AMS 559: Project Proposal
Smart Router for Anonymous Browsing

Team:
Rishabh Jain (111472079) (Leader)
Aman Raj (112071600)
Vinod Kumar Loganathan (111491311)

Problem Description:

Increasing number of websites offer “personalized” web pages which are customized as per user’s interests. There is lack of privacy on the world wide web, so a system to ensure private communication will be helpful. This can be coupled with smart routing where we can manage the routers through a master slave configuration and save energy. Master will control the routers by turning them off whenever they are not getting used.

Importance of solving the problem:

1. User will have an extended range for his/her router
2. Flexibility in changing secondary router locations and hence the signal reach
3. Will provide more security to the user by mitigating the chances of packet sniffing
4. Instead of having multiple router, having one master and few RPs to work as extender will be an energy efficient system.

Potential Challenges:

1. Choosing which router to connect to based on user location, router location and signal strength.
2. Providing TOR support on router while minimizing any delay caused by it.
3. Switching between the routers if user is moving from one router’s range to another and then powering off the idle routers.

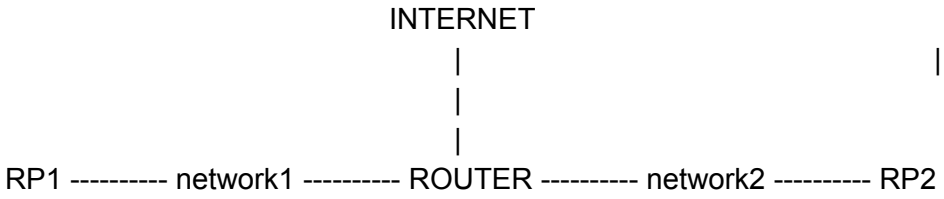
Approach and Roadmap:

Device Requirements:

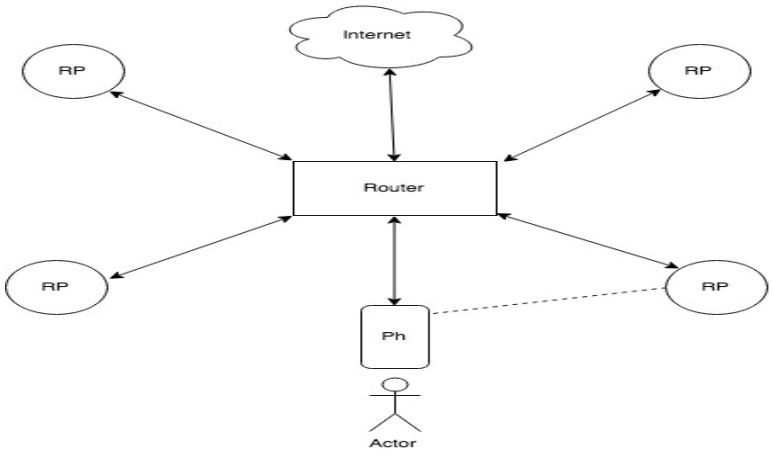
1. Raspberry Pi (RP) x 2 (Including power backup, wires, etc)
2. Raspberry Pi Wifi extender
3. Ethernet cables
4. SD card
5. Laptop (For Routing functionality)

- Each of the RP will be connected to the router physically via ethernet
- The Laptop(Router) will be configured to have routing functionality -> to transmit packets from one network (RP network) to another (Internet)
- Routing software will also be installed and configured on each of the RPs
  Note: The Wifi signals are extended as part of this approach giving a wider range of coverage to the users.

  We now have the following topology



- TOR - The Onion Router is a software that provides anonymous data transfer over the internet. We install this on each of RPs to provide anonymous browsing functionality.
- A captive portal (a portal that uses user login credentials to sign up/login) will pop-up when the user tries to connect to the network. During this time, the router finds the closest RP to the user (using the signal strength as the distance parameter).
- The user has an option to choose “anonymous browsing” functionality. If the user opts for it, the Wifi network connection is going to be re-routed to the RP.
- Now, the packets will flow via the RP and to the router and finally reaches the internet.
- Since the packets go via the RP, it will be encrypted and secure, that guarantees anonymous functionality.
  Note: The routing tables will be updated during this phase to re-transmit the packets.



Week 1-2 : Gather Requirements
Week 3-4: Setup and Configuring the topology
Week 5-6: Algorithms for finding closest RP and changing routing tables
Week 7-8: Integration and Prototyping
Week 9-10: Testing and Bug Fixes