IDENTIFYING ATTACKS IN IOT NETWORK BASED ON LOCATION

Author[1:] PULLETI CHARAN SUMANTH,
Author[2]: POLISETTY NAVEEN SAI KRISHNA,
Author[3]: SYED MOIN KHADRI,
Author[4]: YARRU VENKATA KASI PRAVEEN.

[1] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*
[2] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*
[3] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*
[4] *Student, ECE, VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY, A.P., INDIA*

ABSTRACT

In general, there were various types of networks like local area network (LAN), wide area network (WAN), Low power wide area network (LPWAN), and LOWPAN. The networks are basically used for sharing the information. IoT network is also a type of network for the exchange of data, such networks are attacked by attackers when the network gets hacked or the network contains malicious node or hacker node. The malicious node is used to extract the data present in the network or pollute the network by sending unwanted data to the network. Such attacks are identified in a network with the help of various simulation tools. The paper contains the attacks that were take place in a network and have identified the attacks by using various simulators and the workstations and by using the machine learning classifiers in the Jupiter notebook in order to find the hacker or malicious node accuracy in a network. Thus, we conclude that the network has been attacked by a hacker node or malicious node so we can provide the required measurements for the network and can trouble shoot the network.

***Keyword**: IoT network, Denial of service attacks, Cooja simulator, Wireshark, jupyter notebook.*

1. INTRODUCTION

A network is classified into two types like wired network and wireless network. In most of the cases wireless networks are preferred since they provide the data transfer easy when compared with the wired networks. The networks are basically are of various types and as per the emerging technology the IoT networks are widely used in most of the scenarios. The attacks on the network are also common now-a-days since the use of various hacker nodes or due to malicious nodes present in the network. The data present in the network gets changed or get deleted due to the presence of the attacks in the network. The attacks are also used to increase the traffic by sending various data packets from one node to the other node as that the network gets polluted due to heavy traffic. These attacks are identified which was the main heart of the project.

1.1. IOT NETWORK

IOT NETWROK in simple words refer to the interconnection of various devices that communicate with one another in the form of signals or data and exchange the data form one device to the other device so the exact data is transferred with out any loss of the original data. This communication between devices was generally done by human interface such as autonomous cars, smart home appliances are the major examples of the IoT network.

1.2. TYPES OF ATTACKS IN A NETWORK

Generally, there were two types of attacks in a network they were Active attacks and Passive attacks. The attacks are generally used to enter into the network as unauthorized access and used to steal the data present in the network. The active attacks are the attacks only gain unauthorized access into the network and modify data, either by deleting, encrypting or otherwise harming it. The passive attacks are the attacks gain unauthorized access to a network and can monitor or steal sensitive information present in the network, but without making any change to the data. The major type of attack that was discussed in the paper was DoS attack abbreviated as Denial-of-Service attack.

1.3. DENIAL OF SERVICE ATTACKS

The denial-of-service attacks were the attacks which happen in a network is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. There were various types of DoS attacks they are blackhole attacks, wormhole attacks, Sinkhole attacks. The sinkhole attack is a type of attacks which were carried out by either hacking a node in the network or introducing a fabricated node in the network. The malicious node promotes itself as the shortest path to the base station and tries to guide the traffic from other nodes towards itself and alters the data passing through it.

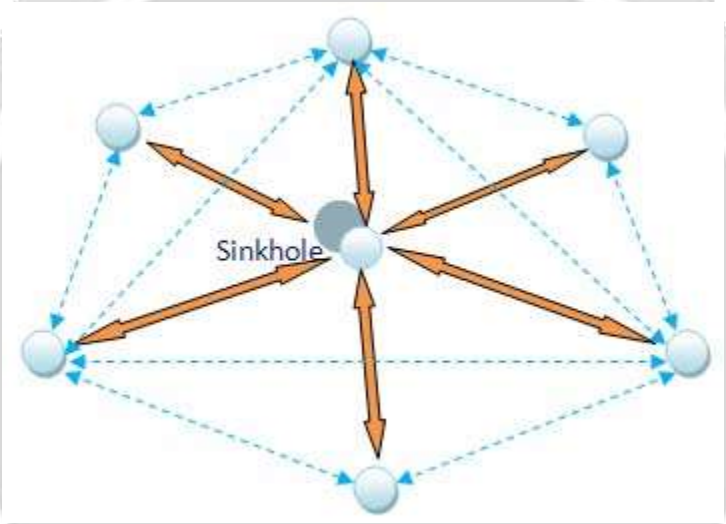

FIG 1. SINKHOLE TYPE OF DOS ATTACK

2. COOJA SIMULATOR

Cooja simulator is a network simulator which permits the usage of real hardware platforms. Cooja is the application of Contiki OS concentrating on network behavior. This simulator tells the data present in a network. Cooja is capable of simulating wireless sensor network without any particular mote or node. Cooja Simulator is a network simulator specifically designed for Wireless Sensor Networks. The Cooja simulator is generally used to give the pictorial representation of nodal parameters that were present in the network. The Cooja is the Contiki network simulator. Cooja allows the small and the large network to be simulated and provide the nodal data. So the network is created by installing a hacker node in the network in the Cooja simulator and the simulation was made to run and the various parameters like power consumption, instantaneous power consumption, average power consumption, average temperature, received packets per node and the radio duty cycle of the nodes were observed by using the Cooja simulator. The Cooja simulator uses “VMware workstation” as the platform to run the entire network. VMware workstation runs on x64 versions of Windows and Linux operating systems it enables users to set up virtual machines on a single physical machine and use them simultaneously along with the host machine. The VMware workstation runs on its own virtual machine. And finally, a network was created in the Cooja simulator and it made rum to get the nodal parameters of the nodes present in the network and their behaviors.

3. WIRESHARK

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, for network analysis, software and communications protocol development, and to get the network information. Originally named Ethereal, and it was renamed as Wireshark later. The data from the Cooja simulator will be get extracted by Wireshark in the form of .csv (comma separated values) file. The extraction of data from Cooja simulator by using Wireshark is done by following the below steps:

- Open the Wireshark which was in-built in the COOJA simulator.
- Go to tools in the simulation window and click on radio messages after that click on analyzer and select LOW PAN analyzer with PCAP.
- To search for PCAP Files. In files open Contiki folder in Contiki folder open tools in tools open Cooja in Cooja click on build folder in build folder search for PCAP files and open them via Wireshark packet analyzer.
- Go to files in the simulation window and click on export file and select as CSV (Comma Separated Values).

4. JUPYTER NOTEBOOK

The jupyter notebook is a web-based application suitable for capturing the whole computation process developing, documenting, and executing code, as well as communicating the results. The jupyter notebook is used to provide the result in various form like graphical representation and matrix maps. The jupyter notebook generally consists of line-to-line execution of the code. The data that is extracted from the Cooja simulator in the form of csv files is used in the jupyter notebook to get the accuracy of the hacker node location or the malicious node in the network. The accuracy is generally found by various classifiers like logistic regression, Random Forest, SVM, Decision tree. These classifiers were generally used to divide the data for clear evaluation. These classifiers are the ml classifiers used in the jupyter notebook for the accuracy calculation.

5. SIMULATION RESULTS AND THE NOTEBOOK OUTPUTS

The outputs from the Cooja simulator and the outputs from the jupyter notebook were presented below:

5.1 COOJA SIMULATOR OUTPUTS

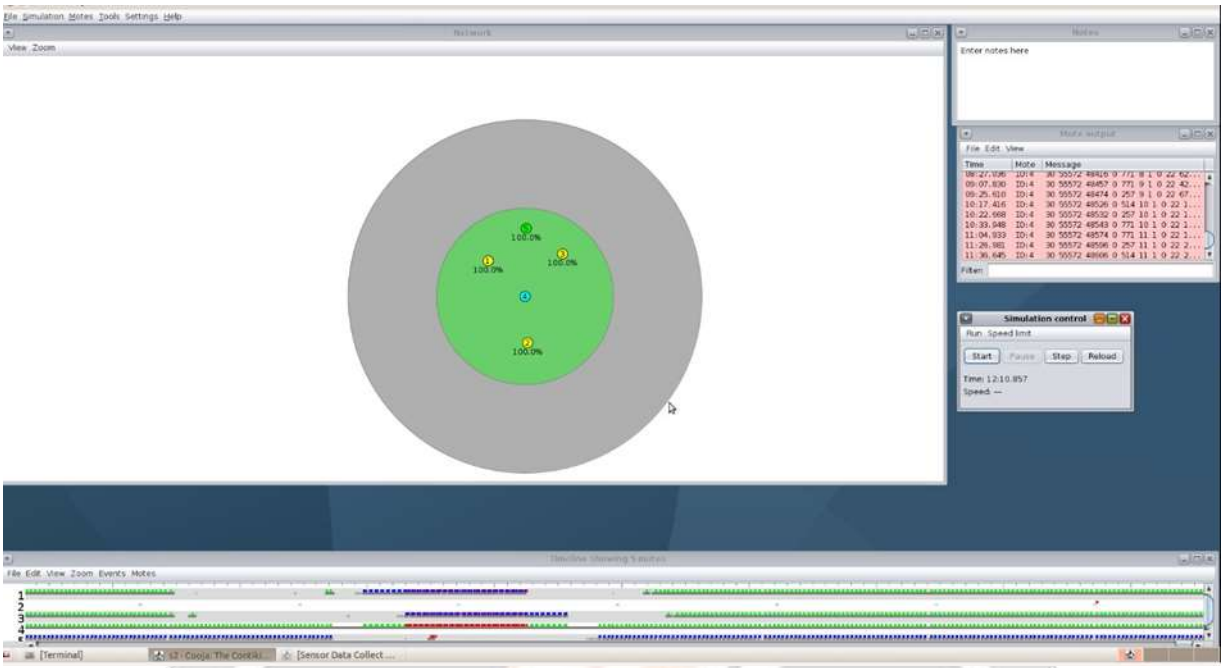

FIG 2. INITIAL COOJA SIMULATOR NETWORK

In figure 2, We see the initial network created in the Cooja simulator.

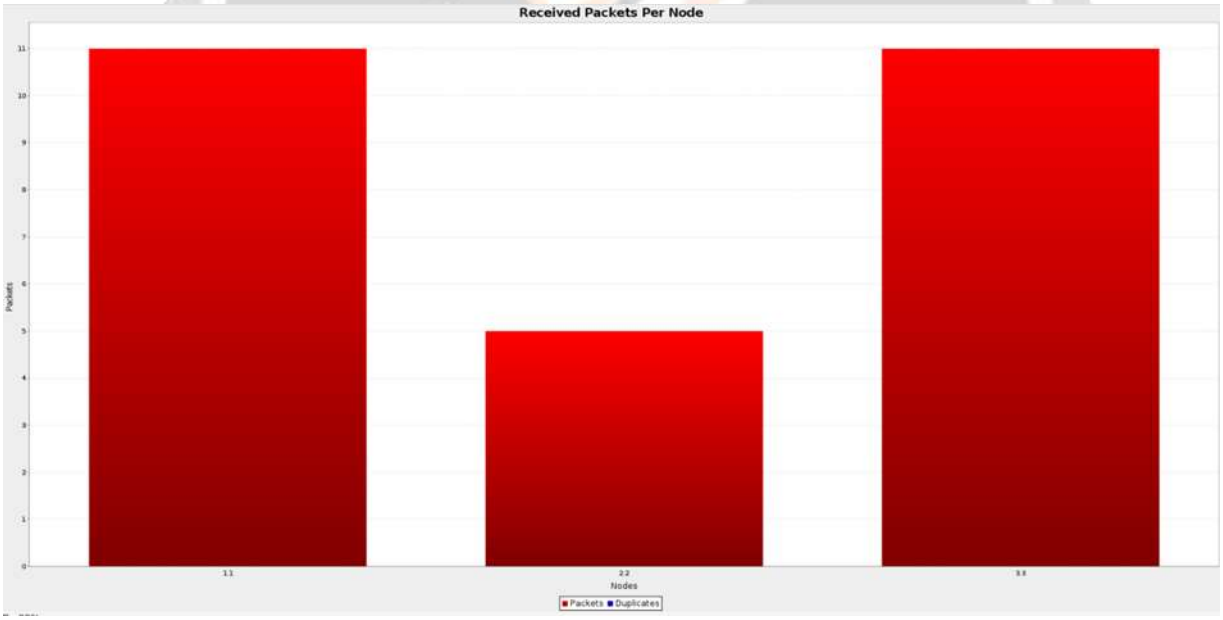

FIG 3. RECEIVED PACKETS PER NODE IN THE NETWORK

In figure-3, we see received packets per node as on the nodal parameter in the network among various parameters. Here the received packets for node-1 and node-3 were more compared with node-2 since the hacker or the malicious node is present near to the node-1 and node-2 and far from node-2. So, the hacker continuously sends unwanted data to the node-1 and 3 compared with node-2.

5.2 JUPYTER NOTEBOOK OUTPUTS

```
from sklearn.linear_model import LogisticRegression
start_time = time.time()
pred_now, acc_lr, acc_cv_lr, lr = fit_algo(LogisticRegression(C=0.1)
                                           , X, Y, 10)

lr_time = (time.time() - start_time)

print("Accuracy: %s" % acc_lr)
print("Accuracy of CV: %s" % acc_cv_lr)
print("Execution time: %s" % lr_time)
```

```
Accuracy: 90.1
Accuracy of CV: 89.05
Execution time: 64.40023922920227
```

FIG 4. LOGISTIC REGRESSION CLASSIFIER ACCURACY

In figure 4, We see the Logistic Regression classifier accuracy output in the jupyter notebook.

```
from sklearn.tree import DecisionTreeClassifier
start_time = time.time()
pred_now, acc_dt, acc_cv_dt, dt = fit_algo(DecisionTreeClassifier(random_state = 1)
                                           , X, Y, 10)

dt_time = (time.time() - start_time)

print("Accuracy: %s" % acc_dt)
print("Accuracy of CV: %s" % acc_cv_dt)
print("Execution time: %s" % dt_time)
```

```
Accuracy: 99.74
Accuracy of CV: 91.44
Execution time: 44.397424936294556
```

FIG 5. DECISION TREE CLASSIFIER ACCURACY

In figure 5, We see the Decision Tree classifier accuracy output in the jupyter notebook.

```
from sklearn.ensemble import RandomForestClassifier
start_time = time.time()
pred_now, acc_rf, acc_cv_rf, rf = fit_algo(RandomForestClassifier(n_estimators = 100)
                                        , X, Y, 10)

rf_time = (time.time() - start_time)

print("Accuracy: %s" % acc_rf)
print("Accuracy of CV: %s" % acc_cv_rf)
print("Execution time: %s" % rf_time)
```

```
Accuracy: 99.74
Accuracy of CV: 92.62
Execution time: 293.2597322463989
```

FIG 6. RANDOM FOREST CLASSIFIER ACCURACY

In figure 5, We see the Random Forest classifier accuracy output in the jupyter notebook.

```
from sklearn.svm import LinearSVC
start_time = time.time()

pred_now, acc_svc, acc_cv_svc, svc= fit_algo(LinearSVC()
                                        ,X,Y,10)

svc_time = (time.time() - start_time)

print("Accuracy: %s" % acc_svc)
print("Accuracy of CV: %s" % acc_cv_svc)
print("Execution time: %s" % svc_time)
```

```
Accuracy: 90.27
Accuracy of CV: 89.21
Execution time: 390.9606738090515
```

FIG 6. STATE VECTOR MACHINE ACCURACY

In figure 5, We see the State Vector Machine (SVM) classifier accuracy output in the jupyter notebook.

6. CONCLUSION

As of our first step we have created a network using the Cooja simulator and with the help of VMware work station. Later on, we implemented the project by using a hacker or malicious node in our network.
In the second step we made that network run for some time using the Cooja simulator and then we observed the nodal behavior in terms of power consumption.
In the third step we extracted the data from the Cooja simulator using wire shark in the form of .csv file.
In the fourth step we used that data set and we executed the code using various classifiers to measure the accuracy of the hack in a network using jupyter notebook.
In the fifth step we conclude our project by using different classifiers to measure the exact accuracy of the hacker node in a network which was present in our network.
The project was concluded by finding the accuracies by using various classifiers and comparing the accuracies we found that the Decision Tree classifier was used in order to find the good accuracy since it has good accuracy and less execution time.

8. REFERENCES

- Ghahramani, Meysam, Reza Javidan, Mohammad Shojafar, Rahim Taheri, Mamoun Alazab, and Rahim Tafazolli. "RSS: An energy-efficient approach for securing IoT service protocols against the DoS attack." IEEE Internet of Things Journal 8, no. 5 (2020): 3619-3635.
- Y.-Y. Cheng and Y.-Y. Lin, “A new received signal strength-based location estimation scheme for wireless sensor network,” IEEE Trans. Consum. Electron., vol. 55, no. 3, pp. 1295–1299, Aug. 2009.
- B. Zhou, Q. Chen, and P. Xiao, “The error propagation analysis of the received signal strength-based simultaneous localization and tracking in wireless sensor networks,” IEEE Trans. Inf. Theory, vol. 63, no. 6, pp. 3983–4007, Jun. 2017.
- S. Pagano, S. Peirani, and M. Valle, “Indoor ranging and localisation algorithm based on received signal strength indicator using statistic parameters for wireless sensor networks,” IET Wireless Sens. Syst., vol. 5, no. 5, pp. 243–249, Oct. 2015.