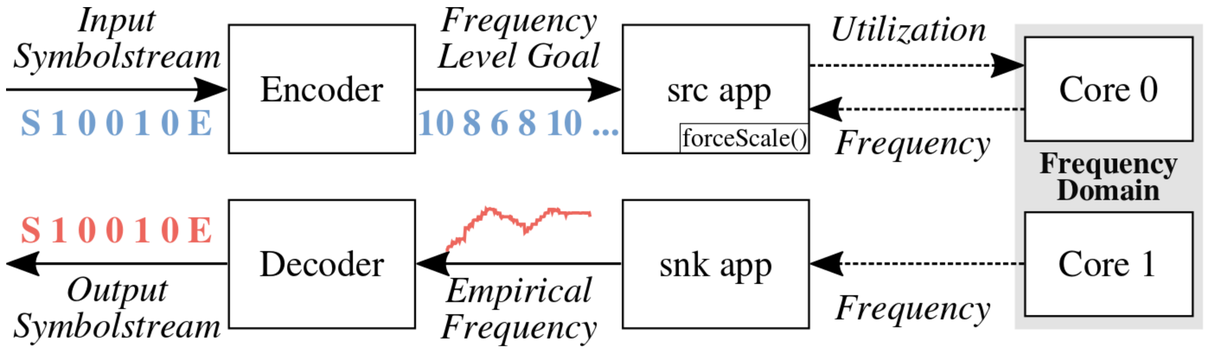
Frequency Scaling as a Security Threat on Multicore Systems

Philipp Miedl
Xiaoxi He
Matthias Meyer
Davide B. Bartolini
Lothar Thiele

Frequency Scaling as a Security Threat on Multicore Systems

Threat Model & Paper Contributions



Shows that application isolation can be broken. [1-3]

Paper Contributions:

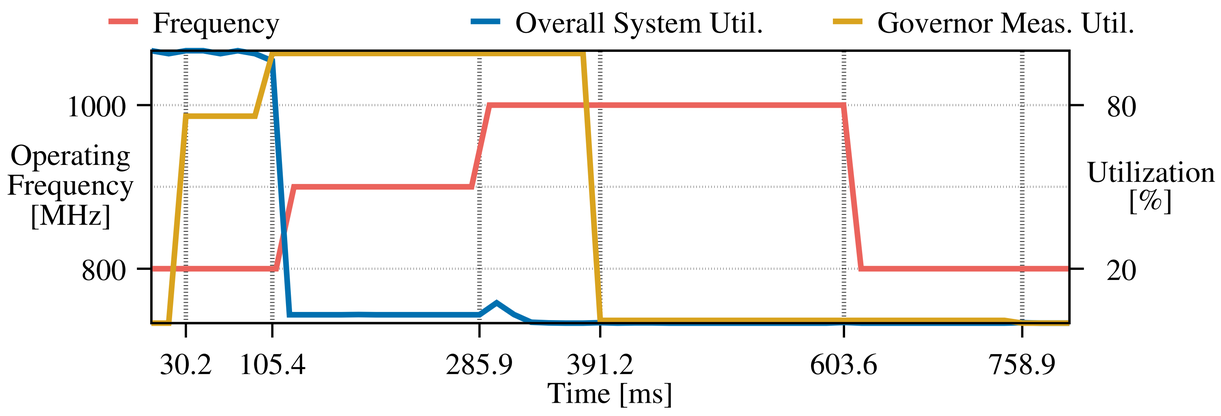
- Formal communication model and derivation of an upper capacity bound
- Usage of a Neural Network based decoder

Governor Implementation Artifacts

Desired frequency scaling 800 MHz ⇒ 900 MHz ⇒ 800 MHz

Unexpected governor behaviour:

- The governor uses an old utilization value at the call at 285.9 ms, resulting in frequency upscaling although the utilisation is low.
- Only one frequency scaling can be observed going from 1000 MHz to 800 MHz at the governor call at 603.6 ms.



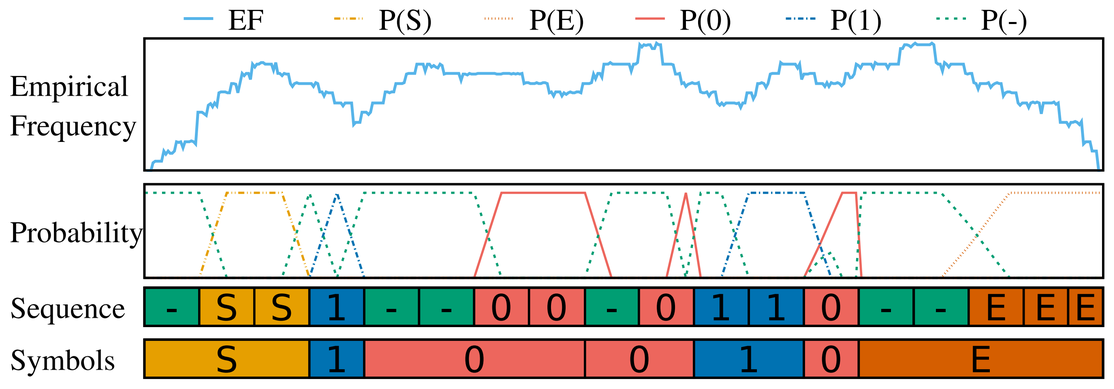
These implementation artifacts lead to a degradation of the throughput of the frequency covert channel.

Neuronal Network based Decoding

Channel characteristics prevent conventional decoder use. [1]

Neuronal Network based decoder

- Decoder based on Long-Short-Term-Memory neurons for Connectionist Temporal Classification (CTC) [4]
- Makes soft labeling decisions at each timestamp using the 5 labels S (preamble), E (postamble), 0, 1 and - (blank).



Neuronal Network decoder outperforms conventional static majority vote decoder.

Capacity Estimation

Derive an upper capacity bound from channel state diagram [2]:

$C = \log_2 \lambda_1$ [bits per channel use] $\qquad B_{\max} = \frac{C}{T_s}$ [bits per second]

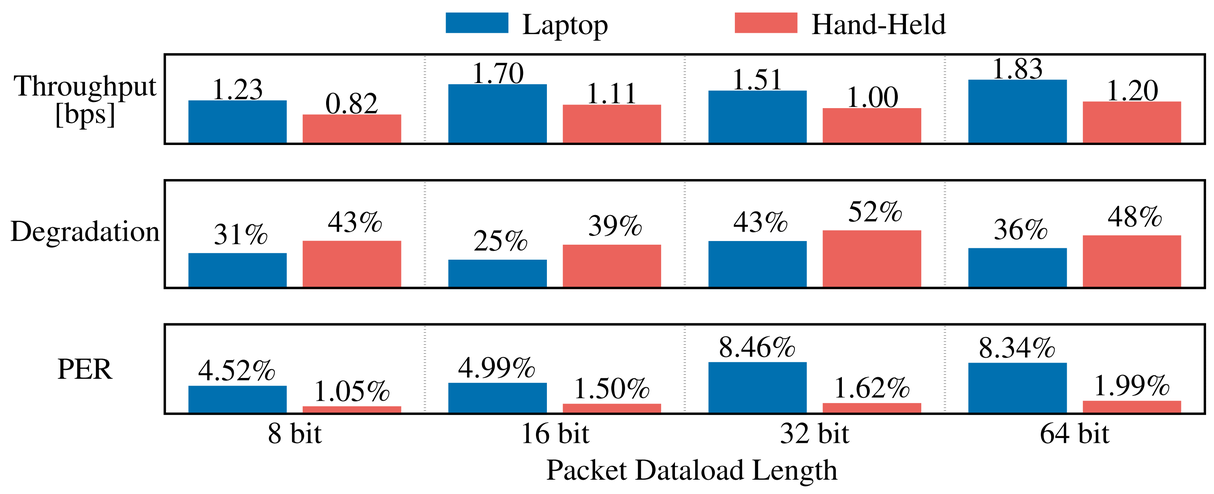
λ_1 . . . prinicpal right eigenvalue of the transition matrix

T_s . . . governor sampling rate

Laptop: $C = 0.972\,\text{bpcu} \Rightarrow B_{\max}(T_s = 80\,\text{ms}) = 12.15\,\text{bps}$

Hand-Held: $C = 0.982\,\text{bcpu} \Rightarrow B_{\max}(T_s = 100\,\text{ms}) = 9.82\,\text{bps}$

Evaluation



- Not ideal symbol coding causes low throughput
- Governor implementation artifacts cause throughput degradation
- Increasing error rate with increasing packet length
- Platform specific differences due to CPU architecture and OS

Despite low throughput, channel can be used to leak highly sensitive information

References

[1] P. Miedl, X. He, M. Meyer, D. B. Bartolini and L. Thiele, "Frequency Scaling as a Security Threat on Multicore Systems," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. IEEE, 2018. doi: 10.1109/TCAD.2018.2857038

[2] P. Miedl and L. Thiele. The Security Risks of Power Measurements in Multicores. In Proceedings of the 2018 ACM symposium on Applied computing. ACM, 2018.

[3] D. B. Bartolini, P. Miedl, and L. Thiele. On the Capacity of Thermal Covert Channels in Multicores. In Proceedings of the Eleventh European Conference on Computer Systems, EuroSys'16, pages 24:1–24:16, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-4240-7. doi: 10.1145/2901318.2901322. URL http://doi.acm.org/10.1145/2901318.2901322.

[4] A. Graves. Supervised sequence labelling. In Supervised sequence labelling with recurrent neural networks, pages 5–13. Springer, 2012.

ETH zürich
TIK Computer Engineering and Networks Laboratory
SAFURE

This project has received funding from the Eupopean Union's Horizon 2020 research and innovation programme under grant agreement No 644080. This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.