installation instrucions

- ubuntu 18.04 required (https://releases.ubuntu.com/18.04/)
- python3.6.9 installed by default should be enough

```
sudo apt update && sudo apt upgrade
sudo apt install xterm
```

do all the 6 commands below as i am not sure which one it needs

```
apt install python3-pip
pip3 install matplotlib graphviz pandas
sudo apt install python3-tk
```

```
apt install python-pip
pip install matplotlib graphviz pandas
sudo apt install python-tk
```

installation FNCS, gridlab, ns3

follow along with the `installation_guide.md` in the project directory except for 1 needed change when installing gridlab switch to the "feature/797" branch

```
git checkout feature/797
```

editing some files to get the simulation to run

we will be using (13 Nodes 73 Houses)

changes:

attack borker python file

`attack_broker.py` on line 103

replace:

```
pid = int(child.communicate()[0].split('\n')[0])
```

with:

```
stdout_data, stderr_data = child.communicate()
pid = int(stdout_data.split(b'\n')[0])
```

gridlab glm file

`gridlab-D.glm` remove on line 75

```
object fncs_msg {
   name fncs_msg;
      parent Market_1;
   route "function:controller/submit_bid_state ->
      auction/submit_bid_state";
   option "transport:hostname localhost, port 5570";
   configure fncs_msg.txt;
}
```

the implementation

- the IDS function is in this same repository in `listings/IDS.cc`
- what the new `ns-3.cc` file in your project should be is `listings/new_ns-3.cc`
- so copy this file (`listings/new_ns-3.cc`) into your `ns-3.ns` to test it

conclusion about the simulation

the ns3 section gets stuck at the line

```
    FncsSimulatorImpl *hb=new FncsSimulatorImpl();
```

tried removing that section but nothing diffrent happend

Important!

i dont think this simulation is well designed to simulate a real cyberattack as they represent those attacks by just changing some configuration values in the simulation to demonstrate the potential effects of an attack therfore i dont think implemeting a real life example of an IDS is possible here

conclusion

in `SecuringtheSmartGridAComprehensiveCompilationofIntrusionDetectionandPreventionSyst`
`RADOGLOU-GRAMMATIKISetc.).pdf`

some of the methodes used to test SG security were

- testing on a real life testbed and used real cyberattacks targeted at them to test IDS
- some used snort IDS on real hardware

not much sources or data was provided on those tests or how to replicate them

i searched for ways to simulate cyberattacks on a smart grid but i found nothing

i searched for other simulation but they are mostly either not implemented or incomplete

i think the remaining solution would be to either implement an IDS for gridlab or a WIPS but i have no hardware to test on or any simulation which leave the only option to try to implement it on my home router as if it is a smart grid component

would like to hear your opinion soon. thank you.