Contactless Control Flow Monitoring via Electromagnetic Emanations

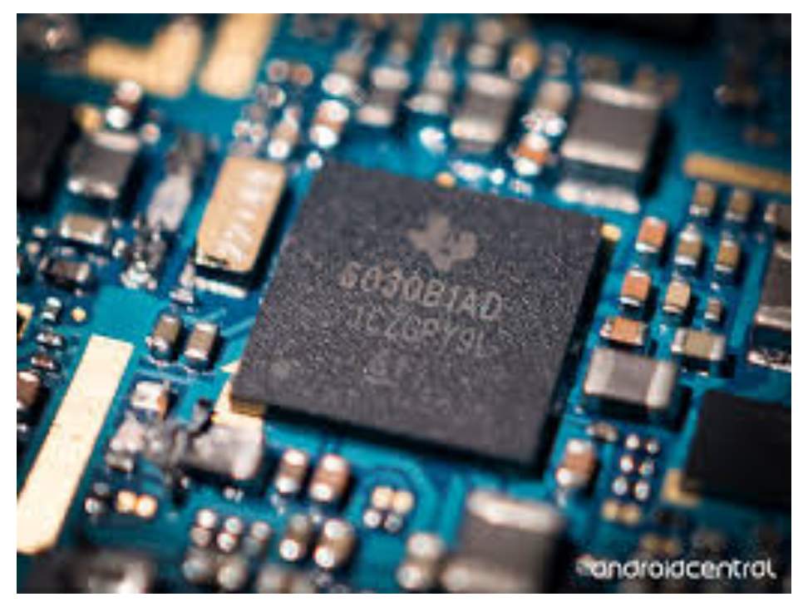
Yi Han, Sriharsha Etigowni, Hua Liu,
Saman Zonouz, Athina Petropulu

Work supported by NSF under grant CPS-1739467

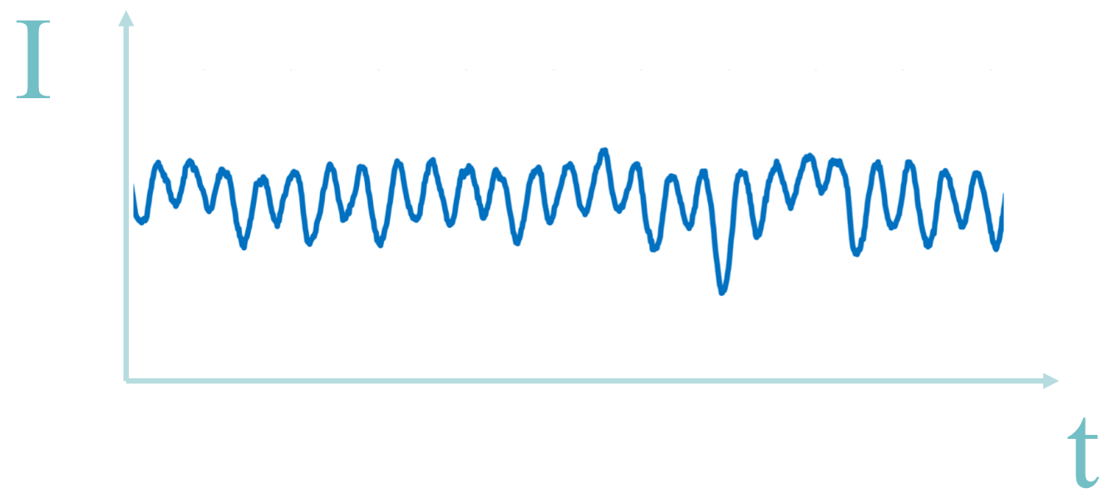
Overview

- ❑ We propose a runtime control flow monitoring system for programmable logic controllers (PLC) using unintentional electromagnetic emanations (EM).
- ❑ Our system can capture dynamic execution information while stays away from the target PLC such that won't cause resource overhead[1].
- ❑ We evaluate our system on various control logic programs and achieve an accuracy of **99%**.

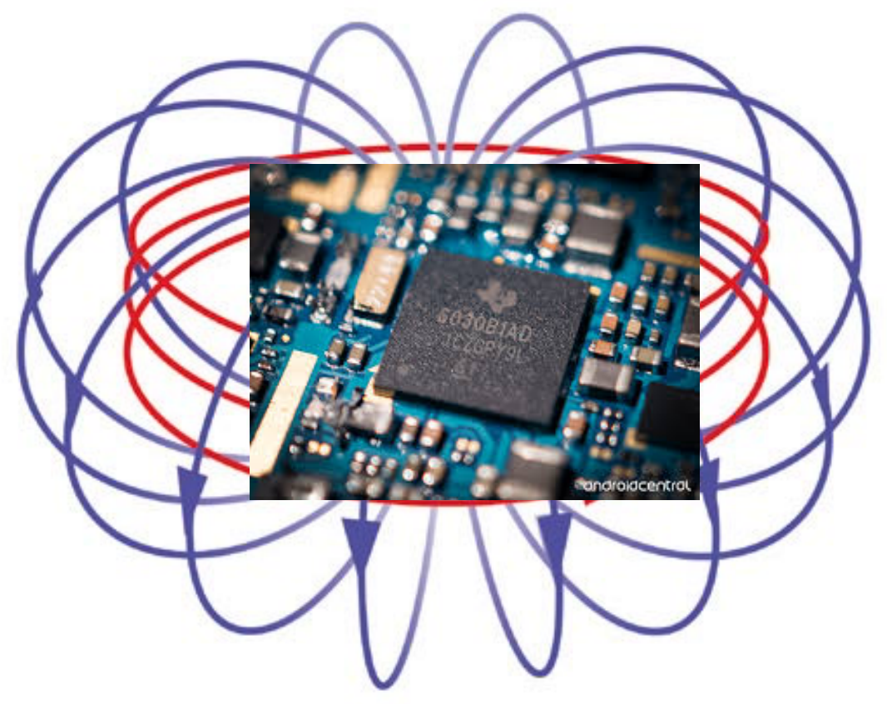
EM Emanations



CMOS components



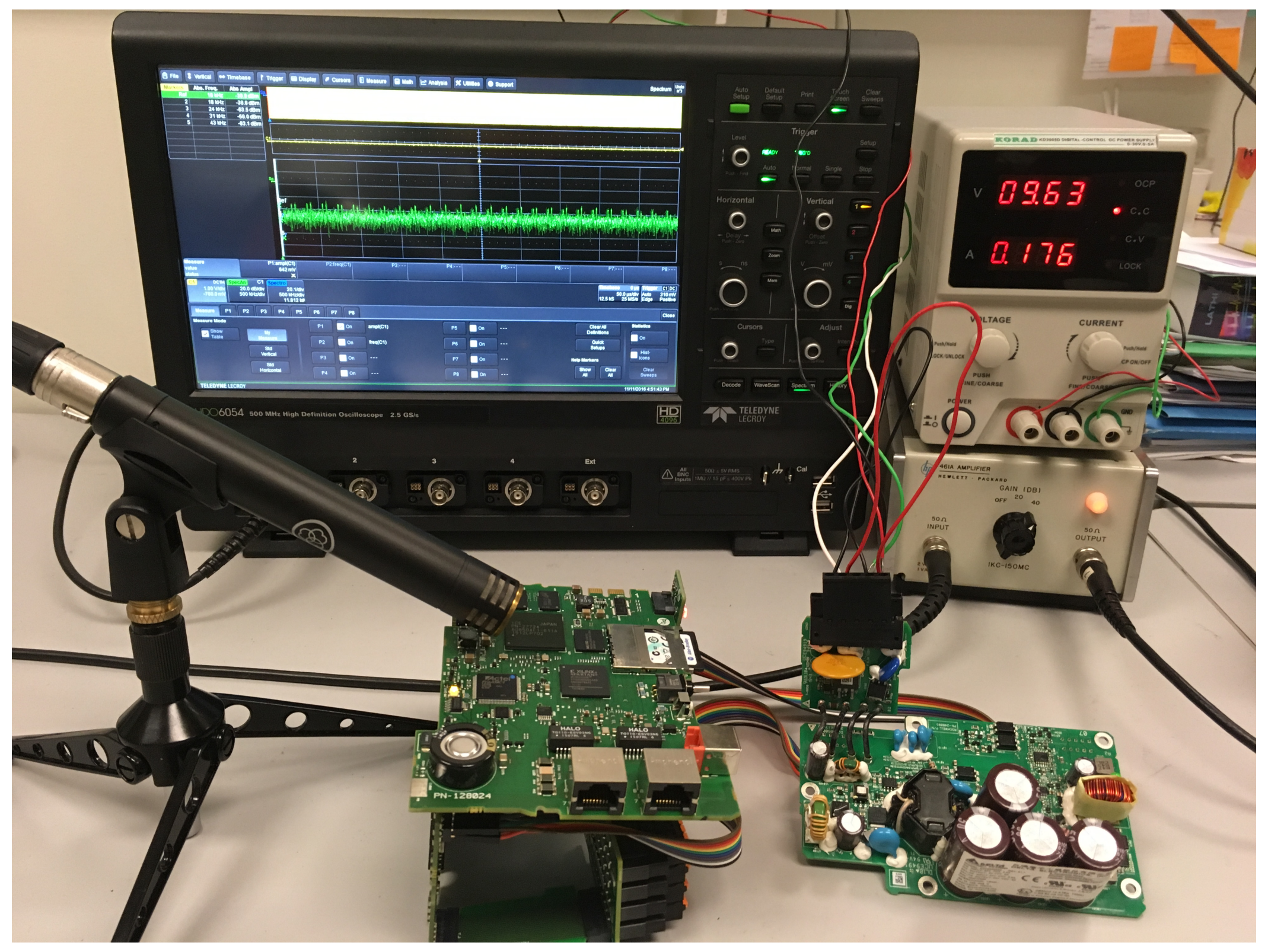
Change of current



Electromagnetic field

- ❑ Switching on and off of CMOS components cause change of current, which transmit to the ambient air in the form of EM field.
- ❑ Different instructions have unique emanation patterns due to utilization of different processor resources.
- ❑ EM signals have unique characteristics according to the runtime control flow.

Experimental Setup



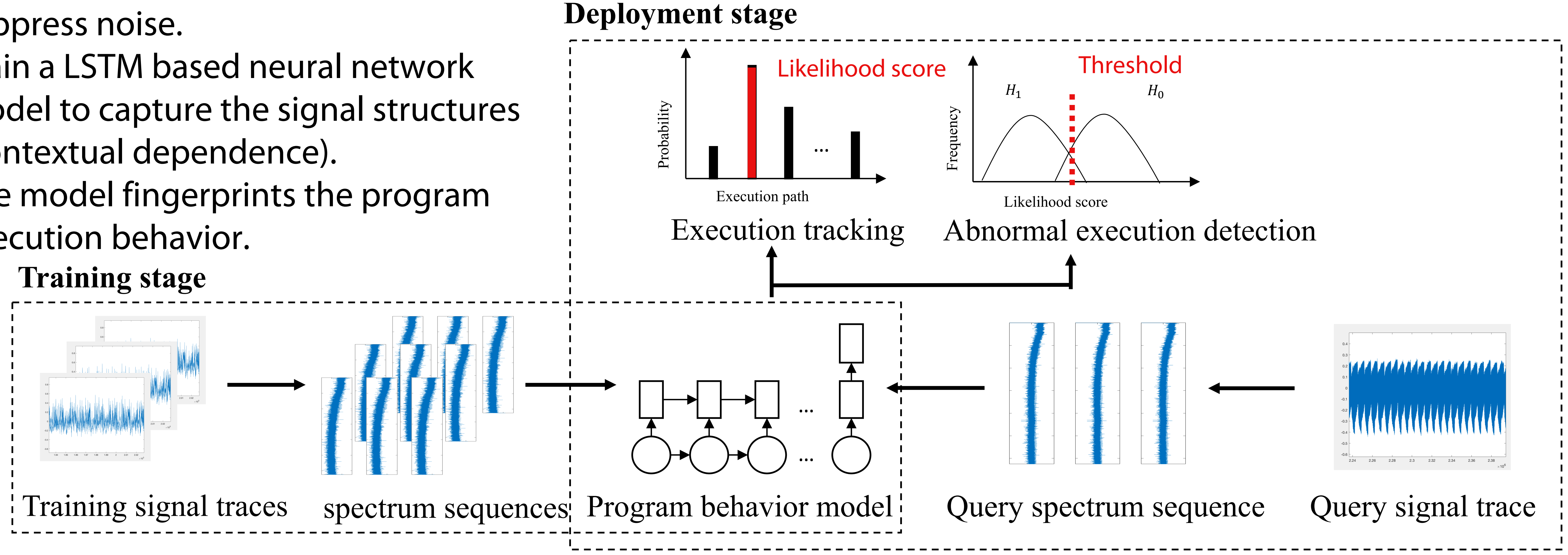
- ❑ Specs:
  - Allen Bradley PLC.
  - AKG P170 microphone.
  - HP-461A amp 40 dB gain.
  - Teledyne Lecroy HDO6054 oscilloscope 50 MHz.

Acknowledgement

We would like to thank National Science Foundation (NSF) for sponsoring our work.

The proposed system

- ❑ Capture EM emanations during program executions that correspond to various execution paths.
- ❑ Extract signal segments that describe the local characteristics using a sliding window with overlap.
- ❑ Convert signal segments into spectra to suppress noise.
- ❑ Train a LSTM based neural network model to capture the signal structures (contextual dependence).
- ❑ The model fingerprints the program execution behavior.



Results

- ❑ Compared frequency and time representation, proposed LSTM and an HMM approach[2].

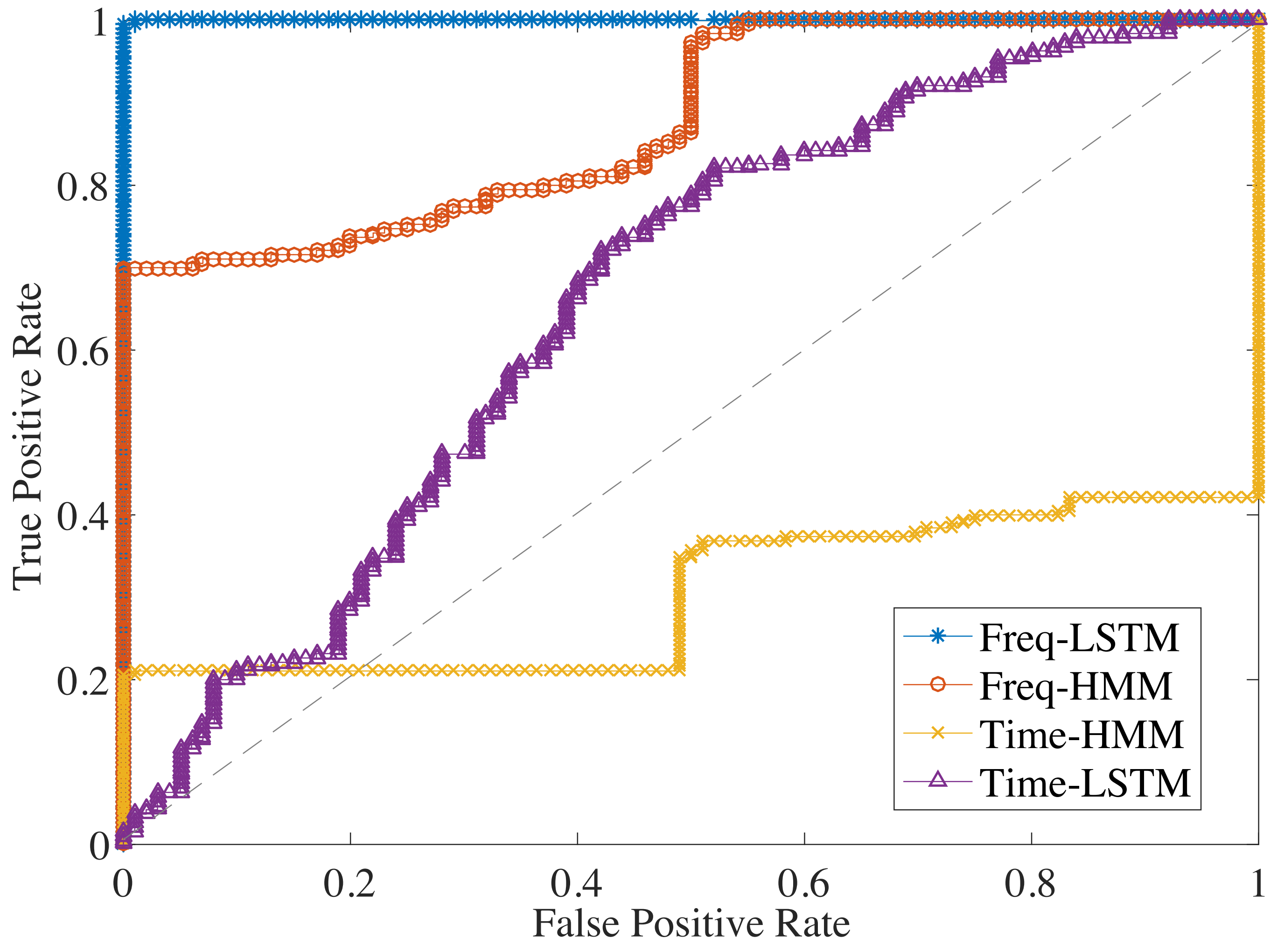


Fig. 1. ROC curve of the detection system.

Program	Time_HMM	Time_LSTM	Freq_HMM	Freq_LSTM
Matrix	55%	52%	60%	**100%**
Q-sort	49%	60%	41%	**100%**
GD	40%	64%	40%	**98%**
Newton	48%	51%	63%	**100%**
Conv	57%	69%	56%	**100%**
DCT	53%	45%	51%	**94%**
Dijkstra	62%	72%	65%	**100%**
AES	50%	50%	67%	**98%**
PID	40%	62%	71%	**99%**
Partfilt	51%	45%	67%	**100%**

Fig. 2. Execution tracking accuracy of the programs

- ❑ Discussion:
  - Frequency representation is considered to be more discriminative.
  - Sequential neural network model captures longer data dependence.

References

[1] Nazari, Alireza, et al. "EDDIE: EM-Based Detection of Deviations in Program Execution." Proceedings of the 44th Annual International Symposium on Computer Architecture. ACM, 2017.

[2] Liu, Yannan, et al. "On code execution tracking via power side-channel." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016.