2021 Summer ELG 5142 Ubiquitous Sensing and Smart City Assignment Four

Instructor: Dr. Wail Mardini

Teaching Assistant: Yu Shen, Email: yshen041@uottawa.ca

Reem Abdel-salam, Email: reem.abdelsalam13@gmail.com

Submission Deadline: Saturday, November 26, 2021 11:59pm (One submission per group)

Assignment Four is based on the network attacks and machine learning algorithms we implemented in tutorial four and tutorial five.

Assignment Background

Consider this: we have a Wireless Sensor Network (WSN). It includes a controller and several sensors. The same as the previous assignment, these sensors collect environment parameters and send them to the only controller. However, there are two malicious nodes that are hackers by a network attacker. The attacker uses one of them to implement the UDP Flood attack and uses the other one to implement the Ping Flood attack. Please capture the network packets, analyze the data and classify the network packets with machine learning algorithms.

Assignment Steps

1. **To simply the assignment four, please obey the following steps**:
    1. Build a WSN consists of one controller and ten sensors. Run the simulation and collect enough normal traffic.
    2. Build a WSN consists of one controller, ten sensors, and one malicious node. Implement the UDP Flood attack with the malicious node according to our previous tutorial. Run the simulation and collect network packets. Do not forget to take down the malicious node port number, address, attack starting time and attack ending time. This information is used to label the dataset later.
    3. Build a WSN and implement Ping Flood attack uses the same way as step two.
    4. For now, there are three .pcap files in hand. Extract features use the network feature extractor provided.
    5. Label the three datasets and merge them together after deleting network hardware information.
    6. Feed the generated dataset to three machine learning algorithms: **Random Forest[1]**, **Naive Bayes[2]**, and **Adaboost[3]**. Check the classifiers' performance by calculating the macro F1 score, precision, recall, accuracy respectively. Also, you need to provide the confusion matrices for each classifier.

Assignment Main Chapters:

Points you need to include in your assignment report:

1. How do you implement the two network attacks?
2. How do you generate the dataset?
3. Compare the performances of the three machine learning algorithms. Do not forget to include the macro F1 score, precision, recall, accuracy and confusion matrices.
4. Give your conclusion.

Support Links:

1. Random Forest Classifier — scikit-learn
2. Naive Bayes — scikit-learn
3. AdaBoostClassifier — scikit-learn