NETWORK INFORMATION HIDING

CH. 8: REPLICATION STUDIES

Prof. Dr. Steffen Wendzel

https://www.wendzel.de

Why Replicating Experiments?

- Replication studies …
  - allow to validate research results, either before or after their publication.
    - In some sciences, e.g. Psychology, there was even a replication crisis, where several (even standard textbook results) could not be replicated and were thus (partially) rejected.
  - allow to extend experiments and thus allow to gain more insights.

cf. Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Jean-Francois Lalande: Network Information Hiding and Science 2.0: Can it be a Match?, *Int. Journal of Electronics and Telecommunications*, Vol. 63(2), pp. 217-222, 2017.

Replicating Experiments

- Almost nobody seems to replicate experimental results of other researchers in the covert channel domain.
  - Manifold reasons, e.g. it is difficult to publish replication studies, no data available, no code available, no time, …
  - Replication studies should be honored as valid contributions in research.

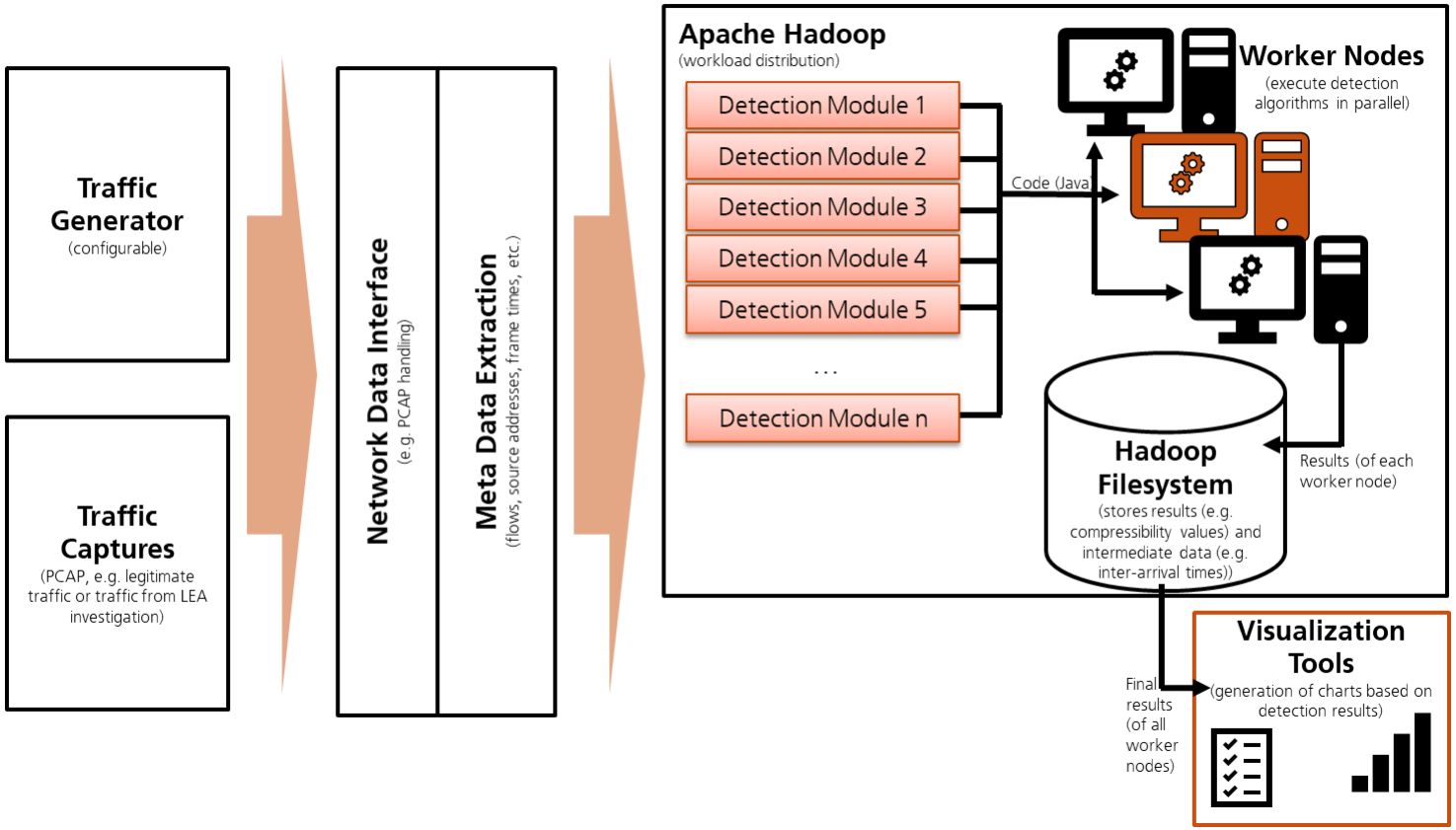
- But: How trustworthy are provided results during review and in papers?
  - Well, conference and journal quality is a good indicator, but not perfect.
  - Publisher name is not a good indicator, e.g. Springer, IEEE, ACM, … they all feature low-quality papers.

- Thus, we initiated the
  Int'l Workshop on Information Security Methodology and Replication Studies (IWSMR)

cf. Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Jean-Francois Lalande: Network Information Hiding and Science 2.0: Can it be a Match?, *Int. Journal of Electronics and Telecommunications*, Vol. 63(2), pp. 217-222, 2017.

Replicating Experiments on Covert Channels

WoDiCoF (*Worms Distributed Covert Channel Detection Framework*)



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

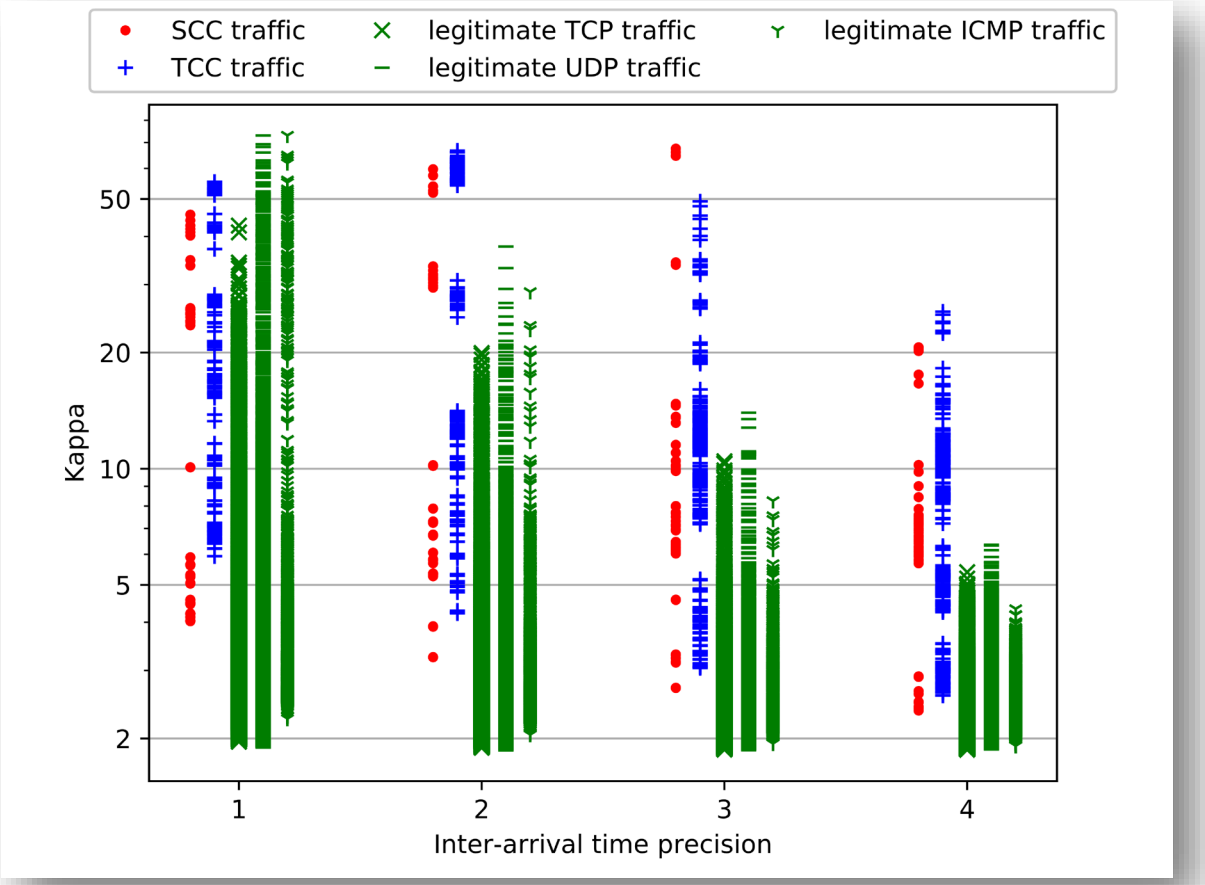
Replication Study: Compressibility of Cabuk et al.

- Published in ACM Transactions on Information and System Security (TISSEC), as an extended version of an ACM CCS paper.
  - 168/556 citations *(Aug-30-2021, src: Google Scholar)*
  - However, compressibility was only covered in the journal version.

R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Replication Study: Compressibility of Cabuk et al.

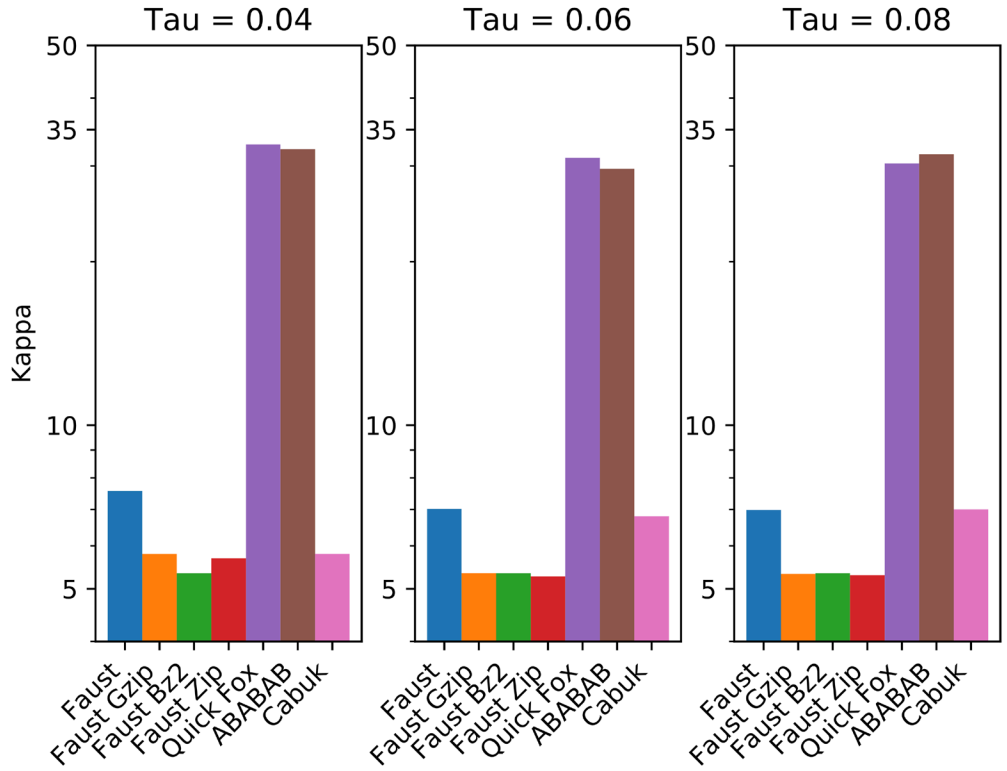
Let's see how the precision of the measured IAT values influences Kappa…



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Replication Study: Compressibility of Cabuk et al.

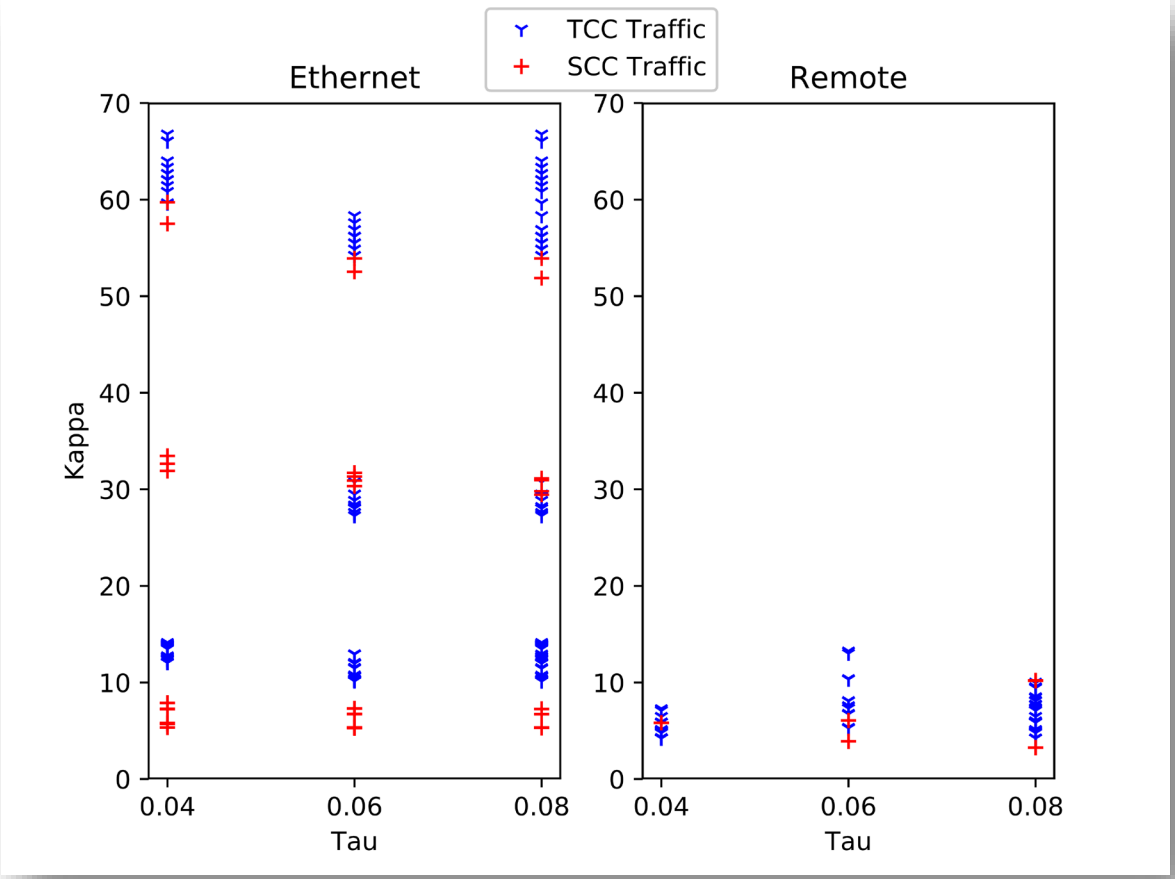
Let's see what happens if we transfer slightly different data over the covert channel …



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Replication Study: Compressibility of Cabuk et al.

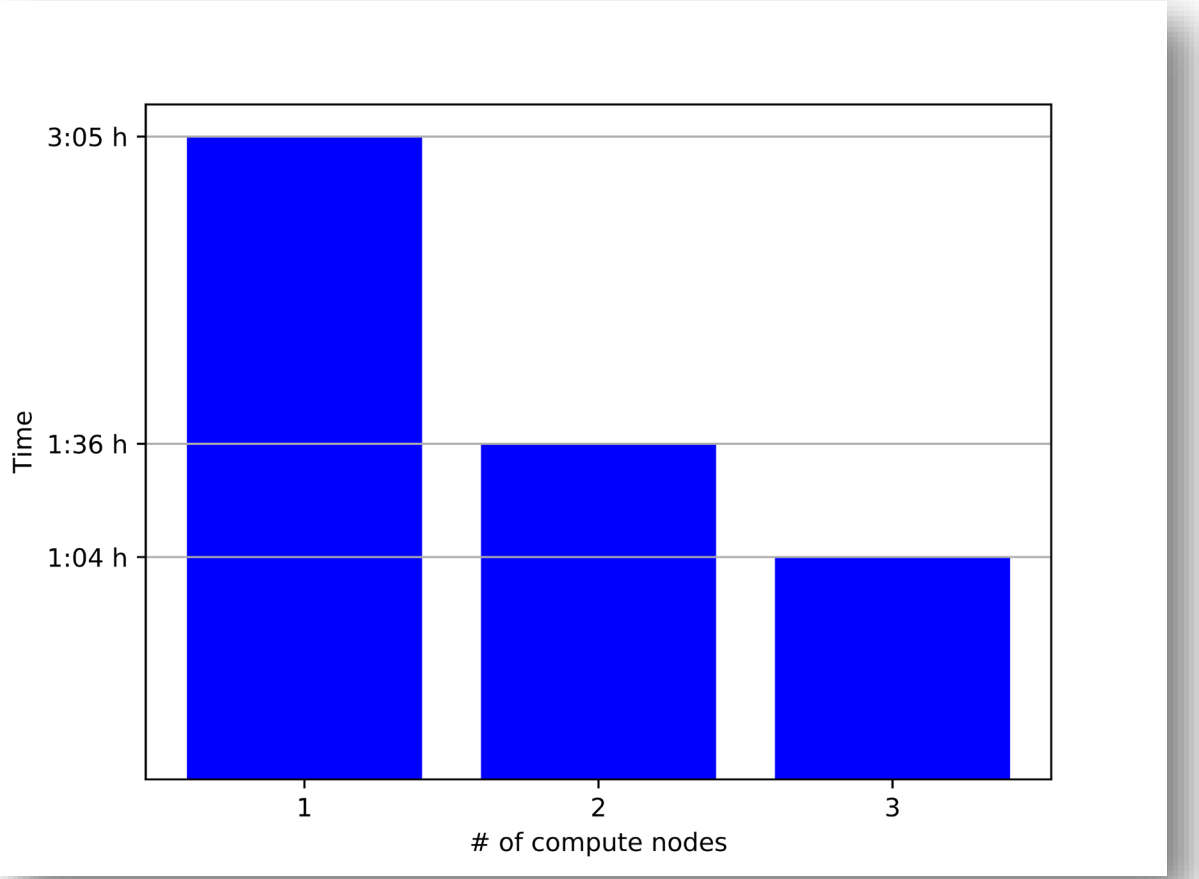
Let's see how Kappa differs when we utilize a different network connection …



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Finally: Testing Parallel Performance

Parallelization using Apache Hadoop with several gigabytes of PCAP recordings.



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Summary

- Replication can lead to new insights:
  - Even if previous work (such as in case of Cabuk et al.) is correct, replication studies can extend our understanding of how a method performs under different circumstances.
  - If previous work is indeed problematic, replication studies can reveal this fact.