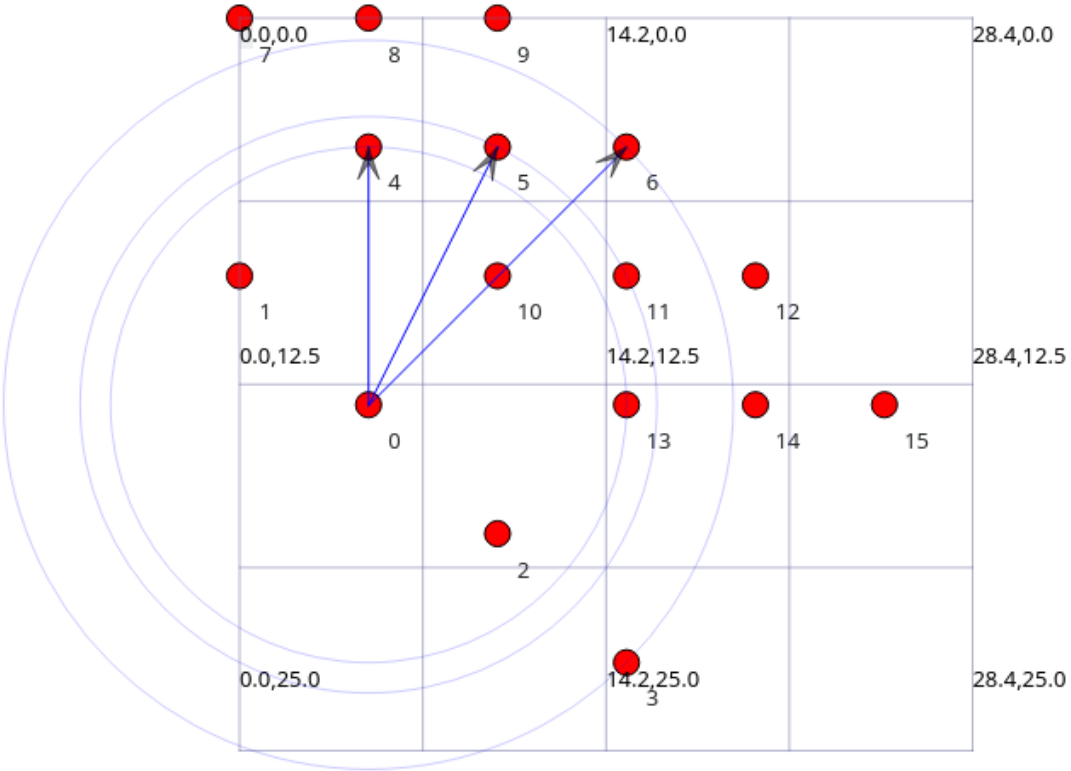
  The network topology of this network contains three devices/nodes that act as Access Points and each of these access points has 3 more station nodes in its range.

  AP1 — — — — — — — — — — AP2 — — — — — — — — — AP3

- **Simulation Parameters**
  - RTS/CTS Threshold value = 2200/10
  - Propagation Loss = Fixed for each pair of Nodes & doesn't depend on their actual positions.
  - For Data Mode DSSS rate = 2 Mbps
  - For Control Mode DSSS rate = 1 Mbps
  - Packet Size = 1400 bytes

- **Simulation using NetAnim with ns3**
  Steps include :
  - Creation of nodes
  - Propagation loss matrix setup
  - Wifi communication channel setup
  - Wireless devices installation
  - TCP/IP stack setup and IP addresses assigned to each node/device
  - Applications: two CBR streams each saturating the channel
  - Mobility and FlowMonitor setup
  - Add for the NetAnim simulation
    - Module package and AnimationInterface is called to create a *.XML file


Alacritty
RtsCts is disabled
Max Packets per trace file exceeded
Data going from IP Address 10.1.4.1 to IP Address 10.1.7.3
Tx Packets: 3374
Tx Bytes: 3468472
Rx Packets: 1353
Rx Bytes: 1390884
Throughput: 1.23634 Mbps
Data going from IP Address 10.1.3.1 to IP Address 10.1.2.3
Tx Packets: 2410
Tx Bytes: 3441480
Rx Packets: 1087
Rx Bytes: 1552236
Throughput: 1.37977 Mbps
RtsCts is enabled
Max Packets per trace file exceeded
Data going from IP Address 10.1.4.1 to IP Address 10.1.7.3
Tx Packets: 3374
Tx Bytes: 3468472
Rx Packets: 1434
Rx Bytes: 1474152
Throughput: 1.31036 Mbps
Data going from IP Address 10.1.3.1 to IP Address 10.1.2.3
Tx Packets: 2410
Tx Bytes: 3441480
Rx Packets: 1123
Rx Bytes: 1603644
Throughput: 1.42546 Mbps
12:08:49 aanya@fedora ns-3.35 →


0.0,0.0
14.2,0.0
28.4,0.0
0.0,12.5
14.2,12.5
28.4,12.5
0.0,25.0
14.2,25.0
28.4,25.0
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

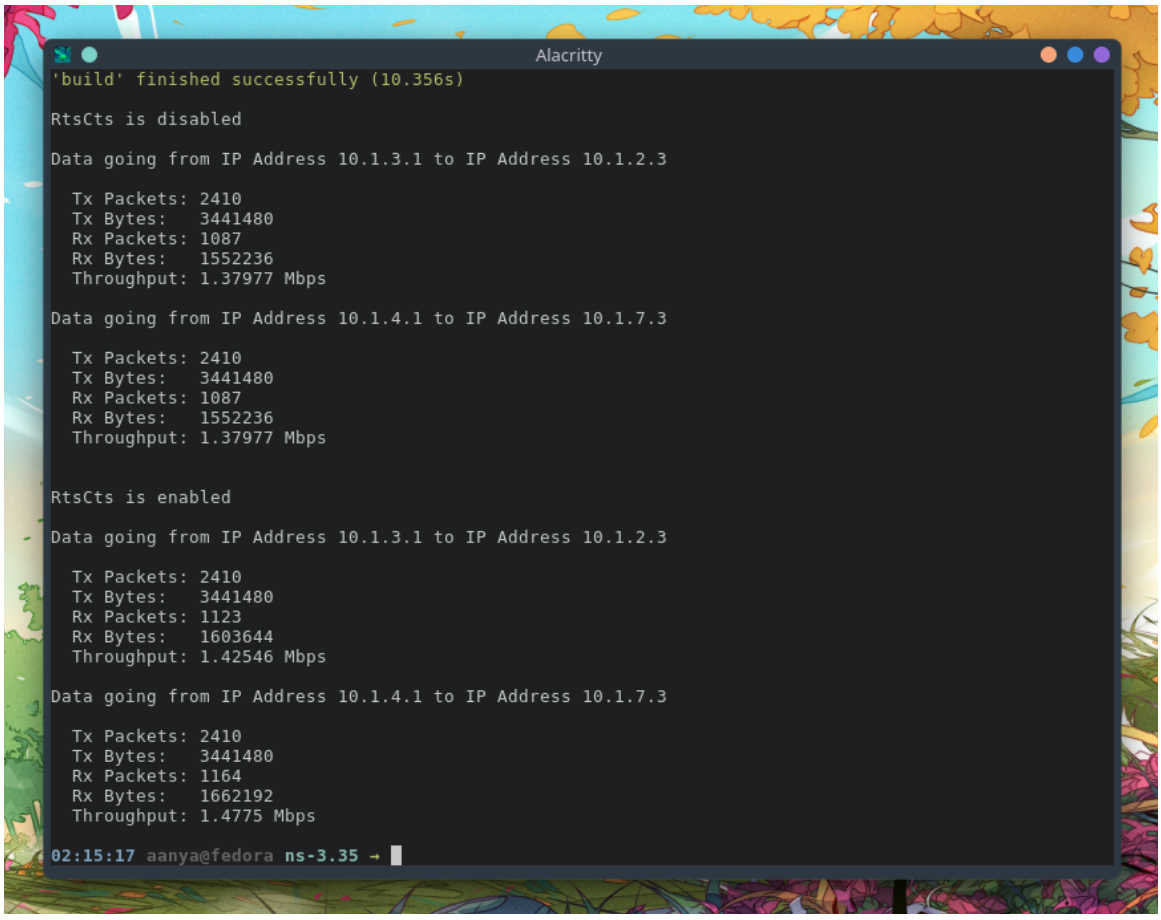
Exposed Terminal Problem:

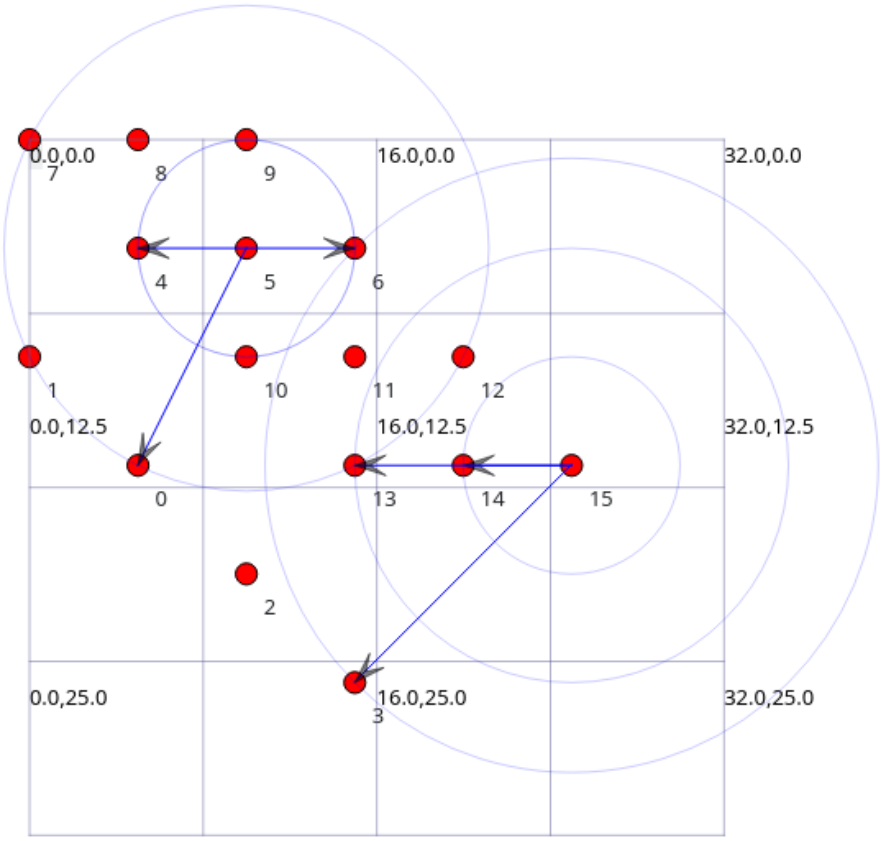
Exposed Terminal Problem occurs when a node is communicating with a node and due to this some other node is unable to communicate with some different node because the former node is in the range of one of the nodes which are communicating. The node becomes exposed to its neighbor node. To avoid this problem one can use RTS/CTS control packets.

- **Network Topology**

  The network topology of this network contains three devices/nodes that act as Access Points and each of these access points has 4 more station nodes in its range.

AP1 — — — — — — — AP2 — — — — — — — AP3 — — — — — AP4





Observations

- Throughput is less without RTS/CTS mechanism. This is so because with RTS/CTS there are excessive collisions as the stations remain hidden and cannot sense if the channel is free or not.
- Throughput can be lower even when RTS/CTS is applied if there are successive continuous collisions among the RTS/CTS control packets.
- The overhead caused by RTS/CTS packets amounts to the #RTS[1], CTS packets exchanged, and the size of these packets.
- Minimum overhead = (RTS+CTS)*#Packets to be transferred assuming #RTS, CTS collisions.

Source Code

[Hidden Exposed Terminal Problem]

[1] # - Number of