Reinforcement Learning for Cyber Security Use Cases

Project Supervisor :

Dr. Om Prakash Vyas

Group Members :

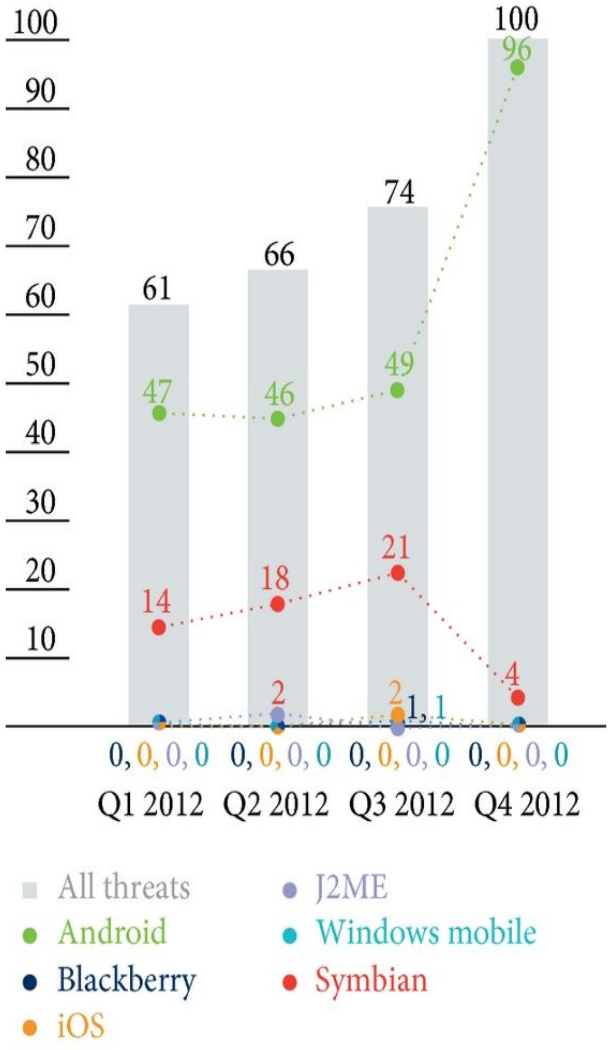
IIT2016053 - Surabhi Gogte
IIT2016088 - Simran Gill
IIT2016103 - Chahak Sharma

Project Objective

Propose a reinforcement learning model for cyber security issues and compare it with the previous models done using Deep Learning.

Motivation

- Recent studies show that the amount of malware that targeted other mobile platforms gradually decreased , whereas Android showed a contrasting result.
- The reason for the increase in Android malware was its open source policy and its leniency to market application verification .
- The main motivation behind this research is to apply reinforcement learning for cyber security issues and compare it with the previous works done using Deep Learning.



LITERATURE REVIEW

Feed-Forward Network Model

- This model identified Android Malware in APK files using Feed-Forward Neural Network.
- The units in input to hidden layer and hidden to output layer were fully connected.
- ReLu(Rectified Linear Unit) acted as a non-linear activation function with sigmoid function in the final fully connected layer.
- 5 layer DNN was used in the model.
- The model detected android malware with 94% accuracy and precision of 0.834 .

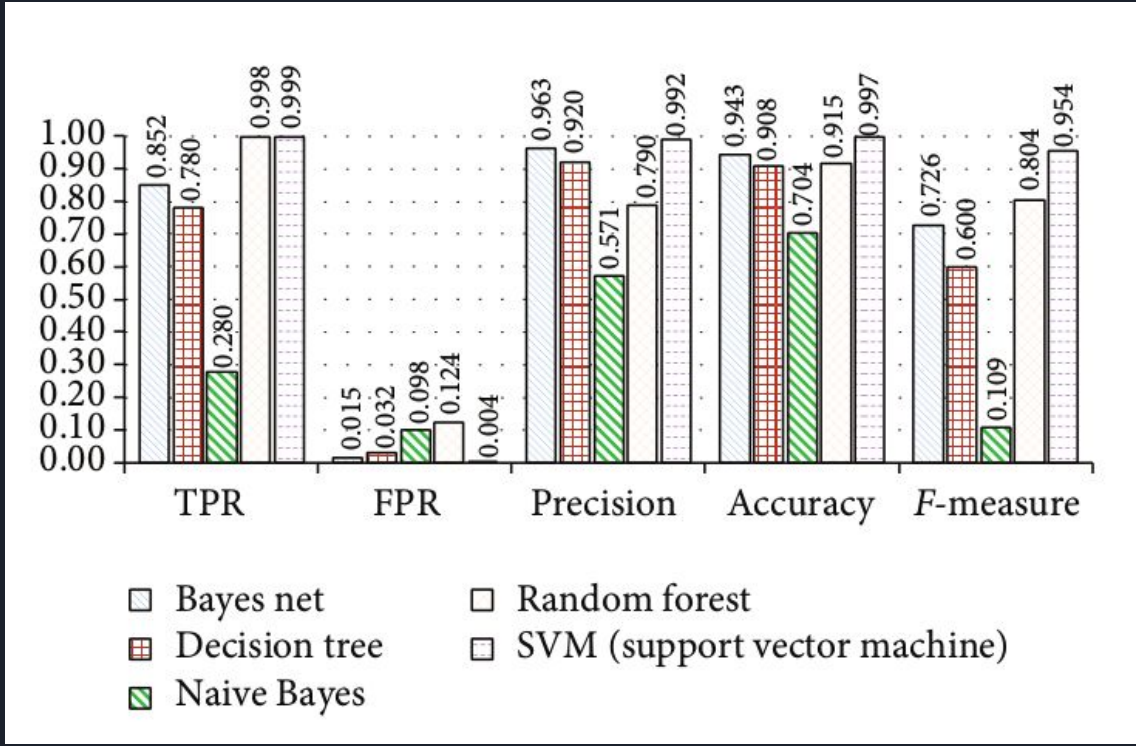
Deep Belief Networks

- The multiple layers of graphical model have both directed and undirected edges.
- The layers compose of hidden units, where each layers are connected with each others but units are not.
- It performs a greedy layer-wise unsupervised pre-training.
- The model gave 99.4% detection accuracy.

Linear Support Vector Machine

- Traditionally, signature-based, behavior based and dynamic analysis techniques have been used for malware detection.
- Behavior-based detection involves the inconvenience of having to determine malware infection status by examining numerous features.
- Using Machine Learning, classification is automated thereby providing more accuracy and precision.
- Of the input features, unnecessary ones are removed by the SVM machine learning classifier itself and the modeling is carried out.
- For SVM True Positive Results came to be 0.999 with 99.7% accuracy and precision of 0.992 .

Comparison with other ML Algorithms



PROPOSED METHODOLOGY :

Reinforcement Learning

Dataset

- We would be using The Drebin Dataset to train our Reinforcement Learning Model.
- Dataset consisting of feature vectors of 215 attributes extracted from 15,036 applications (5,560 malware apps from Drebin project and 9,476 benign apps).
- Contains 5560 malware files collected from August 2010 to October 2012.
- All malware samples are labeled as 1 of 179 malware families.
- Drebin is one of the most popular benchmark datasets for Android malware detection.

Reinforcement Learning Preliminary

- Concept of state,action, and reward.
- It is a trial and error approach .
- Agent takes action at each time step that causes two changes :
  - current state of the environment is changed to a new state,
  - agent receives a reward or penalty from the environment.
- Given a state, the reward is a function that can tell the agent how good or bad an action is.
- Based on received rewards, the agent learns to take more good actions and gradually filter out bad actions.

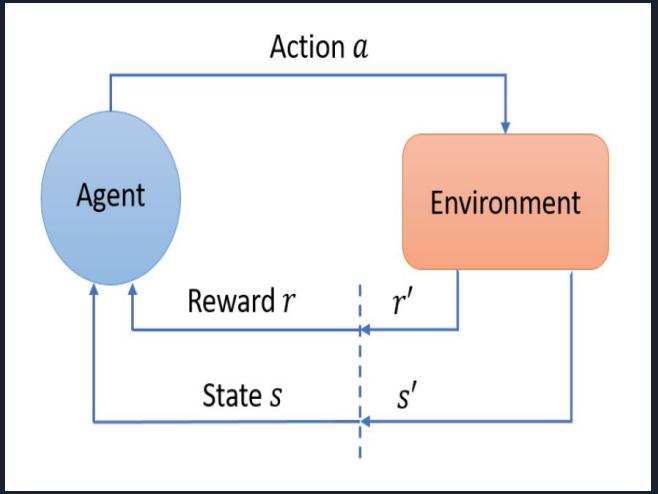
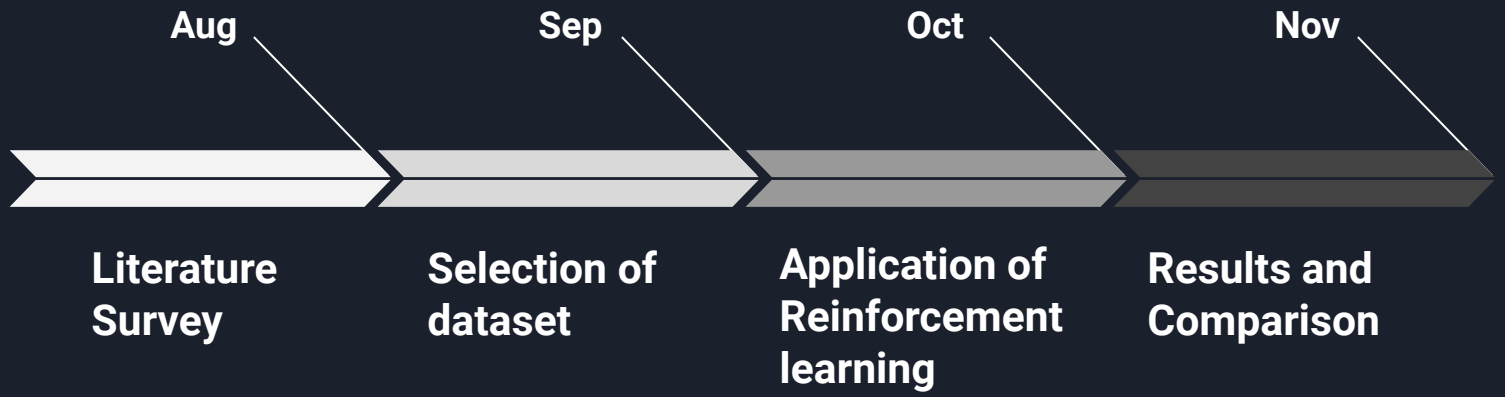


Fig. Iterative process of agent-environment interactions.

Project Timeline



References

1. https://arxiv.org/pdf/1812.03519.pdf
2. https://ieeexplore.ieee.org/document/7846953
3. http://dx.doi.org/10.1155/2014/594501
4. https://www.sec.cs.tu-bs.de/~danarp/drebin/
5. https://www.researchgate.net/publication/333773807_Deep_Reinforcement_Learning_for_Cyber_Security
6. http://web.mst.edu/~gosavia/joc.pdf
7. https://ieeexplore.ieee.org/document/8405026


THANKYOU !