Using Deep Learning to Classify Power Consumption Signals of Wireless Devices: An Application to Cybersecurity

A. Albasir, R. Soundar Raja James, K. Naik & A. Nayak
University of Waterloo, Canada

Motivation

- Smartphones are people's preferred means of performing online banking and health monitoring

- This makes them next big targets of malicious software and security attacks:
  - Over ½ a billion personal information records are stolen or lost in the recent couple of years (at a cost of ~ $315 B)
  - Malwares are becoming more sophisticated and adaptive, which make them go undetected with traditional approaches

- Due to wireless devices limited resources , the task of detecting malwares on-board is becoming more challenging

We propose a proof-of-concept deep learning based approach to detect malware in Smartphone by monitoring its consumed power

Background

The general approach to Malware (anomaly) Detection:

Monitoring → Analysis → Decision

		Data Collection Mechanism (Monitoring)	
		On – Device	Off – Device
Running of the Algorithm (Analysis & Decision)	On – Device	✓	X
	Off – Device	✓	✓ (our approach)

Collected data: OS call traces [1], Network info. [2], Device's power consumption [3], or Device's EM radiation[4]

Drawbacks of traditional techniques: Intrusive, Computationally expensive, Malware can imitate benign apps

Solution Strategy & Method

- ✓The solution strategy in this work relies on the hypothesis that every piece of software, whether malware or benign, will have a trace in the power consumption of the mobile device
- ✓This argument makes it inevitable for malware to go undetected having the right approach to process and analyze power signals
- ✓We treat device's power consumption as a signal carrying insightful information about its operational health
- ✓Apply ML and DL to detect malicious behaviors

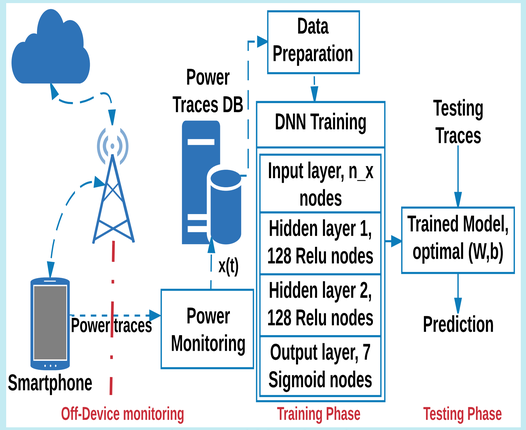


Fig.1: Deep learning model for malware detection

Experimental Set-up

For Validation: Detecting Emulated Malware on Smartphone

- Non-adaptive malware

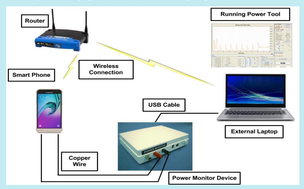
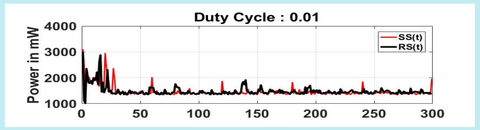
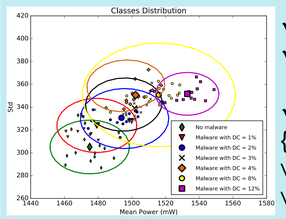


Fig.2: Test bench [3]

- Duty Cycle = $T_{ON}/(T_{ON}+T_{OFF})$
- Duty Cycle represents activity period of the malware

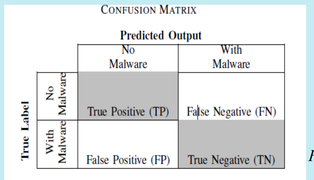




- ✓**The dataset as follows [3]:**
- ✓$\{x, y\}_{i=1}^{m}, where\ y \in C = \{0,1,2,3,4,8,12\}$
- ✓**7 classes**

{No Malware, Malware with DC = 1%, Malware with DC = 2%, and so on,

Results



$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F\text{-}measure = \frac{2 * precision * recall}{precision + recall}$$

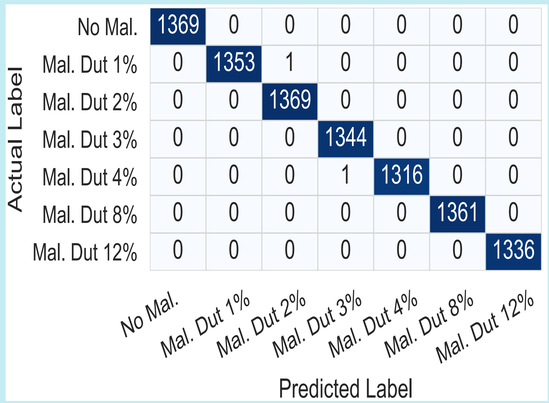


Fig.4: Confusion matrix of nx=5000 samples/trace and measurement sampling frequency Fs =5000 samples/sec

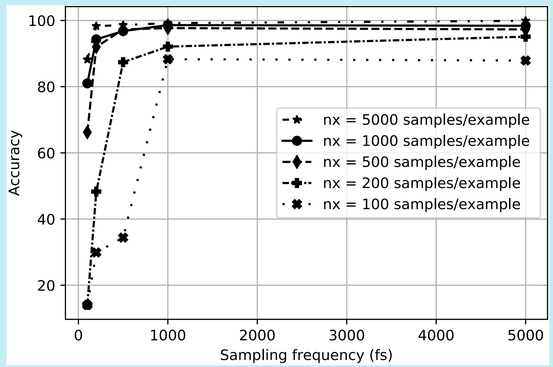


Fig.5: Detection accuracy vs sampling rate

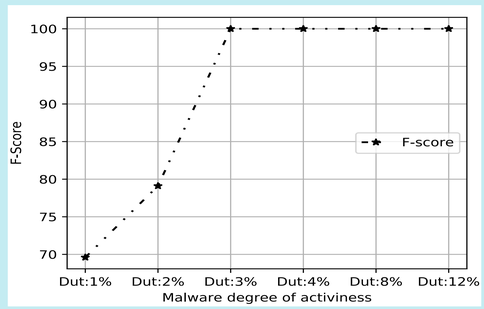


Fig 6: Results of SVM for Malwares with different Duty Cycles [3]

The results show:

- ✓**The impact of measurements' sampling freq. (f_s) and measur. window size (n_x) on the detection accuracy**
- ✓ **DL performance on raw data surpasses ML performance on processed data**
- ✓**DL was not only able to detect malware with high accuracy, but was also able to to differentiate the degree of activity of each malware**

Summary

This work presents a new proof-of-concept smartphone malware detection technique. The results were promising and show a potential of applying this technique to detect more insights about the smartphone operational state (e.g. hardware failure). As a next step, we will validate our approach using real malwares and including other apps to build more realistic scenarios.

Contact:

Abdurhman Albasir
PhD candidate, University of Waterloo
Email: aalbasir@uwaterloo.ca

References

[1] Ahmet ˙Ilhan Aysüan and Sevil Sü en, "API call and permission based mobile malware detection," in Signal Processing and Communications Applications Conference, 2015 23th . IEEE, 2015, pp. 2400–2403.

[2] Shun Tobiyama, Yukiko Yamaguchi, Hajime Shimada, and et. al., "Malware detection with deep neural network using process behavior," in the 40th Annual IEEE Conference (COMPSAC) . IEEE, 2016.

[3] R. Soundar Raja James, A. Albasir, K. Naik, and et. al., "Detection of anomalous behavior of smartphones using signal processing and machine learning techniques," in 2017 IEEE 28th Annual International (PIMRC) , 2017.

[4] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic, "Eddie: Em-based detection of deviations in program execution," in Proceedings of the 44th Annual International Symposium on Computer Architecture. ACM, 2017, pp. 333{346.