SECURING THE SWARM: EXPLORING STATE-OF-THE-ART COLLECTIVE ATTESTATION AND CHALLENGES

EDLIRA DUSHKU
ASSISTANT PROFESSOR
AALBORG UNIVERSITY, COPENHAGEN, DENMARK
EDU@ES.AAU.DK

AALBORG UNIVERSITY
DENMARK

Communication, Media and Information technologies

A large group of insects, such as bees, that move and act together as a cohesive unit

Photo credit: Image by serhii_bobyk on Freepik

Image By vecstock

Image By vecstock

History of Remote attestation in IoT

2004

SOFTWARE-BASED

SWATT (S&P 2004)
Pioneer (SOSP 2005)

2012

HYBRID-BASED

SMART (NDSS 2012)
TrustLite (Eurosys 2014)

2015

SWARM (COLLECTIVE)

SEDA (CCS 2015)
SANA (CCS 2016)

2016

CONTROL-FLOW

C-FLAT (CCS 2016)
ATRIUM (ICCAD 2017)

2018

DYNAMIC SWARMS

SALAD (ASIACCS 2018)
PADS (SIOT 2018)

2019

DISTRIBUTED

RADIS (SDS 2019)
SARA (TIFS 2020)
— **Distributed services**

ESDRA (IOT-J 2019)
DIAT (NDSS 2019)
— **Distributed verifiers**

2023

PRIVACY

ZEKRA
(ASIA CCS 2023)

History of Remote attestation in IoT

2004 — SOFTWARE-BASED

SWATT (S&P 2004)
Pioneer (SOSP 2005)

2012 — HYBRID-BASED

SMART (NDSS 2012)
TrustLite (Eurosys 2014)

2015 — SWARM (COLLECTIVE)

SEDA (CCS 2015)
SANA (CCS 2016)

2016 — CONTROL-FLOW

C-FLAT (CCS 2016)
ATRIUM (ICCAD 2017)

2018 — DYNAMIC SWARMS

SALAD (ASIACCS 2018)
PADS (SIOT 2018)

2019 — DISTRIBUTED

RADIS (SDS 2019)
SARA (TIFS 2020)
— **Distributed services**

ESDRA (IOT-J 2019)
DIAT (NDSS 2019)
— **Distributed verifiers**

2023 — PRIVACY

ZEKRA
(ASIA CCS 2023)

Swarm attestation

2004

SOFTWARE-BASED

SWATT (S&P 2004)
Pioneer (SOSP 2005)

2012

HYBRID-BASED

SMART (NDSS 2012)
TrustLite (Eurosys 2014)

2015

SWARM (COLLECTIVE)

SEDA (CCS 2015)
SANA (CCS 2016)

2016

CONTROL-FLOW

C-FLAT (CCS 2016)
ATRIUM (ICCAD 2017)

2018

DYNAMIC SWARMS

SALAD (ASIACCS 2018)
PADS (SIOT 2018)

2019

DISTRIBUTED

RADIS (SDS 2019)
SARA (TIFS 2020)
— **Distributed services**

ESDRA (IOT-J 2019)
DIAT (NDSS 2019)
— **Distributed verifiers**

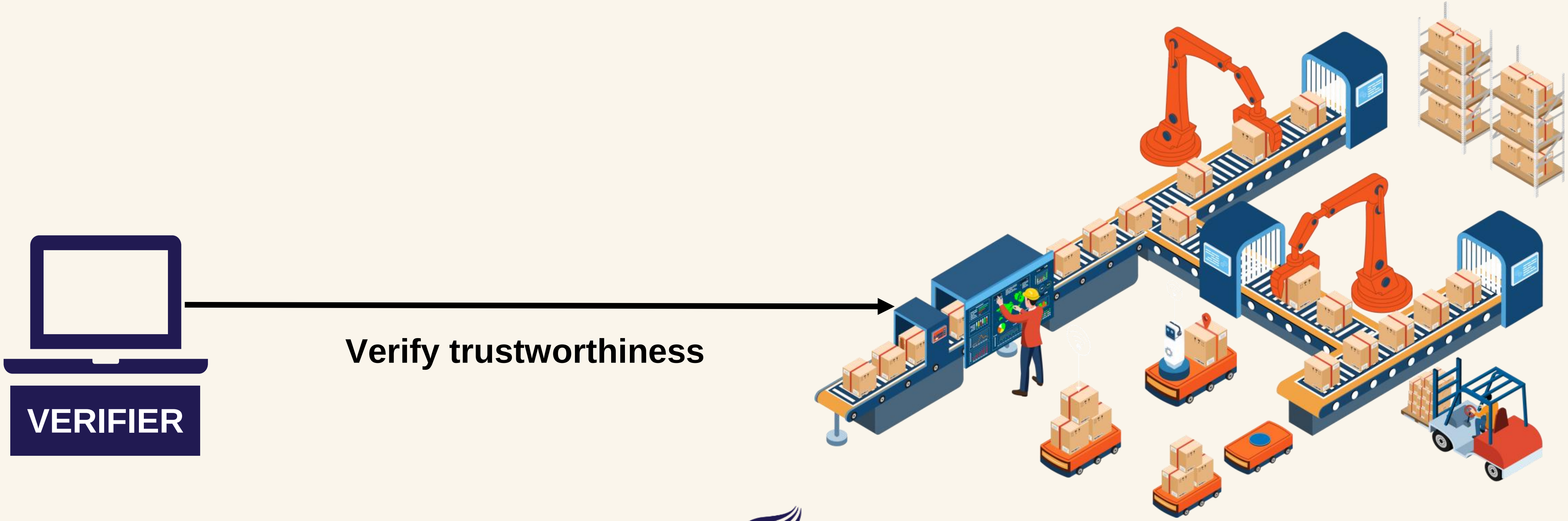
2023

PRIVACY

ZEKRA
(ASIA CCS 2023)

Swarm attestation: The problem

- Verify the internal state of a **large group** of devices
- Should be **more efficient** than attesting each node individually



Swarm attestation: The approach

I think that I shall never see
A graph more lovely than **a tree**.

A tree whose crucial property
Is **loop-free** connectivity.

A tree that must be sure to span
So packets can reach every LAN.

First, **the root** must be selected.
By ID, it is elected.

Least-cost paths from root are traced.
In the tree, these paths are placed.

A mesh is made by folks like me,
Then bridges find **a spanning tree**.

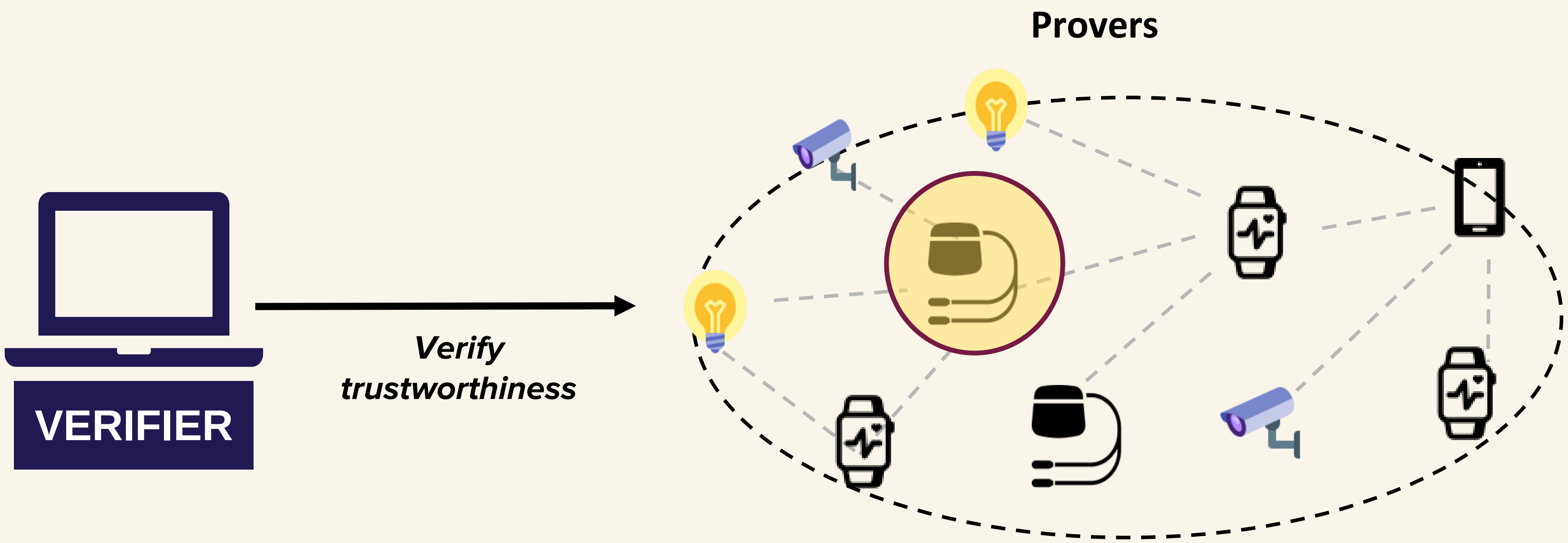
Radia Perlman

https://lemelson.mit.edu/resources/radia-perlman

SEDA: Scalable Embedded Device Attestation

- ALL devices equipped with a trusted component
  (implementation based on SMART and TrustLite security architectures)

- Devices talk only to their neighbors

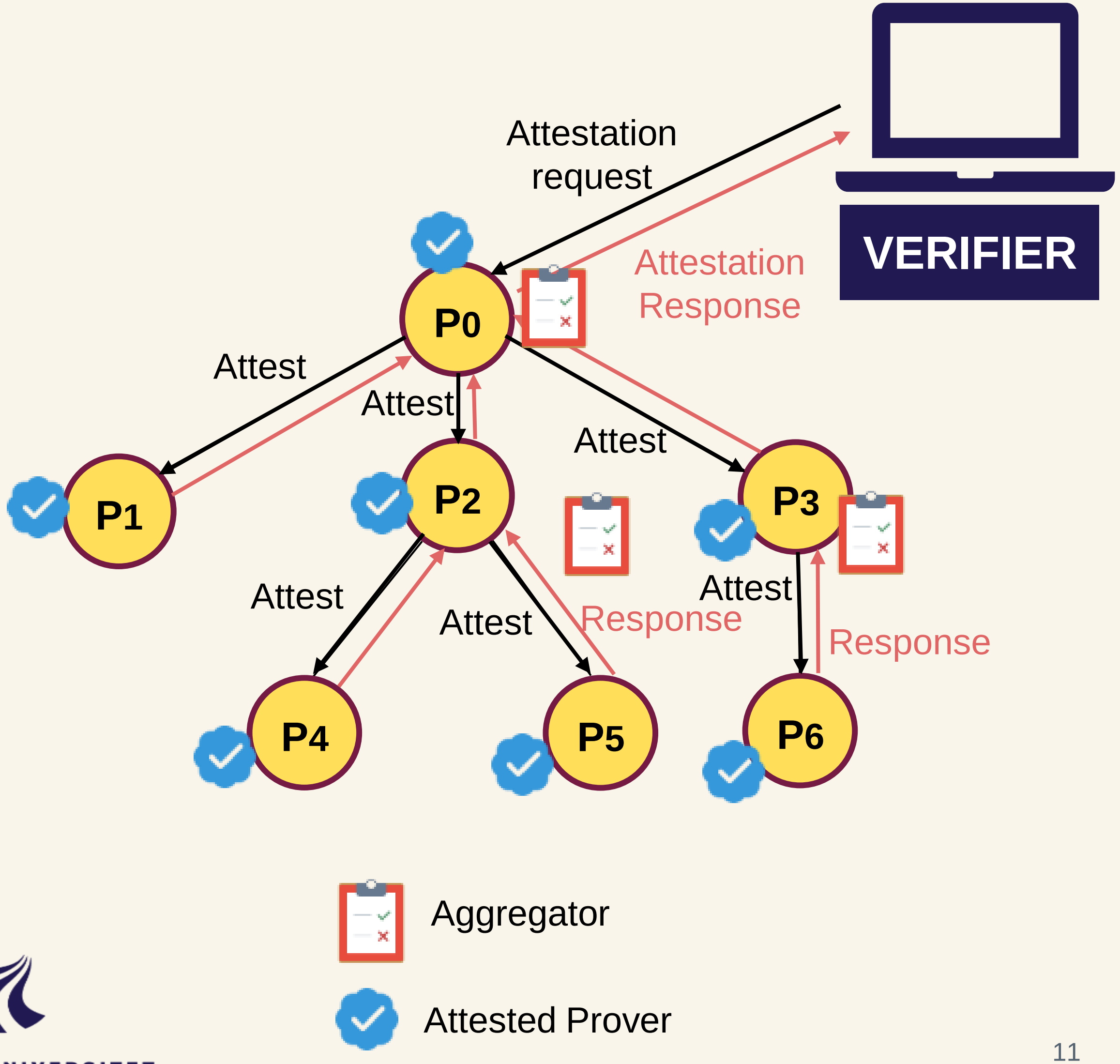


Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A.R., Schunter, M., Tsudik, G.,Wachsmann, C.: Seda: Scalable embedded device attestation. CCS ’15, New York, NY, USA, ACM (2015)

SEDA: Scalable Embedded Device Attestation

Algorithm logic:

1. Verifier selects random Prover (P_0) initializes attestation
2. Spanning tree is created rooted at P_0
3. Each Prover (device) gets attested by its parent (leaves first)
4. Sub-tree roots accumulate results and reports to their parent
5. P_0 reports overall result to Verifier



AALBORG UNIVERSITET

SEDA: Scalable Embedded Device Attestation

Advantages

- Efficient attestation
- Has served as a building block for many other swarm RA protocols
- Has been extensively extended by other procotocols to precisely identify compromised devices, detect physical attacks, etc.

Disadvantages

- Lack of flexibility (ALL devices must participate to attestation), final result is boolean
- Aggregators should be trusted, single point of failure
- Network topology is static

Swarm attestation

2004

SOFTWARE-BASED

SWATT (S&P 2004)
Pioneer (SOSP 2005)

2012

HYBRID-BASED

SMART (NDSS 2012)
TrustLite (Eurosys 2014)

2015

SWARM (COLLECTIVE)

SEDA (CCS 2015)
SANA (CCS 2016)

2016

CONTROL-FLOW

C-FLAT (CCS 2016)
ATRIUM (ICCAD 2017)

2018

DYNAMIC SWARMS

SALAD (ASIACCS 2018)
PADS (SIOT 2018)

2019

DISTRIBUTED

RADIS (SDS 2019)
SARA (TIFS 2020)
Distributed services

ESDRA (IOT-J 2019)
DIAT (NDSS 2019)
Distributed verifiers

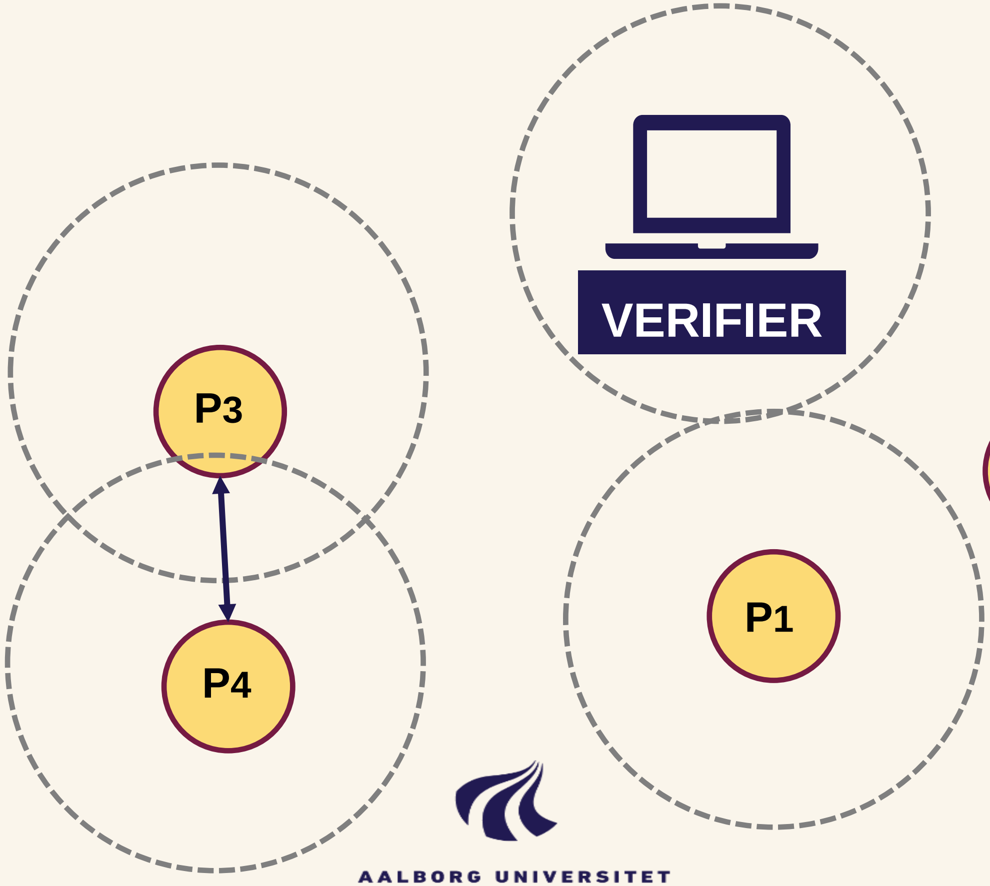
2023

PRIVACY

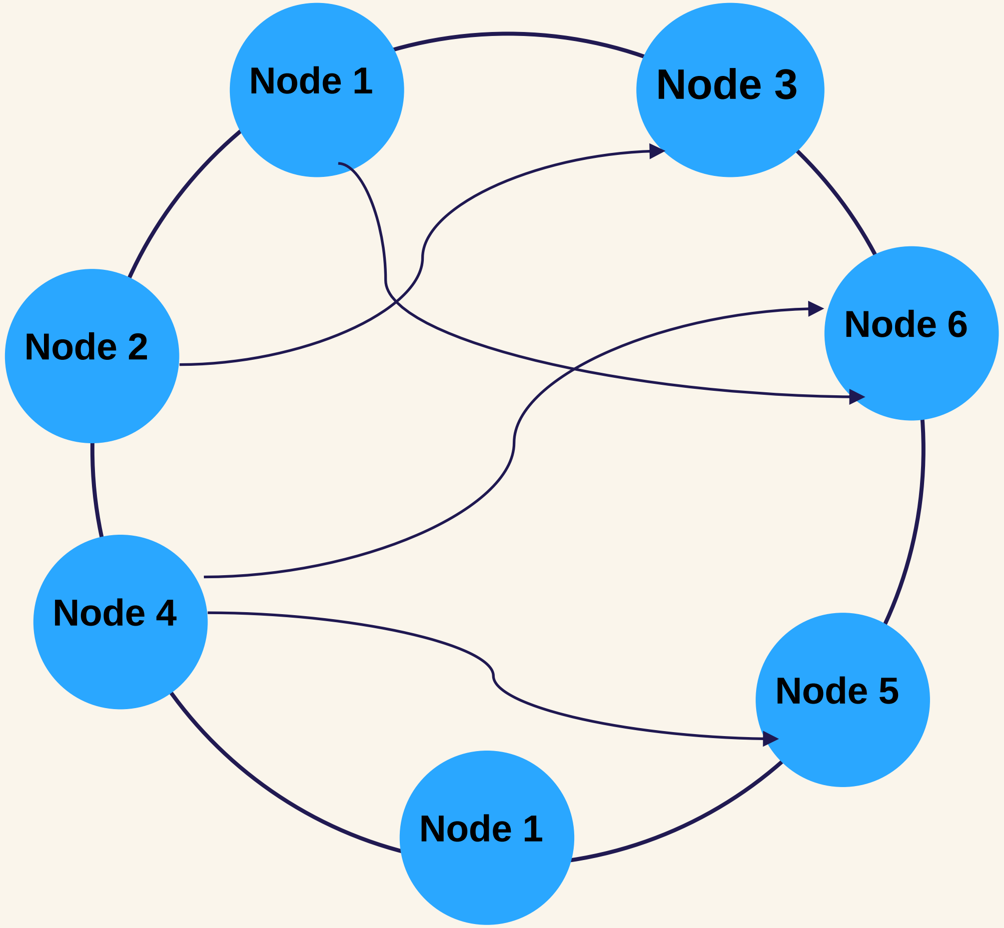
ZEKRA
(ASIA CCS 2023)

Highly Dynamic Swarms: The problem

- **Heterogeneous** and **mobile** devices
- Devices interact **without forming spanning tree**

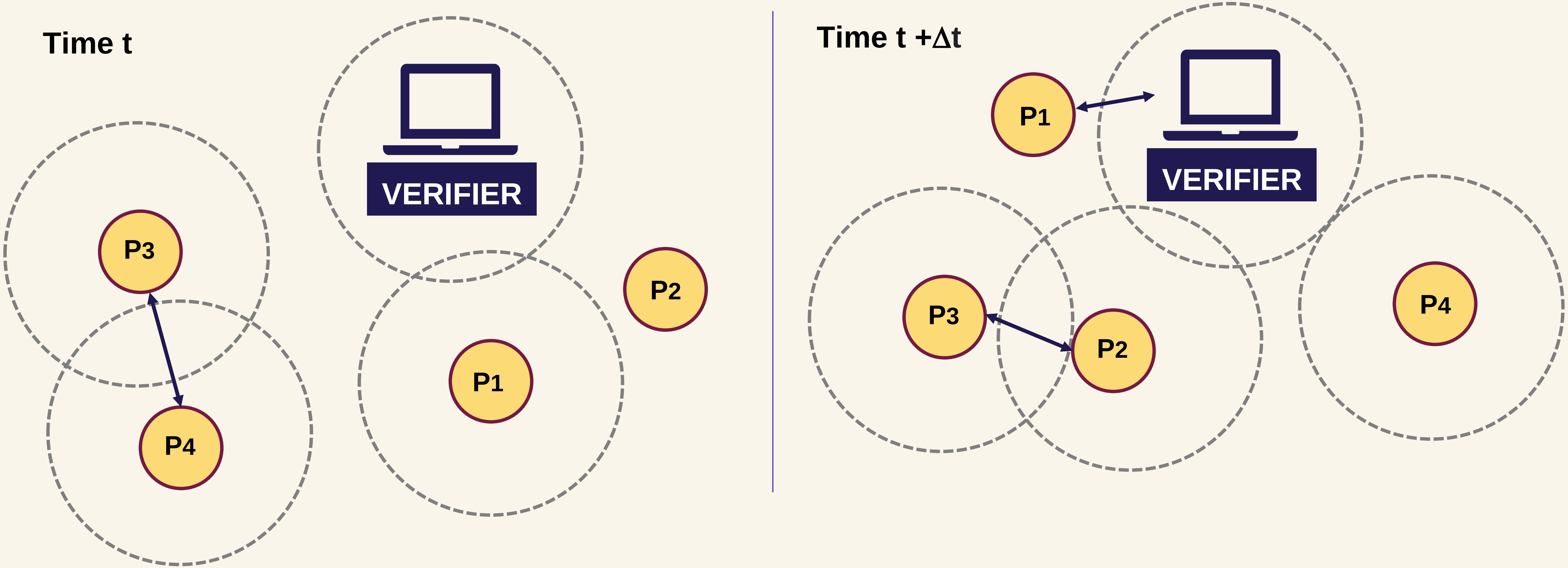


Highly Dynamic Swarms: The approach



Gossip protocol – Peer to Peer communication

PADS: System model



Ambrosin, M., Conti, M., Lazzeretti, R., Masoom Rabbani, M.,and Ranise, S.PADS: Practical Attestation for Highly Dynamic Swarm Topologies. ArXiv e-prints (2018).

PADS: System model

- Only **Provers** (P_j) require a Trusted Execution Environment (TEE)
  - P_j builds an ***attestation proof***
    - Contains hash value of the underlying software
    - Consists of three states (Good-10; Bad-00; Unknown-11)
    - Every prover will share its knowledge with other nodes in range
- **Verifier**
  - Attest individual node before getting its knowledge about the network

PADS: Consensus concept

- Two distinct devices (X_i and X_j) will share there MAC-ed observation for time t
- Consensus among 2 devices will be like

[1 0] GOOD   [0 0] BAD   [1 1] UNKNOWN

	0	1	2	3	…	n-1
x_i^t	1 1	1 0	1 1	0 0		1 1
x_j^t	0 0	1 0	1 0	0 0		1 1
$X_i^{t+1} = x_j^{t+1}$	**0 0**	**1 0**	**1 0**			**1 1**

Summary of Dynamic Swarms

- **Advantages**
  - Suitable for dynamic networks
  - Consider device movement during attestation
  - Verifier can have the snapshot of the network at run-time

- **Disadvantages**
  - Complexity of the protocol in terms of both communication and required processing for resource-constrained devices
  - Do not consider the communication data exchanged among devices
  - Physically compromised Provers can evade detection

Swarm attestation

2004

SOFTWARE-BASED

SWATT (S&P 2004)
Pioneer (SOSP 2005)

2012

HYBRID-BASED

SMART (NDSS 2012)
TrustLite (Eurosys 2014)

2015

SWARM (COLLECTIVE)

SEDA (CCS 2015)
SANA (CCS 2016)

2016

CONTROL-FLOW

C-FLAT (CCS 2016)
ATRIUM (ICCAD 2017)

2018

DYNAMIC SWARMS

SALAD (ASIACCS 2018)
PADS (SIOT 2018)

2019

DISTRIBUTED

RADIS (SDS 2019)
SARA (TIFS 2020)
— **Distributed services**

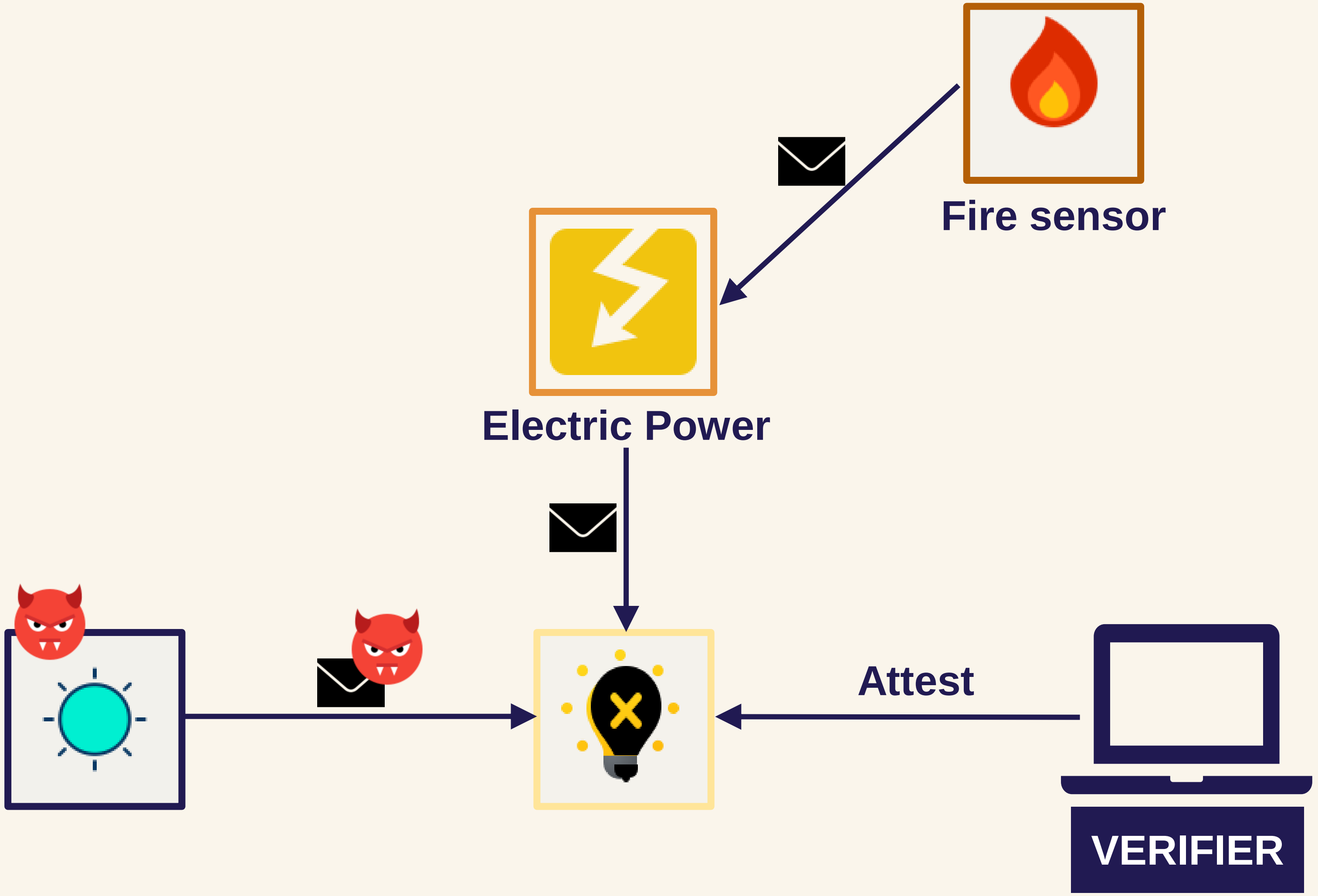
ESDRA (IOT-J 2019)
DIAT (NDSS 2019)
— **Distributed verifiers**

2023

PRIVACY

ZEKRA
(ASIA CCS 2023)

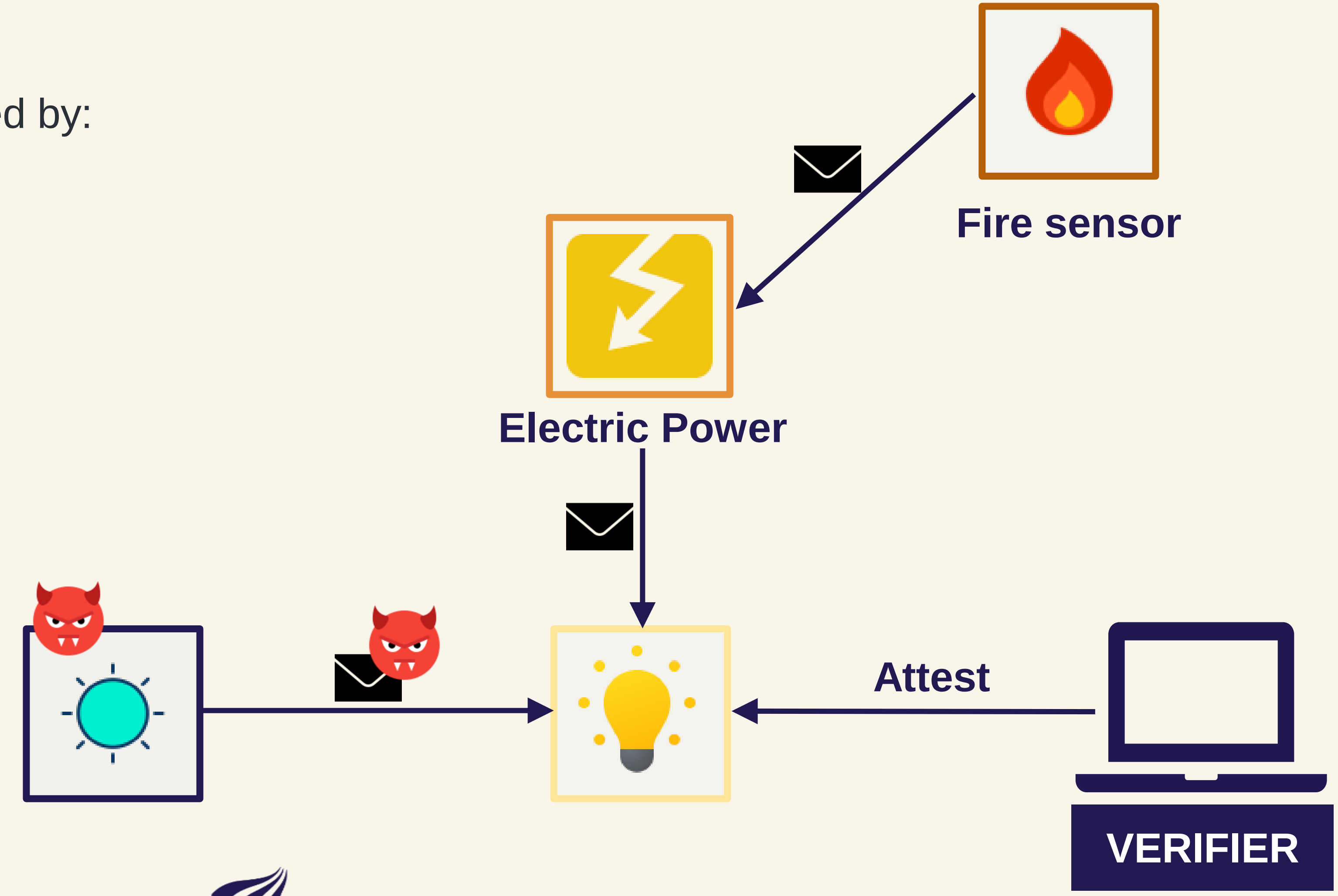
Motivating example: Distributed IoT service (Async)



Motivating example: Distributed IoT service (Async)

Legitimate state of Smart bulb is affected by:

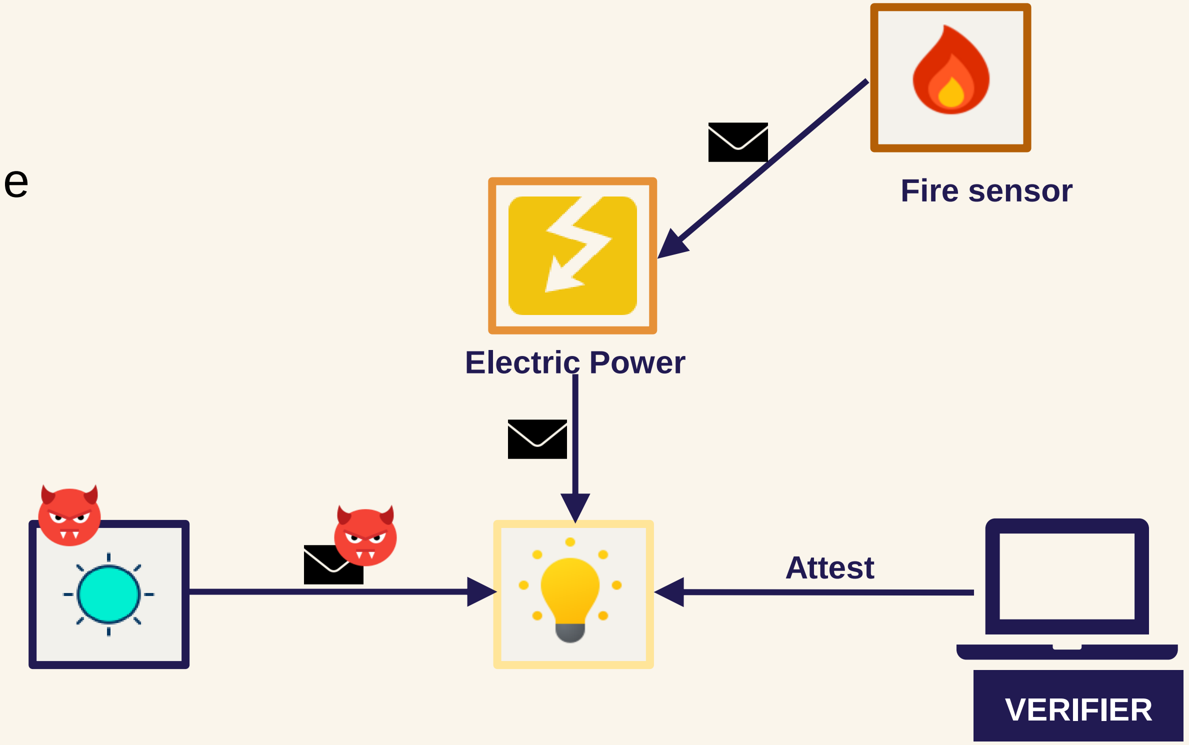
- history of the events
- order of occurrence of events
- the data exchanged among events



AALBORG UNIVERSITET

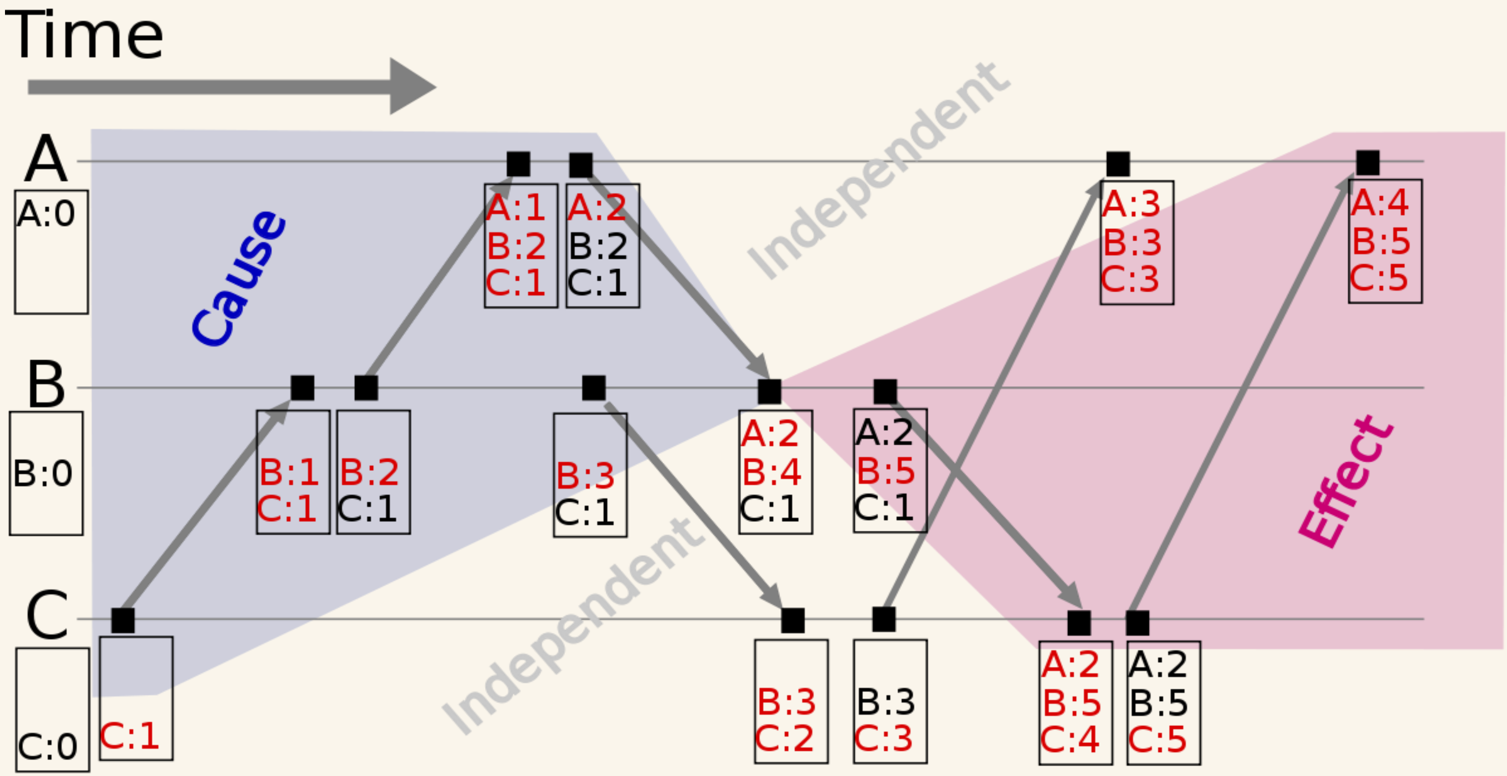
Realistic assumptions

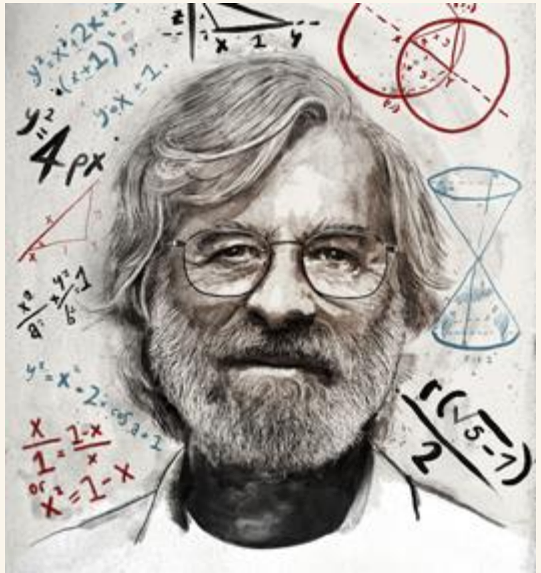
- **Distributed IoT services**
  - Event-driven interactions
- **Distributed Publish/Subscribe pattern**
  - The occurrence of the events in not predictable
- **Clock synchronization**
  - Local clocks on IoT devices are not perfectly synchronized



AALBORG UNIVERSITET

Distributed IoT service: The approach

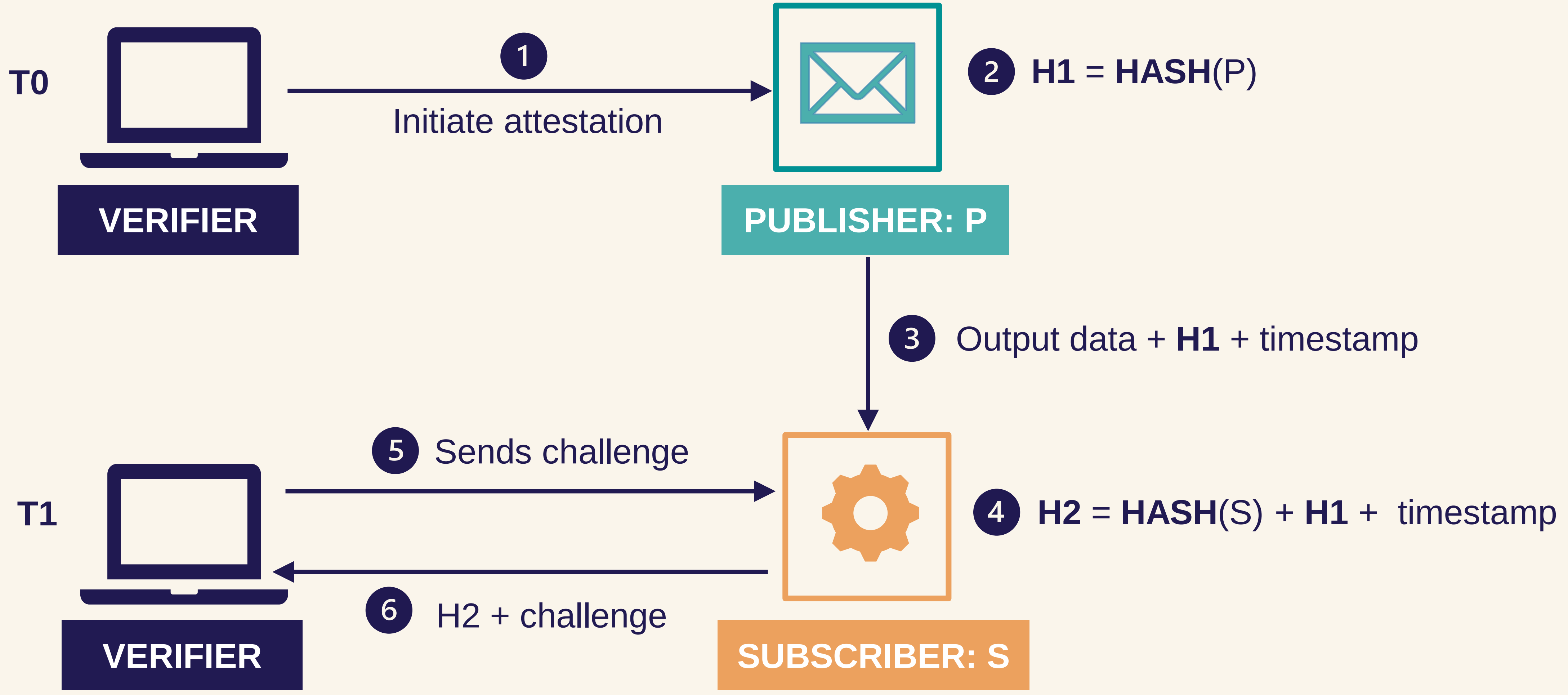




https://www.brandeis.edu/magazine/2017/fall/featured-stories/lamport.html

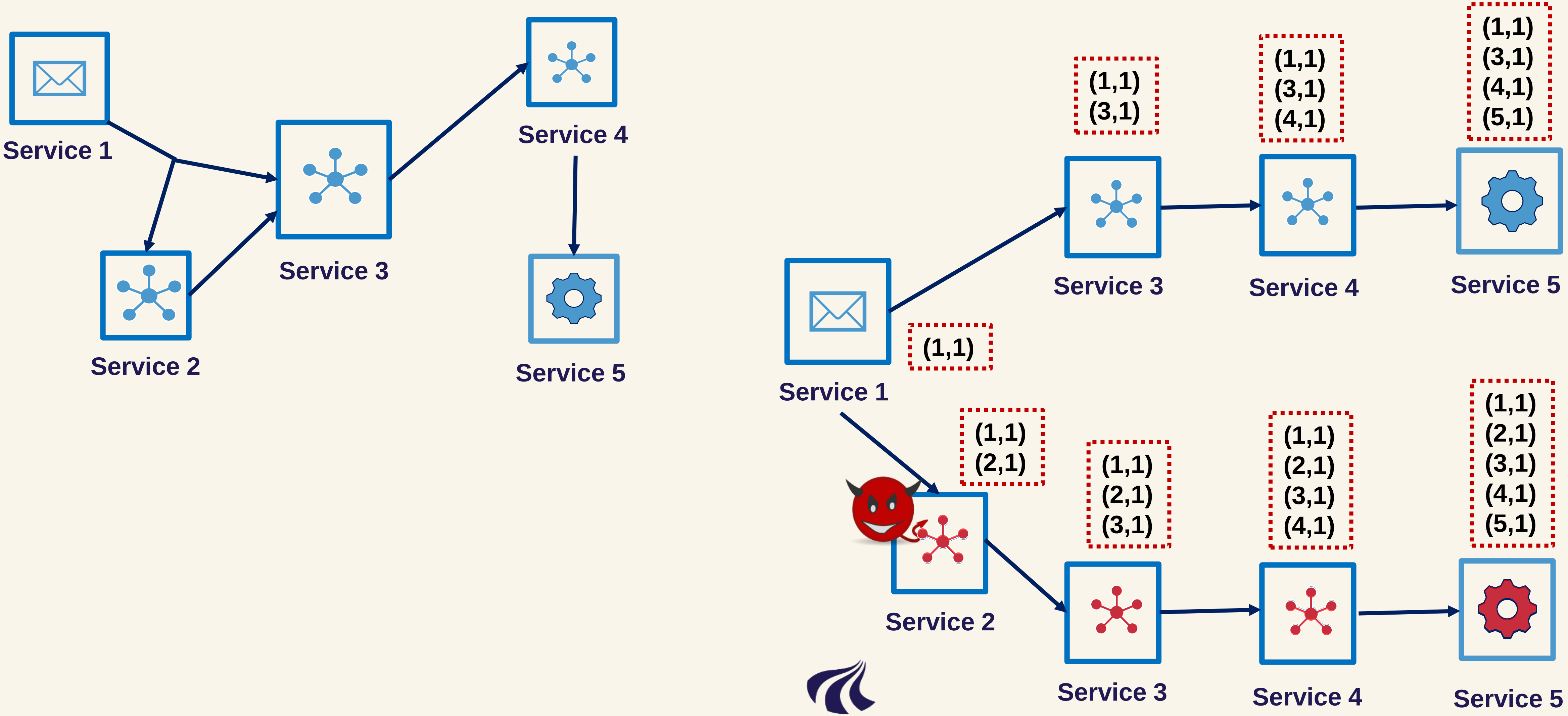
AALBORG UNIVERSITET

SARA: Protocol Overview



Dushku, E., Rabbani, M. M., Conti, M., Mancini, L. V., and Ranise,S. SARA: Secure Asynchronous Remote Attestation. In IEEE Transactions on Information Forensics and Security, vol. 15, pp.3123-3136, 2020..

SARA: Logical Vector clock



AALBORG UNIVERSITET

Summary of Distributed Services attestation

Advantages

- Verifies both trustworthiness of the devices and legitimate operations

Disadvantages

- In SARA, the attestation result is long and it should be optimized

Open challenges and Ongoing projects

1 Attestation time

- **Challenge:** Attestation is typically performed **randomly**
- **The approach:** Use blockchain technology to store a history of attestation results and make the attestation decentralized
- **Proposal:**

S. F. J. J. Ankergård, E. Dushku, and N. Dragoni, **"Publicly Verifiable Remote Attestation through Blockchain"**, 14th International Symposium on Foundations & Practice of Security (FPS), 2021.

1 Attestation time

Algorithm	Family	Throughput	Scalability	Overhead
Proof-of-Work (PoW)	Proof-of-X	Low	Low	Computational
Proof-of-Authority (PoA)	Proof-of-X	Low	High	None
Proof-of-Stake (PoS)	Proof-of-X	Low	Low	None
Proof-of-Elapsed-Time (PoET)	Proof-of-X	Low	High	None
Proof-of-Capacity (PoC)	Proof-of-X	Low	Low	None
Proof-of-Burn (PoB)	Proof-of-X	Low	Low	None
Proof-of-Importance (PoI)	Proof-of-X	Low	Low	None
Byzantine Fault Tolerance (BFT)	Voting	High	Low	Communications
Crash Fault Tolerance (CFT)	Voting	High	High	Communications

AALBORG UNIVERSITET

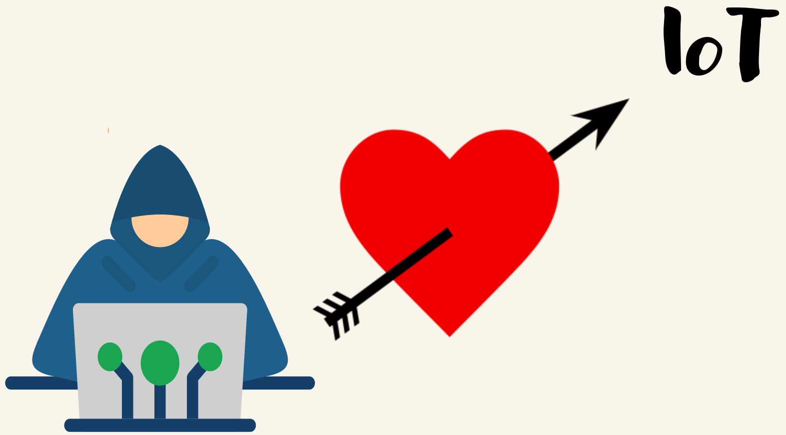
2 Attestation verification

- **Challenge:** Typically, Provers and Verifiers have **pre-shared information**
- **The approach:** Publicly verifiable historical attestation results
- **Proposal:**

Dushku E., Rabbani M. M., Vliegen J., Braeken A., and Mentens N. **PROVE: Provable Remote attestation for public Verifiability.** Journal of Information Security and Applications. Volume 75, 2023, 103448, ISSN 2214-2126.

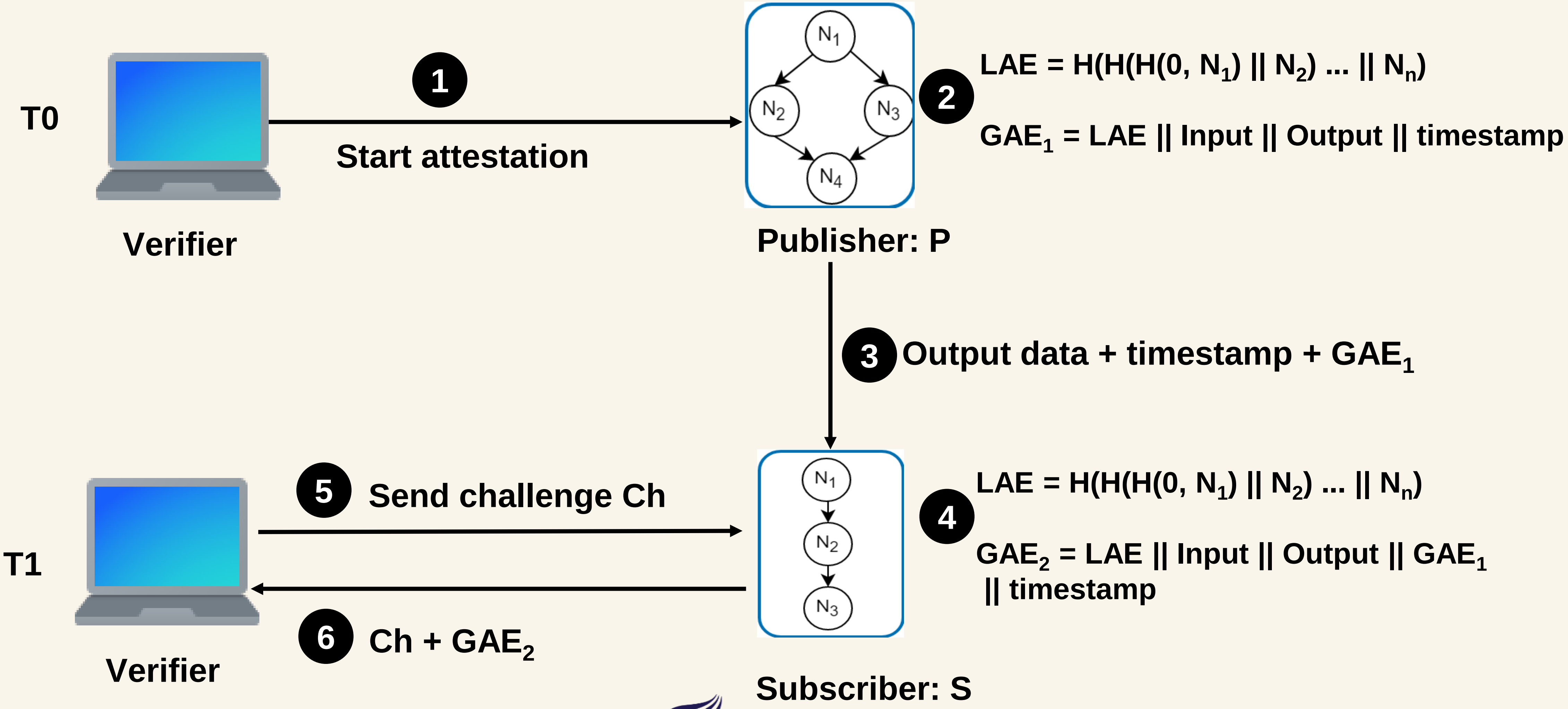
3 Beyond code-injection attacks

- **Challenge:** Most of swarm attestation protocols perform **static attestation**
- **Approach:** Design novel approaches to detect **physical** and **runtime** attacks in swarms
- **Proposal:**



R. M. Halldórsson, E. Dushku, and N. Dragoni, **“ARCADIS: Control-Flow Attestation of Asynchronous Distributed IoT Services”**, IEEE Access, 2021.

3 Beyond code-injection attacks



4 Energy Harvesting devices

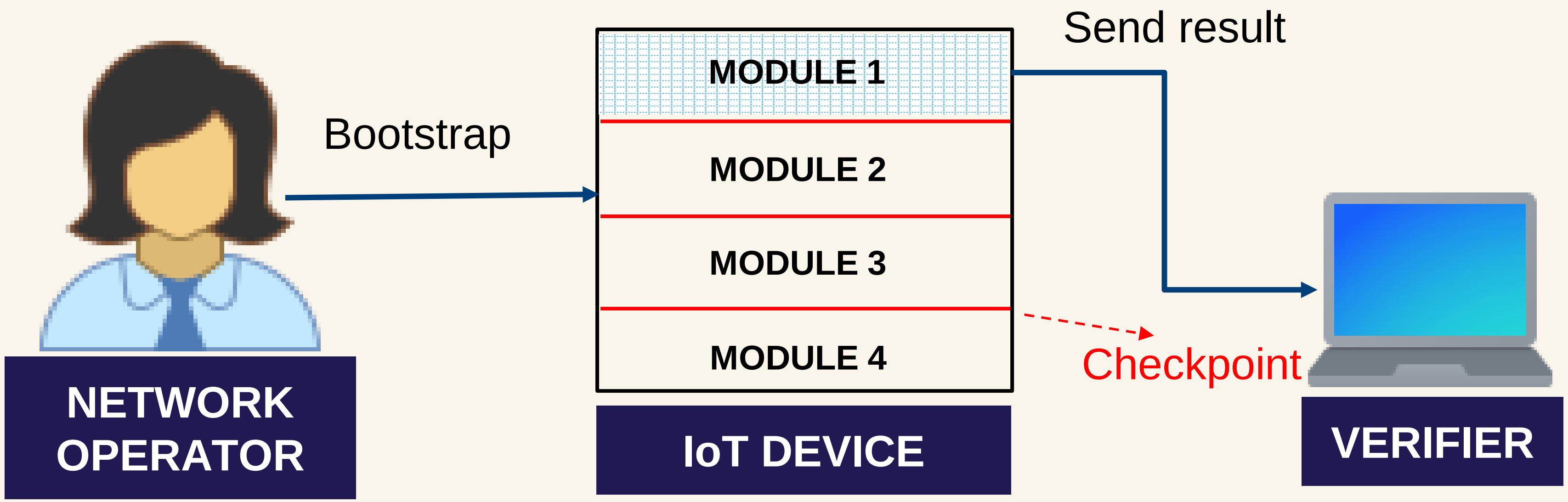
- **Challenge: Interruptible attestation** is an open research problem even for single-device attestation

- **Approach:** Design interruptible/partial attestation for swarms

- **Proposal for single-device:**

Rabbani M. M., Dushku E., Vliegen J., Braeken A., Dragoni N., Mentens N. **RESERVE: Remote Attestation of Intermittent IoT devices.** *In the Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys ’21).* 2021.

4 Energy Harvesting devices



Rabbani M. M., Dushku E., Vliegen J., Braeken A., Dragoni N., Mentens N. **RESERVE: Remote Attestation of Intermittent IoT devices.** *In the Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21).* 2021.

5 Privacy

- **Challenge:** Privacy is generally overlooked in attestation of IoT devices

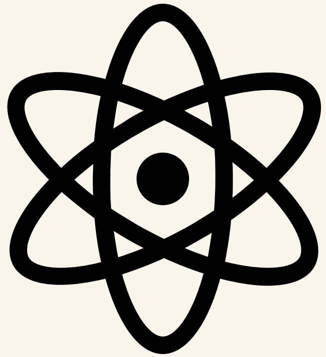
- **Approach:** Design a zero-knowledge attestation for swarms

- **Proposal for single-device:**

Debes H.B., Dushku E., Giannetsos Th., and Marandi A. **ZEKRA: Zero-Knowledge Control-Flow Attestation.** In Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security (ASIA CCS '23). Association for Computing Machinery, New York, NY, USA, 357–371.

6 Post quantum

- **Challenge:** In the IoT domain, existing attestation schemes rely on RSA or ECC
- **Approach:** Design post-quantum attestation for swarms
- We have started a PhD project



Conclusions

- Presented an overview of the main swarm RA protocols proposed in the literature (swarm, dynamic, distributed services)

- Despite many swarm RA approaches, some cyber attacks remain undetected, e.g., data attacks, physical attacks

- There is no RA of large mobile IoT networks, in which nodes join or leave during the remote attestation

- Some open issues for single-device attestations can be extended to swarms

AALBORG UNIVERSITET

EDLIRA DUSHKU

EDU@ES.AAU.DK

QUESTIONS?

AALBORG UNIVERSITY
DENMARK

Communication, Media and Information technologies