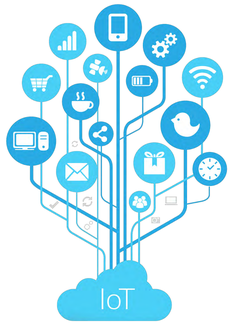
Anomaly Detection In IoT Devices Using Data Mining Techniques

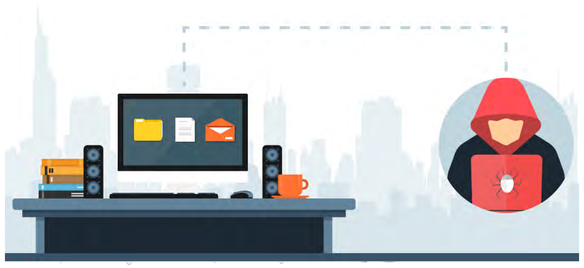
Tolulope A Odetola*, Hawzhin Mohammed*, Syed Rafay Hasan*, and William Eberle**
*Department of Electrical & Computer Engineering, **Department of Computer Science

I. Introduction



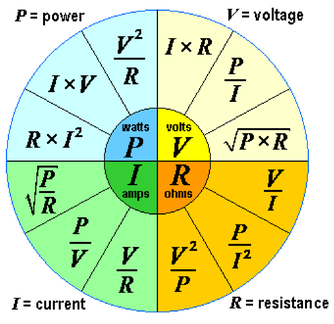
- IoT has found adoption in many fields and applications.
- Analysts have predicted that the IoT will become the “next big thing” in upcoming years.

II. Problem Formulation



- Security is one of the major challenging issues in IoT.
- This is due to the wireless medium characteristics of data transmission.
- Hardware Trojan is used to steal data information from IoT.

III. Approach



- This approach collects data on power usage.
- The data is used to create a machine learning model.
- The model used in the identification any malicious behaviors of the IoT device based on aberrant power behavior.

IV. Methodology

For this research the IoT devices under test include:

Arduino UNO R3

Raspberry Pi 3

Arduino YUN

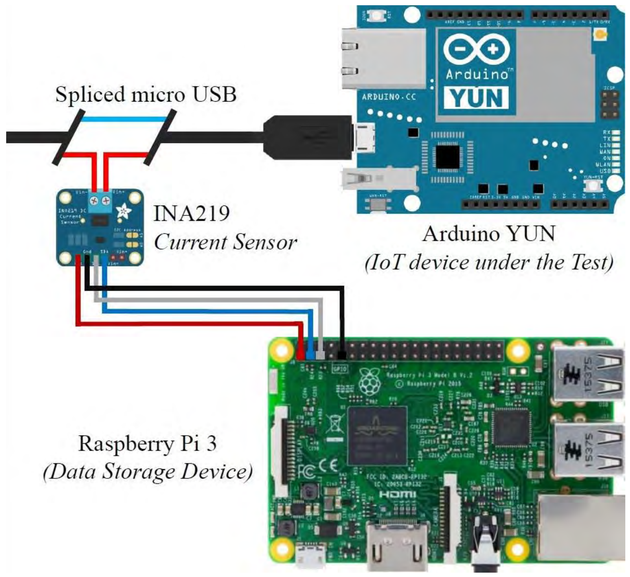
Raspberry Pi 0

The following device is used for the research:

1. IoT device under test (shown above)
2. Measuring device: Current Sensor (INA219)
3. Storage device: Raspberry Pi 3 (Model B)

TestBed Setup

- The power cord of the IoT device in question is connected to the current sensor INA219, as shown below
- The current sensor collect the measurement and send it to the storage unit.
- The IoT device is monitored for 1 hour and we collected 36000 measurements per device in each mode.



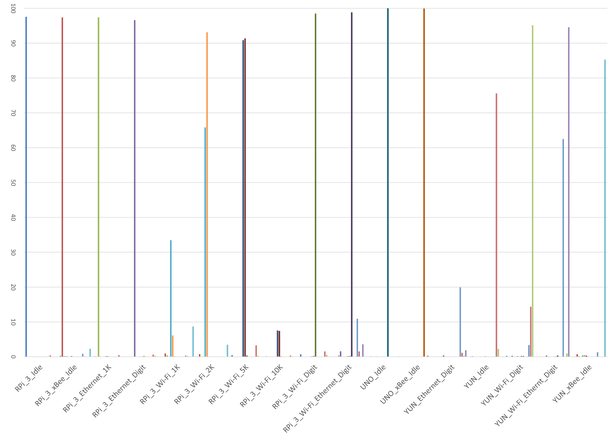
V. Result

- The attributes obtained from the data includes the following: Current, Voltage, and Power.
- We feed this data to a machine learning algorithm for classification purposes.
- The data generated consist of 17 classes and a total of 612,000 data points
- The classifier employs supervised machine learning using Multilayer Perceptron.
- 90% of the data points are used as training samples.
- 10% is used as test samples for the classifier.
- The classifier shows:
  - 82% accuracy on the data points
  - 18% data points are wrongly classified.

IoT Device and Mode (Class)	Total Data Respective Points	% Correctly Classified	% Wrongly Classified
Raspberry_Pi _3_Idle	3578	0.976	0.024
Raspberry_Pi_3_xBee_Idle	3579	0.974	0.026
Raspberry_Pi_3_Ethernet_15secMessage_1k	3623	0.974	0.026
Raspberry_Pi _3_Ethernet_15secMessage_Normal	3564	0.966	0.034
Raspberry_Pi_3_WiFi_15secMessage_1k	3632	0.330	0.670
RaspberryPi_3_WiFi_15secMessage_2k	3664	0.931	0.069
Raspberry_Pi_3_WiFi_15secMessage_5k	3517	0.908	0.092
Raspberry_Pi_3_WiFi_15secMessage_10k	3566	0.070	0.930
Raspberry_Pi_3_WiFi_15SecMessage_Normal	3586	0.985	0.015
Raspberry_Pi_3_WiFi_Ethernet_15SecMessage	3621	0.988	0.012
UNO_Idle	3725	1.000	0.000
UNO_xBee_Idle	3627	0.999	0.001
YUN_Ethernet_15SecMessage_Normal	3549	0.200	0.800
YUN_Idle	3648	0.756	0.244
YUN_WiFi_15SecMessage_Normal	3513	0.952	0.048
YUN_Ethernet_WiFi_15SecMessage	3616	0.946	0.054
YUN_xBee_Idle	3617	0.853	0.147

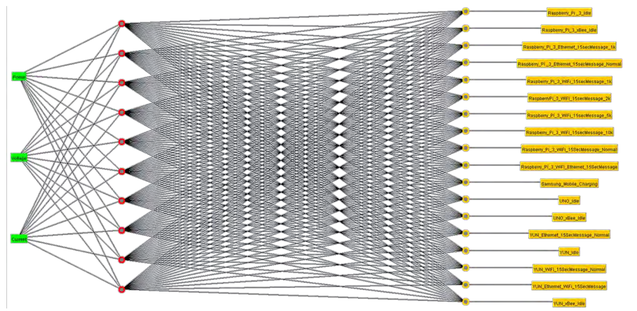
From the graph below, it is depicted

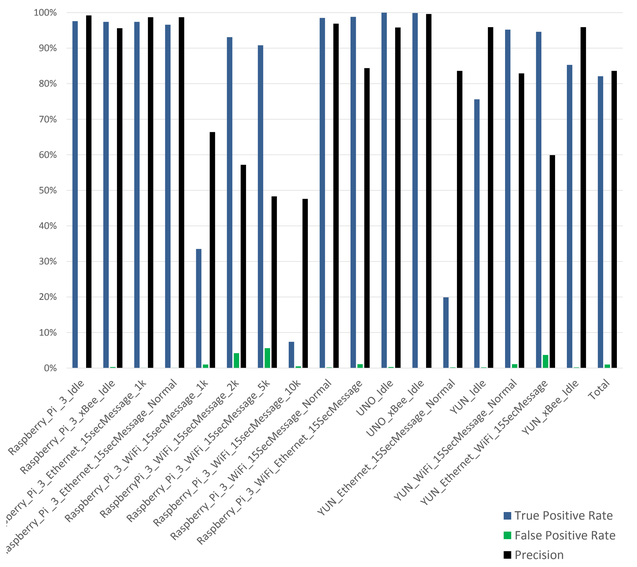
- The classifier correctly classify all UNO device (100%).
- The average device classification is more the 80%
- Some classes poorly classified, the algorithm cannot distinguish between some of classes.



VI. Conclusion

- Neural Network used for classification purposes.
- Total true positive rates is 82%.
- Total precision is 84%.
- Total false positive is 1%.
- The algorithm correctly classifies most classes.





VII. Acknowledgment

Funding partially provided by Tennessee Tech University, College of Engineering for achieving Carnegie classification.

References

[1] Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. "Internet of things (IoT) security: Current status, challenges and prospective measures." In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for, pp. 336-341. IEEE, 2015.

[2] Sedjelmaci, Hichem, Sidi Mohamed Senouci, and Tarik Taleb. "An Accurate Security Game for Low-Resource IoT Devices." IEEE Transactions on Vehicular Technology 66, no. 10 (2017): 9381-9393.

[3] Sedjelmaci, Hichem, Sidi Mohammed Senouci, and Mohamad Al-Bahri. "A lightweight anomaly detection technique for low-resource iot devices: A game-theoretic methodology." In Communications (ICC), 2016 IEEE International Conference on, pp. 1-6. IEEE, 2016.

[4] Stiawan, Deris, Mohd Yazid Idris, Reza Firsandaya Malik, Siti Nurmaini, and Rahmat Budiarto. "Anomaly detection and monitoring in Internet of Things communication." In Information Technology and Electrical Engineering (ICITEE), 2016 8th International Conference on, pp. 1-4. IEEE, 2016.