Device Fingerprinting

Device Fingerprinting, accuracy using Convolution Nets and applications in security

By:
Dr Sandhya Aneja and Nagender Aneja

Universiti Brunei Darussalam
Brunei Darussalam

ORGANISATION OF PRESENTATION

- Definition
- Why Fingerprinting is important?
- Issues
- Existing Strategies
- Proposed Solution
  - Graphs of Inter Arrival Time (IAT) as Fingerprint
  - Evaluation of Proposed Scheme
- Future work and open issues

Definition

- Identifying a target device through its Wireless/Wired Traffic by generating a Signature
  - Without using IP Address or MAC address, that can be easily forged
- Active Approach
  - sending traffic to the target device
- Passive Approach
  - observing the traffic sent by the target device

Why Fingerprinting?

- Corporates implement MAC address based Internet Access
  - By spoofing MAC address, an Attacker can access the network
- Internet Service Provider sell hotspot time to MAC address and an attacker can steal MAC address
- Detecting Fake Access Point

Issues

- Device Fingerprinting is quite challenging on aspects of data collection and computation complexity

- Device type and vendor identification using supervised and unsupervised learning may not lead to desired accuracy since significant efforts are required to extract the features from captured communication

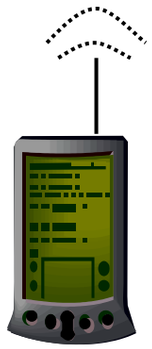
- Using features from different layers for device fingerprinting

Existing Techniques

- **LAN based Fingerprinting: GTID - A technique for physical device and device type fingerprinting,"**
  - A. S. Uluagac, S. V. Radhakrishnan, C. Corbett, A. Baca, and R. Beyah, IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 519–532, 2015.
  - statistical technique of making bins for the inter-arrival time (IAT) of packets of protocols like TCP, UDP etc First estimating the possible bins sizes of IAT used trained ANN with similarity measure to place the device into its identified class. Identification of bin sizes and some bins impose a challenge towards improving the rate of identification
- **Wireless Fingerprinting : Identifying unique devices through wireless fingerprinting**
  - L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, Proceedings of the first ACM conference on Wireless network security. ACM, 2008, pp. 46–55.
  - Time interval between frames is used to fingerprint the device followed by coarse and finer level clustering for classification. Also, in another latest approach, entropy analysis of bits in Probe Request frame of IEEE 802.11 WLAN used for generating the fingerprint of device.
- **IoT Sentinel: Automated device-type identification for security enforcement in IoT :**
  - M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, in Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017, pp. 2177–2184.
  - A fingerprinting approach which listens over the network and extracts 23 features from each packet. The features include ARP,LLC, IP, ICMP, ICMPv6, EAPoL, TCP, UDP, HTTP, HTTPS,DHCP, BOOTP, SSDP, DNS, MDNS, NTP, Padding,RouterAlert Size, Raw data, Destination IP counter, Source and Destination from all layers. The feature set is extended to 23X12= 276 by concatenating 12 contiguous packets to improve the granularity of the feature set.

Our Technique

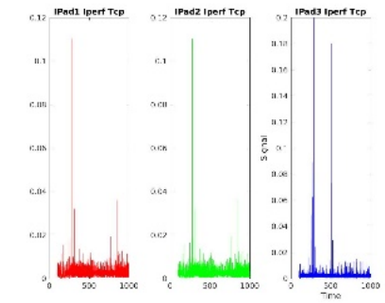
imac

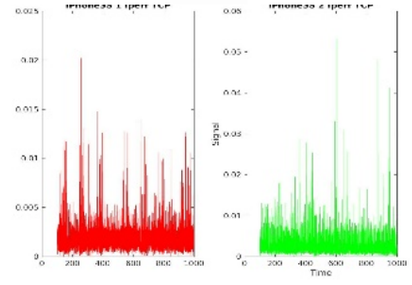


D

iphone

ipad



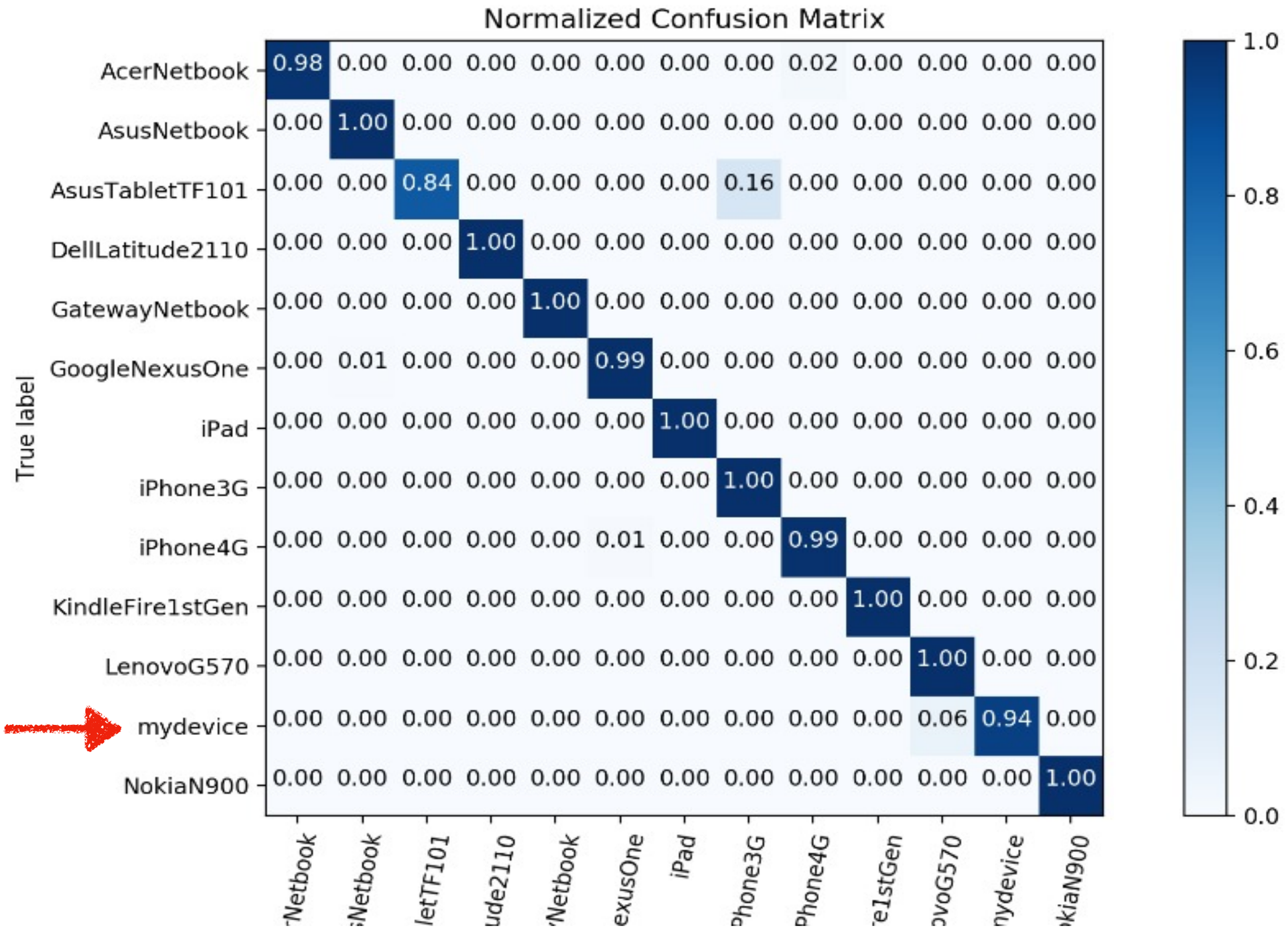


1000 milliseconds of IAT

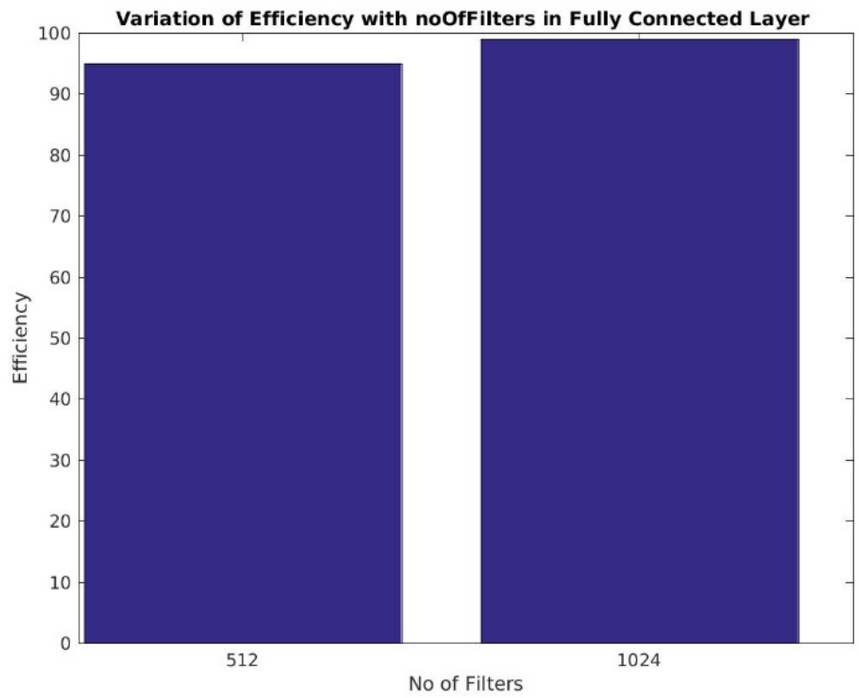
Parameters used in Convolution Network

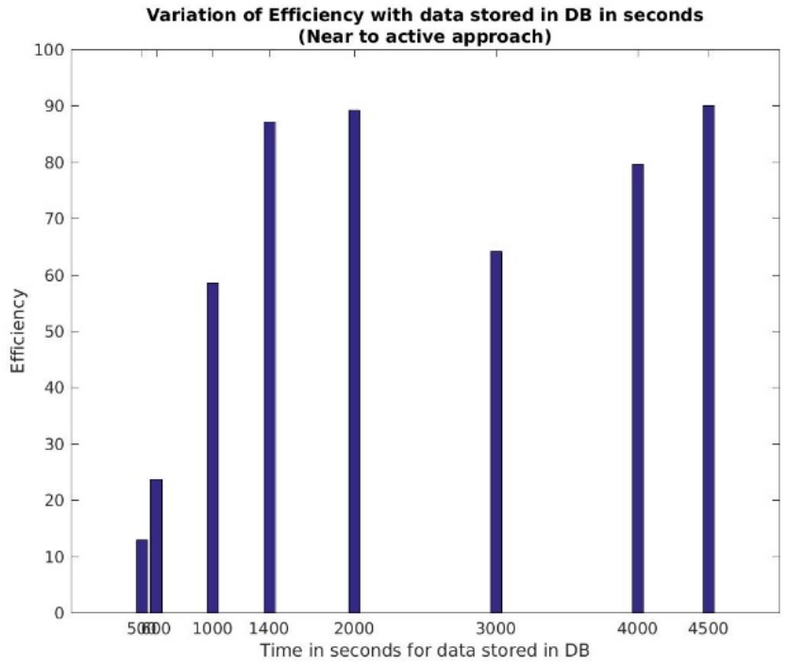
Sr. No.	Parameter	Value
1	Size of Image	50x50
2	Number of Convolution Layer	5
3	No. of Filters in each Layer	32,64,128,64,32
4	Parameters for each Convolution Layer	xf = 0, yf = 0; px = 0, py = 0; sx = 5, sy = 5;
5	No of pooling Layers	5
6	Parameters for each Pooling Layer	xf = 0, yf = 0; sx = 5, sy = 5;
7	No of Fully Connected Layers	1024
8	No of Fully Connected Layers with no of filters	1
9	Dropout %age in no of Fully Connected Layers	80%

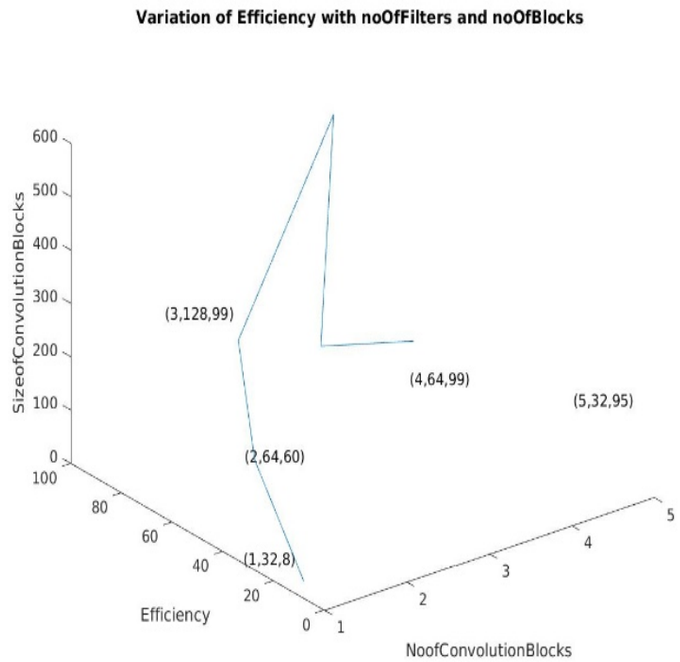
Confusion Matrix



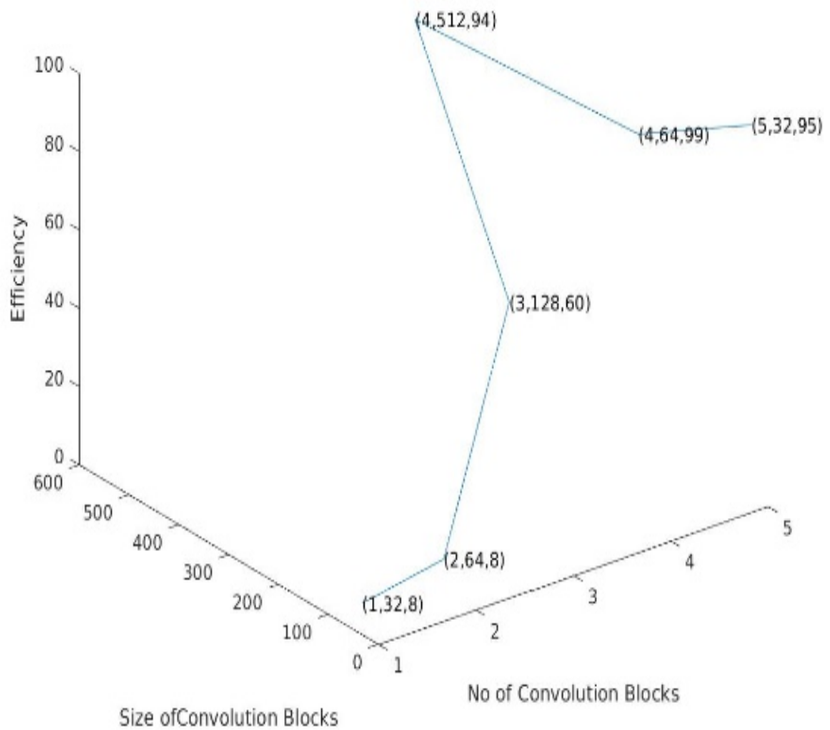
Results based on Variation of Parameters of Convolution Network during Training



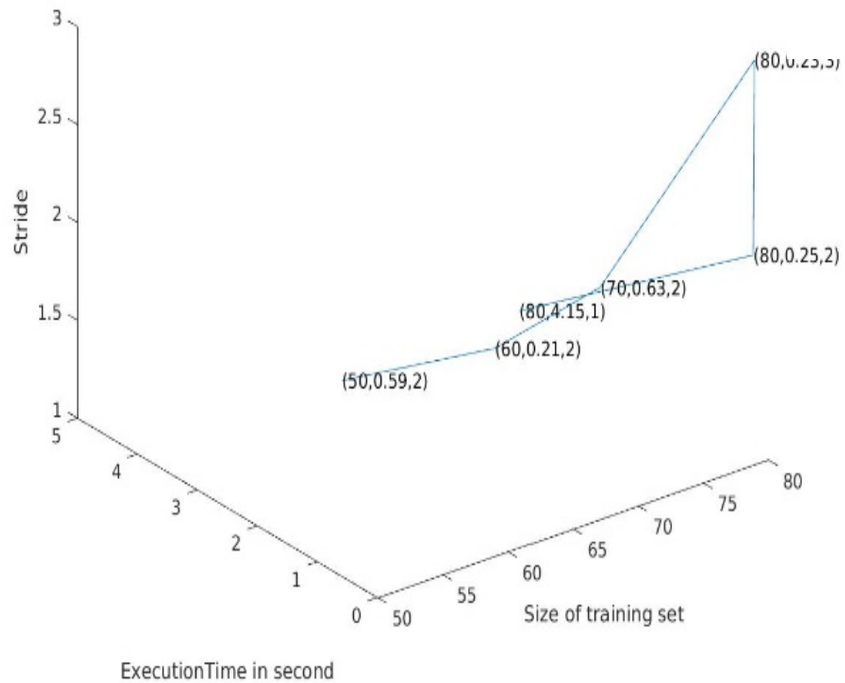




Variation of the Efficiency of the device identification with no of Blocks and size of Blocks



Execution time of model with Taining set size and stride



Future Work

- Improving the accuracy on real time network
- Include packets from Cellular Network, Wireless Network
- Improve the convolution network.
- Extend the model toward identifying packets of multi-hop wireless network
- Specific Device of one type (e.g. whose iPhone X) Identification at more finer level so that it could be fingerprint of a particular device

Thank You

Dr Sandhya Aneja[*] and Nagender Aneja[#]
[*]Faculty of Integrated Technologies, Universiti Brunei Darussalam
[#]Institute of Applied Data Analytics, Universiti Brunei Darussalam

[*]sandhya.aneja@ubd.edu.bn
[#]nagender.aneja@ubd.edu.bn