Deep learning for Minimal Context Classification of Block-types through Side-Channel Analysis

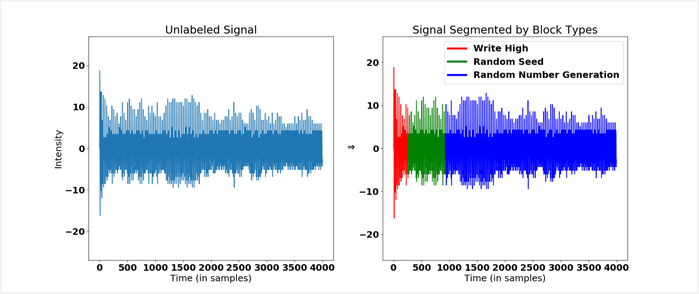
L. Jensen G. Brown X. Wang J. Harer S. Chin

Boston University

Goals and Motivation

- We desire to ultimately track the execution of programs using only the external electromagnetic (EM) and power side channels.
- Tracking program executions via side channels detected externally allows for the monitoring of devices whose hardware is incapable of self-monitoring. For example, Internet of Things (IoT) devices and other embedded systems which run on limited hardware.
- More precisely, in this work we aim to analyze the measurement time required to make meaningful predictions about program execution.

Data Labelling and Problem Statement

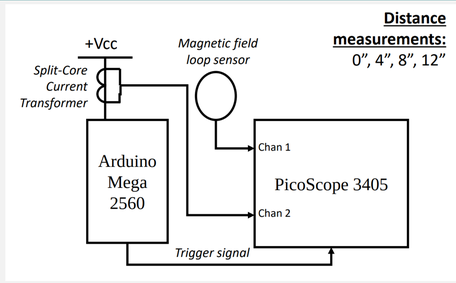


We ran two different programs in our experimental setup with the following block-types:

- Math program: write-low, write-high random number seed, random number generation, loop
- bit-toggle: write-low, write-high, loop

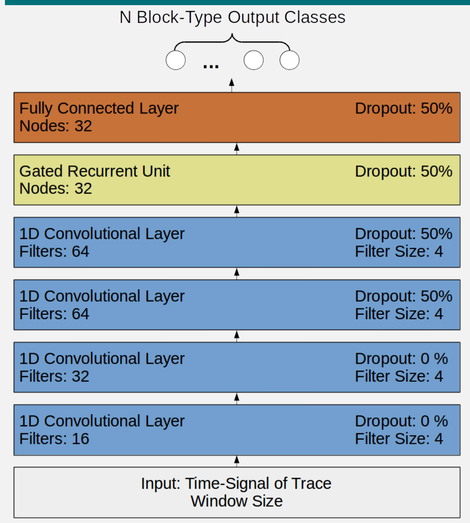
Each time of each measured sample was labelled with the appropriate block-type, the block-type running at that time. Thus, each sub-window of time in a program becomes its own classification problem.

Data Collection



The schematic for the experimental setup used to measure the EM and power side channels is shown to the left. Measurement were taken from 0", 4", 8", and 12" distances to observe the effect of noisy measurements on classification accuracy.

Network Architecture

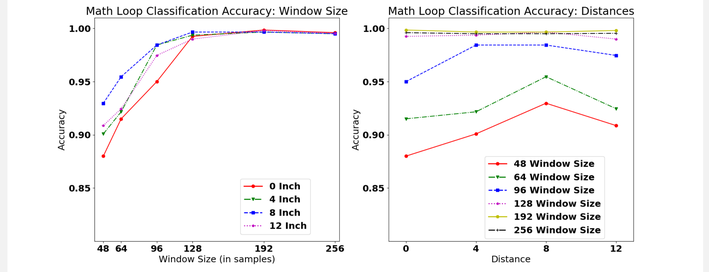


- The network architecture began with a fixed length input sequence.
- We used four 1D convolutional layers to pick up on signal features.
- We used a Gated Recurrent Unit layer to combine these features and to allow for the opportunity for variable length input.
- Finally a fully connected layer mapped to the N-labelled output classes for an N block-type labelled sample.

Windowing the Data

Because our dataset repeated program execution of the same couple programs many times, we were careful to avoid our model simply 'memorizing' the sequence of blocks that appear in those programs. Thus, when classifying the block-type at a time we only use a trailing sub-window of measurements. To analyze the effect of this window context on accuracy, we tested window contexts of 48, 64, 96, 128, 192, and 256 time samples in length.

Important Results



Shown above are classification accuracy results for varied window context and experimental measurement distance. The results above our for the math program.

- We see classification accuracy seem to converge at a window size of 128 or larger.
- This window size is equivalent to four clock cycles in our setup, and for this task we recommend this as the minimal context required to classify at full potential.
- Across distance we so no noticeable pattern or change in accuracy.

Outlook

- We are now tackling the problem of using unsupervised learning for side-channel analysis. The ability to analyze unlabelled side-channel data would improve the scalablity of applications.
- We also intend to attempt supervised instruction-level tracking, allowing for a more granular program analysis.
- Eventually we will aim to combine these objectives for unsupervised instruction-level tracking