There are three code files that we have written and one we have modified as per the needs of the project.
The codes we have written:

- trafficGen.py
    - It should be placed in mininet/custom
- attackLauncher.py
    - It should be placed in mininet/custom
- detectAttack.py
    - It should be placed in pox/pox/forwarding

The code we have modified:

- l3_modified.py
    - It is present in pox/pox/forwarding as l3_learning.py, you can either edit the code within it or simply make an l3_modified.py file

Before starting we need a network topology, in the research paper we are implementing, 9 switches and 64 hosts are there in the topology. To create a topology with these parameters with the help of mininet, the following command should be run on the terminal:

```
sudo mn --switch ovsk --topo tree,depth=2,fanout=8
-controller=remote,ip=127.0.0.1,port=6633
```

Open a new terminal and run the following commands:

```
cd pox
python ./pox.py forwarding.l3_modified
```

To generate traffic, trafficGen.py should be run. The terminal in which mininet is running, run:

```
xterm h1
```

The xterm window will open for node h1, in that run:

```
cd mininet/custom
python trafficLaunch.py -s 2 -e 60
```

Now, again open the terminal in which mininet is running, this time run:

```
xterm h64
```

In the xterm window of the node h64, run:

```
script h64.txt
tcpdump -v
```

Now, its time to attack, we will be attacking node h64 using node h1, h2 and h3. Therefore, on the terminal with mininet running, run:

```
xterm h2 h3
```

Now, on the xterm windows of h1, h2 and h3, run:

```
cd mininet/custom
python attackLauncher.py 10.0.0.64 # attack on h64
```

The problems one may encounter:

- While implementing the network topology in the mininet on one terminal and going inside the pox on another terminal, when the `python ./pox.py forwarding.l3_modified` is run multiple times then an error saying, controller already in use may occur. To resolve it run the following commands on the same terminal:

  ```
  sudo netstat -lpn |grep :6633
  ```

  An output of this form will be expected:

  ```
  tcp6       0     0 :::6633  :::*     LISTEN      6782/java
  ```

  The process Id, which is 6782, now this is the process that is using port 6633. To Kill the process, type:

  ```
  sudo kill 6782
  ```

- There is a high possibility of incurring this error:

  ```
  INFO:packet:(ipv6) warning IP packet data incomplete (114 of
  316)
  INFO:packet:(dns) parsing questions: incomplete name
  ```

  This error will occur after running the following command:
  `python ./pox.py forwarding.l3_modified`

The POX source code has some bugs which lead to the occurrence of the above errors. It can be corrected by making the following changes:

1. Add at line 244 in packet.dns (pox/pox/lib/packet/)

```
elif r.qtype == 28:
    assert isinstance(r.rddata, IPAddr6)
    return s + r.rddata.toRaw()
```

2. Change at line 4431 in openflow.libopenflow_01.py the value of OFP_DEFAULT_MISS_SEND_LEN to a bigger value (default is 128). This error happens because DHCP packets are truncated. For my project, I have set it to 1000. It is present in pox/pox/openflow. Also, edit the .pyc file corresponding to it or relocate it