Don‘t You Touch My Nuts:
Information Hiding in Cyber-physical Systems

Workshop on Bio-inspired Security, Trust, Assurance and Resilience (BioSTAR)
(IEEE Symp. on Security & Privacy Workshops 2017)
San Jose, CA, May 25th, 2017

Steffen Wendzel[1,2], Wojciech Mazurczyk[3,4], Georg Haas[1]

[1] Hochschule Worms, Germany
[2] Fraunhofer FKIE, Germany
[3] Warsaw University of Technology, Poland
[4] FernUniversität Hagen, Germany

Information Hiding & Cyber-physical Systems

Information Hiding:
Steganography, copyright marking, anonymity, obfuscation [1]

+

Cyber Physical Systems (CPS):
integrations of computation with physical processes [2]

=

Information Hiding in Cyber-physical Systems
(specially Steganography for CPS (**CPSSteg**))

Related Work (Chronological Order)

- *Wendzel/Kahler/Rist* (2012) [3]:
  Scenario identification and description of secret data transmission in networked buildings; MLS-based protection approach
- *Tuptuk/Hailes* (2015) [4]:
  Two covert channels (relying on modulation of transmission power and of sensor data) in persuasive computing.
- *Howser* (2015) [5]:
  Data leakage in CPS and MLS-based protection (DLP)
- *Tonejc/Güttes/Kobekova/ Kaur* (2016) [6]:
  Detection of selected covert channels in building automation networks using unsupervised machine learning methods.

Goals & Strategies

- **Goals:**
  - Determining **how much data can be hidden** in a CPS **and for how long**.

- **Possible Benefits:**
  - Storing secret data in a location where currently nobody will search for it, e.g. embedding a cryptographic key in a smart home.
  - *Fighting product piracy* [in progress]

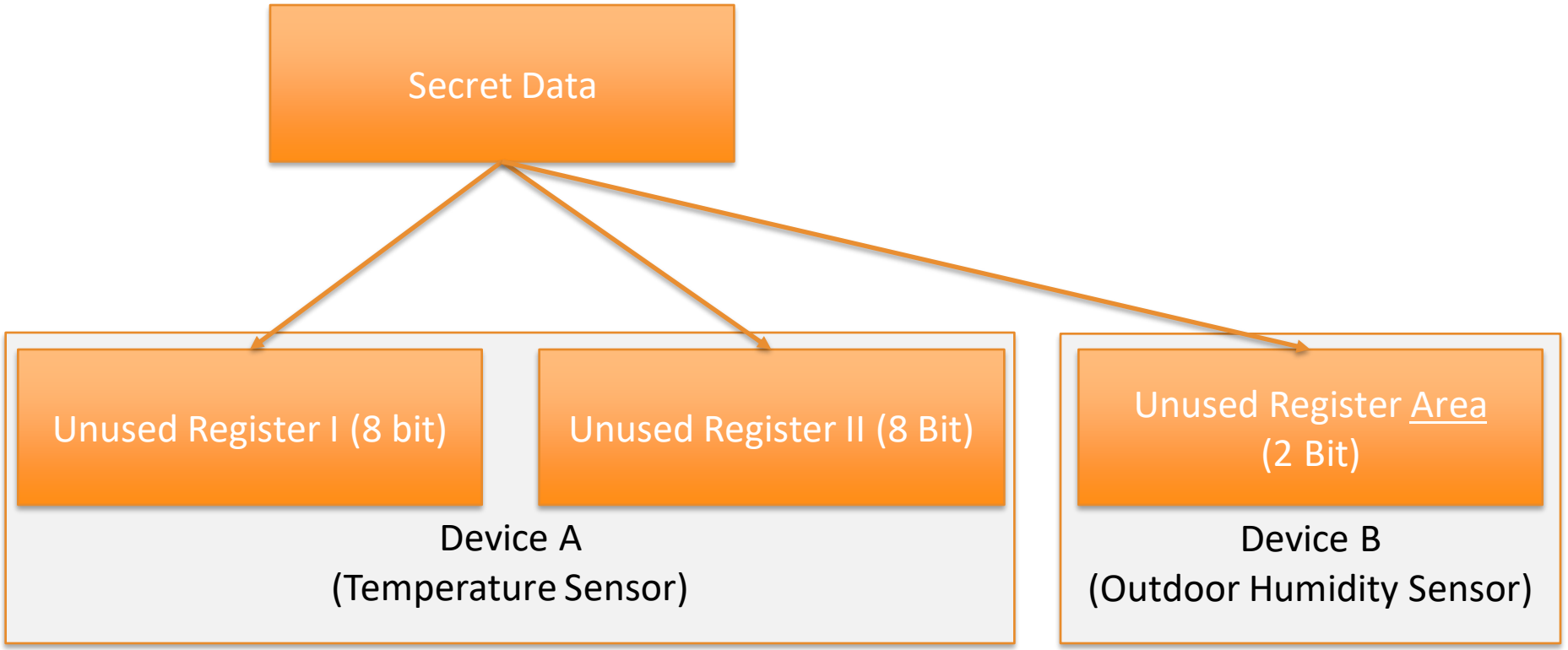
- Analyzed **two different strategies**:
  - Register strategy: utilization of unused memory registers
  - Actuator strategy: storing data in actuator states (e.g. heating level of a heater) in a way that it will not be recognized

Hochschule Worms
University of Applied Sciences

THE REGISTER STRATEGY

Register Strategy: Concept

- We store data in unused registers of CPS components.



Register Strategy: Concept

- Drawbacks:
  - Writing registers may require direct (local bus) access to a CPS device
  - Register size (and thus steganographic storage) limited
  - Each different device model must be analyzed separately (e.g. datasheets)

- Advantages:
  - Several CPS components and CPS types contain unused registers
    - We used a temperature sensor that contains two unused registers; sensor could be embedded in several types of CPS.
  - Good reading and writing performance
  - Valuable to compare performance of **actuator strategy** (later) – is the more sophisticated approach actually *better*?

Register Strategy: Experiments

- Used Maxim Integrated Products, Inc., 1-Wire DS18B20 temperature sensor
  - Communication via 1-Wire protocol

- Approach:
  - Store data in the alarm registers (2x8 bits) of up to 4 sensors.
  - Sort data by sensor-internal unique serial number (can be read via bus connection)

- In experiment, measured time consumption of 100 reading operations from 1, 2 and 4 sensors simultaneously and of 100 writing operations (0x0000 followed by 0xffff in a loop) to one sensor.

Register Strategy: Results

- Reading performance (avg.) per sensor increased with the number of sensors as addresses were only required to be fetched once.
- Values remained robust (0% reading errors within 180.000 operations)
- Thus, performance for steganographic operations not an issue.

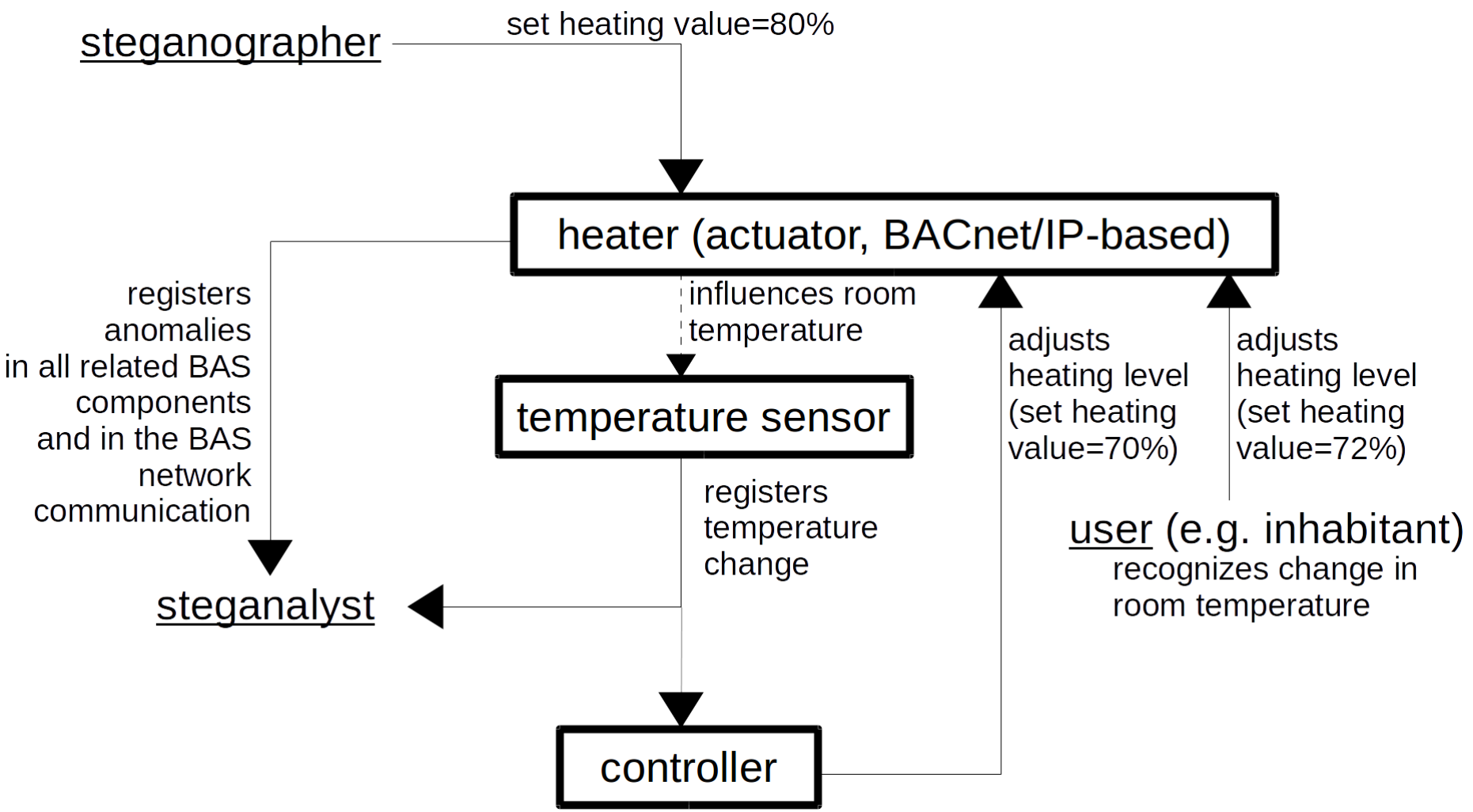
Scenario	Avg. Time [µs]	Min. Time [µs]	Max. Time [µs]
Reading 1 Sensor	12.841	12.800	12.844
Reading 2 Sensors	12.804	12.784	12.806
Reading 4 Sensors	12.802	12.788	12.804
Writing 1 Sensor	71.827	71.800	71.834

No general conclusion on storage space possible, *probably* around *#SelectedDevices * 4-8 bits* (available register bits on average).
A single 128 bit crypto key would then require 16-32 devices.

Hochschule Worms
University of Applied Sciences

THE ACTUATOR STRATEGY

Actuator Strategy: Concept



Animal Scatter Hoarding

- For storing collected food, determine locations (caches) which remain mostly untouched by competing animals.
- Split food storage over many storage locations

Image source: Wikipedia, © SajjadF

Adaptive Information Hiding

- How to **determine suitable actuators** for secret data storage?
  - Scan for devices in a CPS environment, e.g. BACnet: “Who-Is” broadcast to determine present devices
  - Afterwards scan these devices to determine their objects and present values
  - Monitor changes of all actuator values over time and sort out unsuitable devices (e.g. door openers or devices with frequently changed states)

- Not a perfect solution:
  - Steganographer operates on the assumption that the CPS will behave as it behaved in the past (based on recordings of its historic behavior)
  - But future CPS behavior cannot be predicted with 100% accuracy based on the historic behavior
    - imagine an open house presentation: building automation system’s actuators will most likely be used in different way, e.g. a previously unused room will be heated
  - Still requires use of error detecting/correcting codes, e.g. parity bits or spreading of redundant data over several devices

Actuator Strategy: Experiments

- Simulated scatter hoarding using the BACnet protocol
  - ISO standard for communication in automated buildings
  - **How well can we store steganographic data under different conditions?**

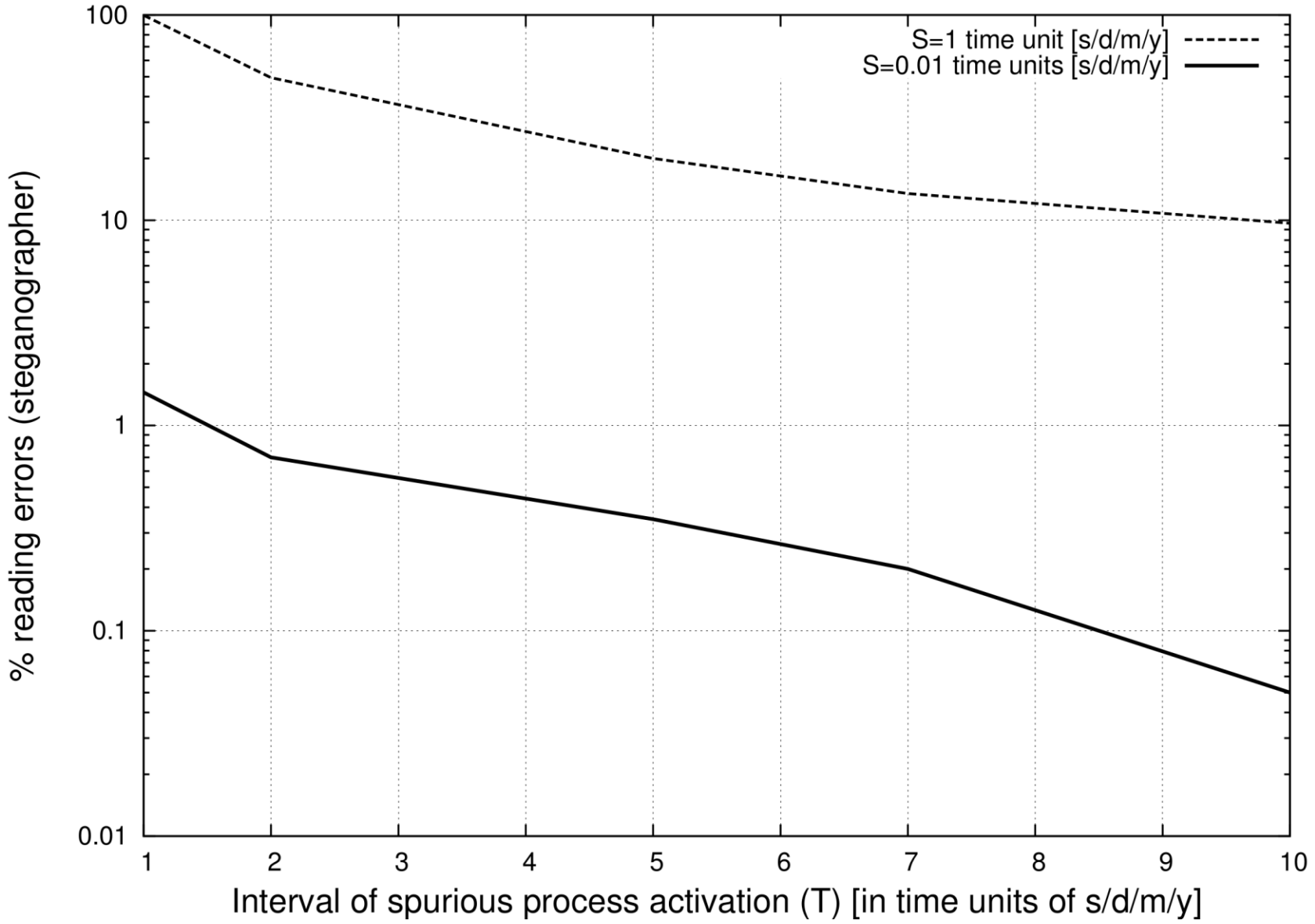
- **In general:** Wrote 100.000 values to an actuator (iterating through values 0°C…100°C). After each value written, the current value was read from the device.

- **Experiment 1**: Introduction of a Spurious Process [7] (**Read-only**)
  - Spurious read-only process (resulted in slow-down of steganographer's process but no data loss as BACnet protocol was able to re-send non-acknowledged packets).

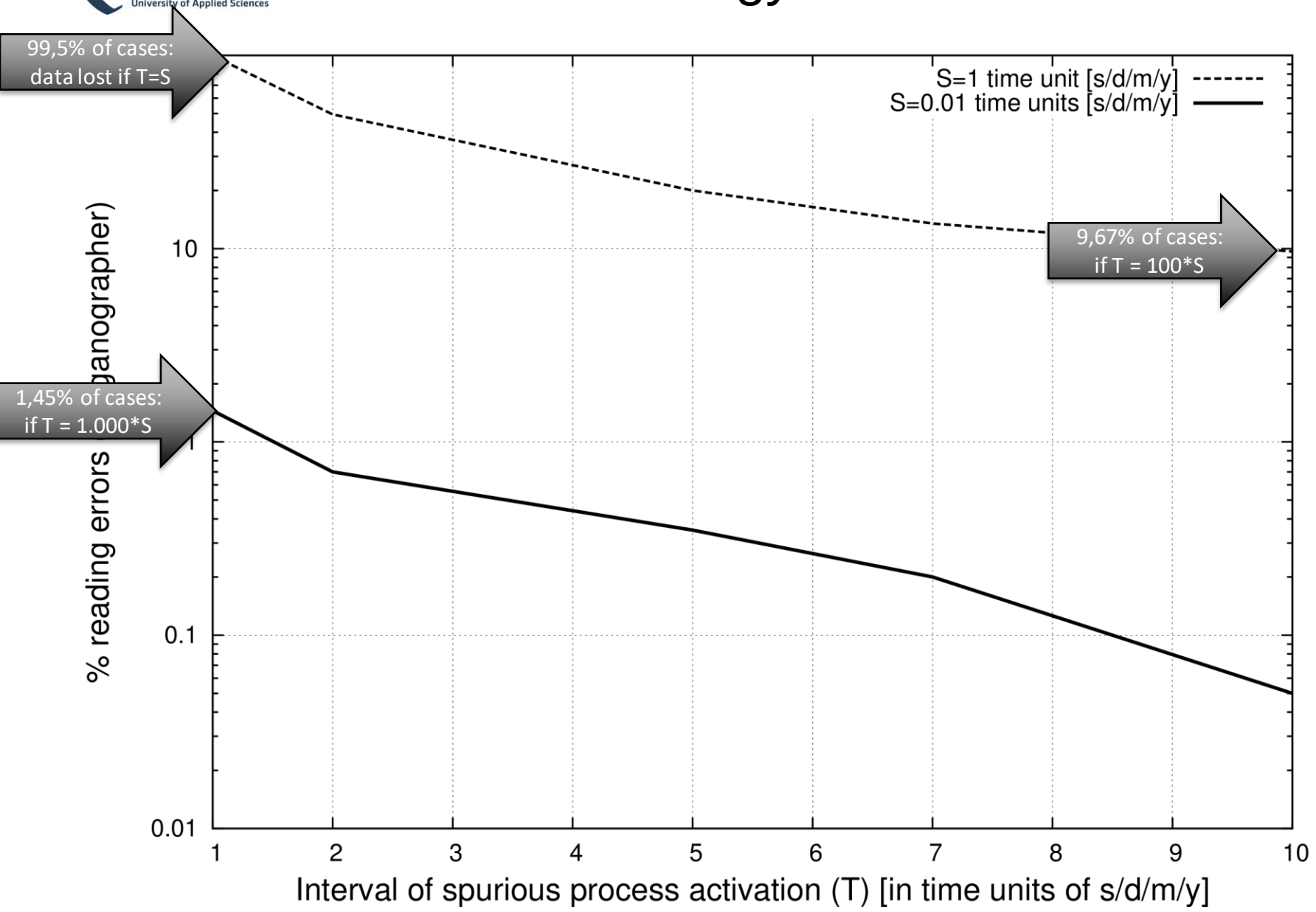
Actuator Strategy: Experiments

- **Experiment 2**: Spurious Process (**Read-Write**)
  - SP represents inhabitant or control logic that changes actuator states
  - Competing animal detects hoarding location (read) and steals food (replacing stored value with a random value)
  - Spurious process writes data every T seconds while the desired storage time was S seconds.
  - Simulated situations reaching from highly spurious ($T = S$) to few spurious intrusions ($S \ll T$).

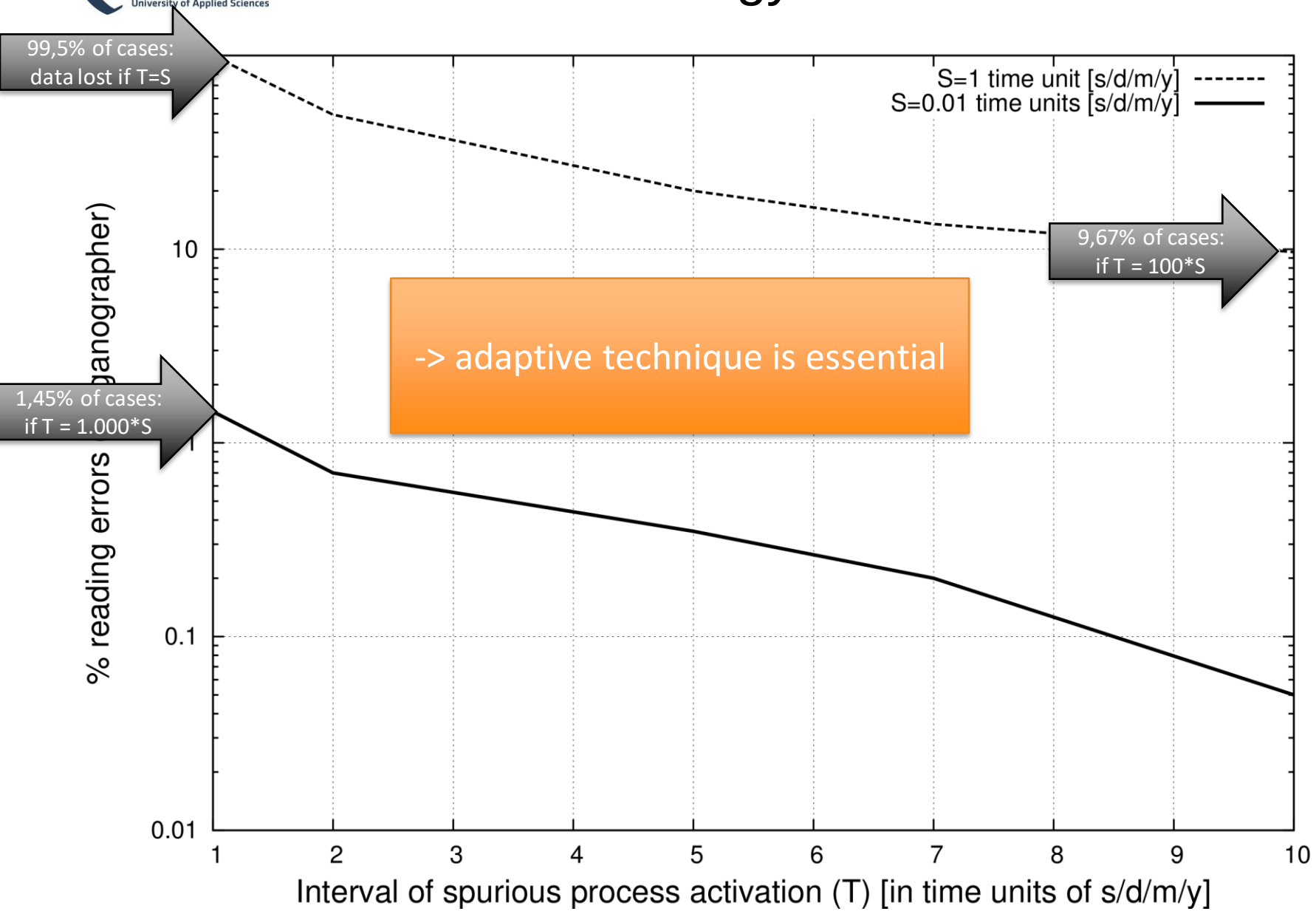
Actuator Strategy: Results



Actuator Strategy: Results



Actuator Strategy: Results



Actuator Strategy: Results

- Storage capacity of actuators highly depends on actuator type (e.g. boolean on-off switches or heaters that provide a fine distinction between heating levels).
- We can assume storage capacity of *2-7* bits per *useful* actuator
  - *18-64* actuators for a 128 bit AES key (**more than in case of register approach!**)

- If we further assume *5-10*% of actuators could be utilized in medium-sized BACnet environments (e.g. 1.000-20.000 actuators), we could store approx. *350* bits - *1.7* Kbytes if *7* secret bits/device can be stored.

- **Advantage: unified accessibili**ty of actuator approach using common protocol (BACnet) over register approach (individual register access needed!)
  - Especially in larger installations

- Performance: ~0.0055 sec per value that must be written/read
  - some actuators much slower
  - some bus systems much slower
  - 0% reading errors without RW spurious process

Hochschule Worms
University of Applied Sciences

CONCLUSION

Conclusion

- The amount of data we can store in a CPS highly depends on
  - How we embed data (hiding method)
  - How many devices are available (e.g. #actuators)

- Similarly, these factors influence the robustness of the embedded data.

Limitations and Future Work

- Structure, environments and capabilities of CPS can vary strongly between different CPS types (e.g. smart building vs. wearable).
  - Further studies needed for other CPS types.
  - Caused influence of steganographer on CPS (and its physical environment) not necessarily clear -> CPSSteg considered risky.
    - Probably not suitable for ICS.

- Novel approaches for Information Hiding in CPS can be expected.
  - We plan to utilize **BACnet COV Subscription** relationships to encode steganographic data.
  - Embedding data for copyright marking, e.g. DRM for smart buildings to fight piracy of products (e.g. using CPS traffic obfuscation or covert channels).

References

1. W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski: **Information hiding in communication networks**, Wiley-IEEE, 2016.

2. E. A. Lee: **Cyber physical systems: design challenges**, Proc. 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), IEEE, 2008.

3. S. Wendzel, B. Kahler, T. Rist: **Covert channels and their prevention in building automation protocols: a prototype exemplified using BACnet**, Proc. IEEE CPSCom Workshop on Security of Systems and Software Resiliency, IEEE, 2012.

4. N. Tuptuk, S. Hailes: **Covert channel attacks in pervasive computing**, Int. Conf. on Pervasive Computing and Communications (PerCom), IEEE; 2015.

5. G. Howser: **Using information flow methods to secure cyber-physical systems**, in: Critical Infrastructure Protection IX, Springer, 2015.

6. J. Tonejc, S. Güttes, A. Kobekova, J. Kaur: **Machine learning methods for anomaly detection in BACnet networks**, Journal of Universal Computer Science (J.UCS), Vol. 22(9), 2016.

7. Y. Fadlalla: **Approaches to Resolving Covert Storage Channels in Multilevel Secure Systems**, Ph.D. Thesis, University of New Brunswick, 1996.