LIghtweight Swarm Attestation: a Tale of Two LISA-s

Xavier Carpent[1], Karim ElDefrawy[2], Norrathep Rattanavipanon[1] and Gene Tsudik[1]

[1]University of California, Irvine and [2]SRI Interanational

Contributions

- Define a new metric that captures the type of information offered by a swarm attestation technique.
- Construct two practical attestation protocols with different QoSA features and communication and computation complexities.
- Investigate the impact of proposed protocols on the underlying security architecture.
- Assess their performance using the open-source Common Open Research Emulator (CORE) [1].

Introduction

- Various Remote Attestation (RA) techniques have been proposed for the single-prover scenario.
- New issues emerge for attesting a swarm of devices.
- SEDA [2] represents the first step towards swarm RA.

Motivation

- SEDA under-specifies several **practical** aspects:
  - Impact on security architecture,
  - Overall attestation timeout
  - Initiator selection
- It is unclear whether SEDA handles mobility
- It is unclear how to compare efficacy of different swarm RA techniques

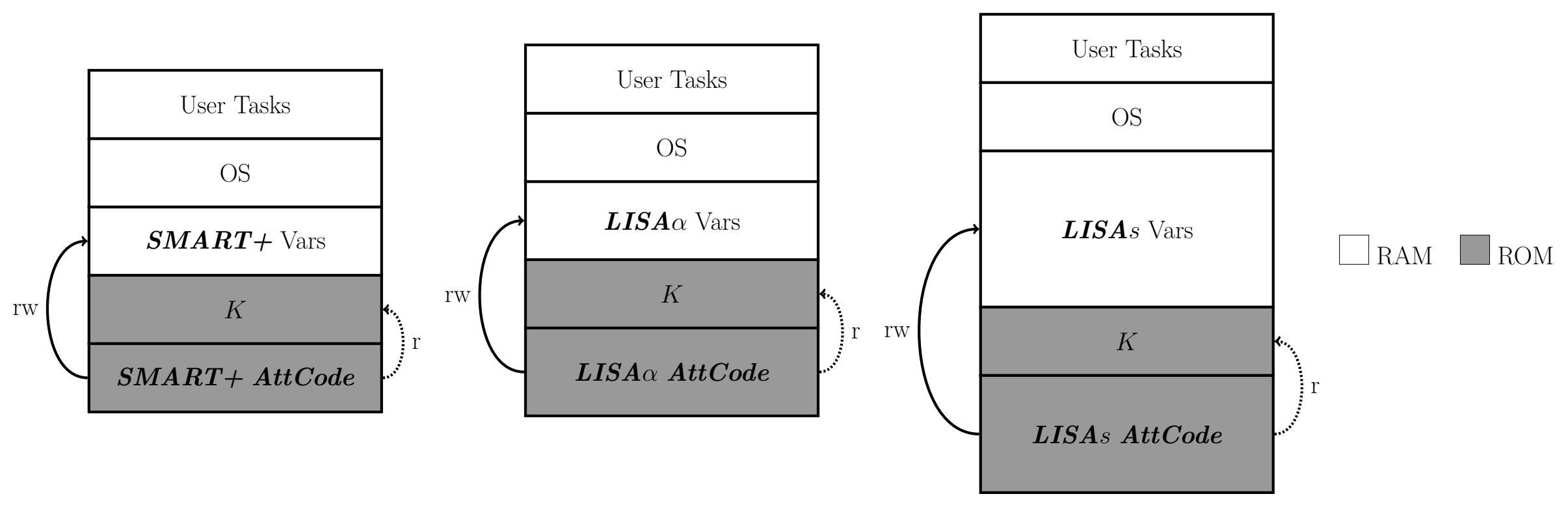
QoSA

- Quality of Swarm Attestation
- A notion capturing information provided by swarm RA
- Enables comparing multiple swarm RA protocols
- Loosely categorized as: Binary, List, Intermediate, Full QoSA

Security Architecture

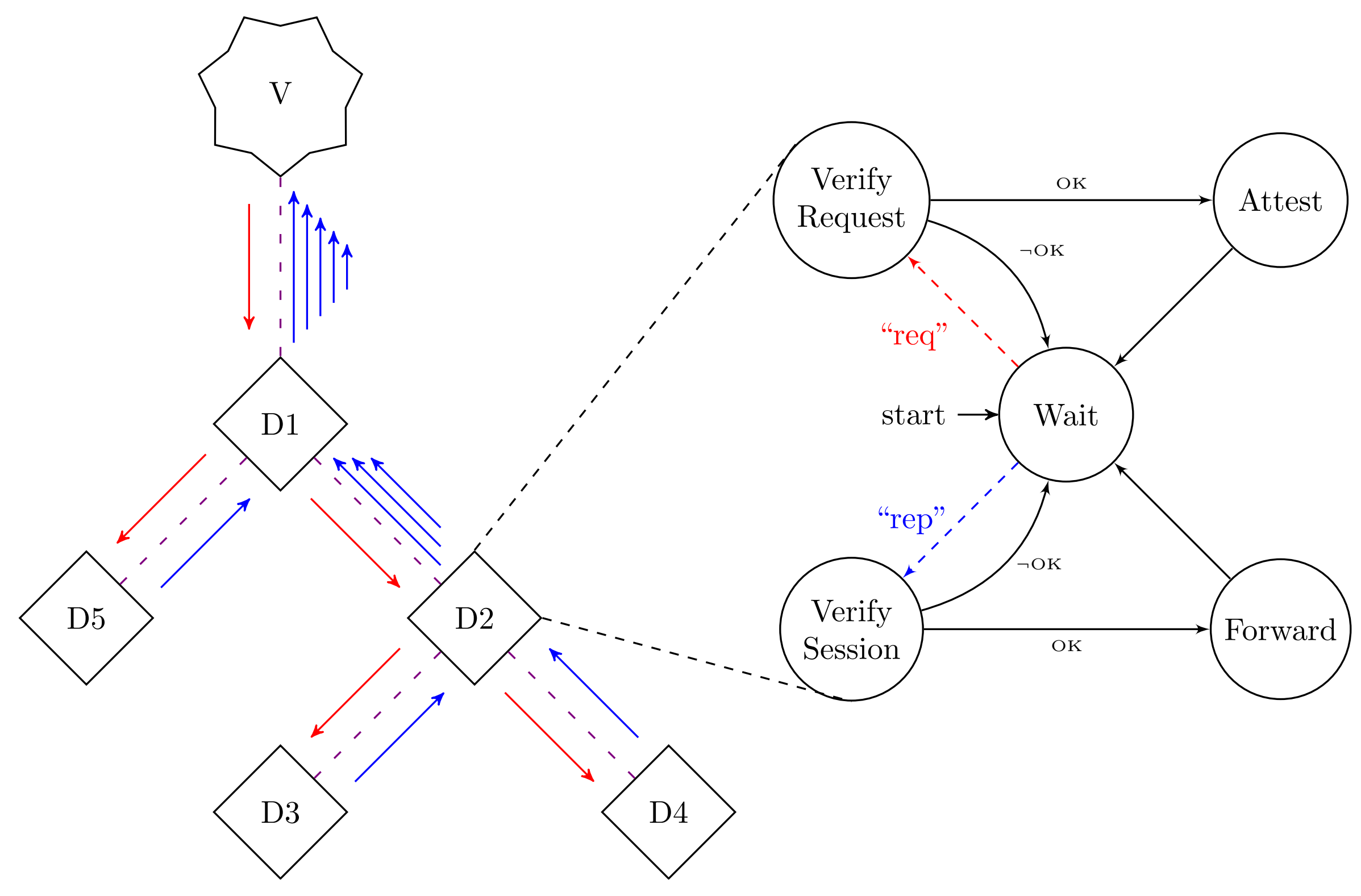
A swarm device adheres to ***SMART+*** ([4], [3]) architecture. Key aspects are as follows:

- ***AttCode*** in ROM does not leak info.
- Execution of ***AttCode*** is atomic and complete.
- A key is stored in ROM and can only be read from within ***AttCode***.
- A fixed-size block of secure RAM.



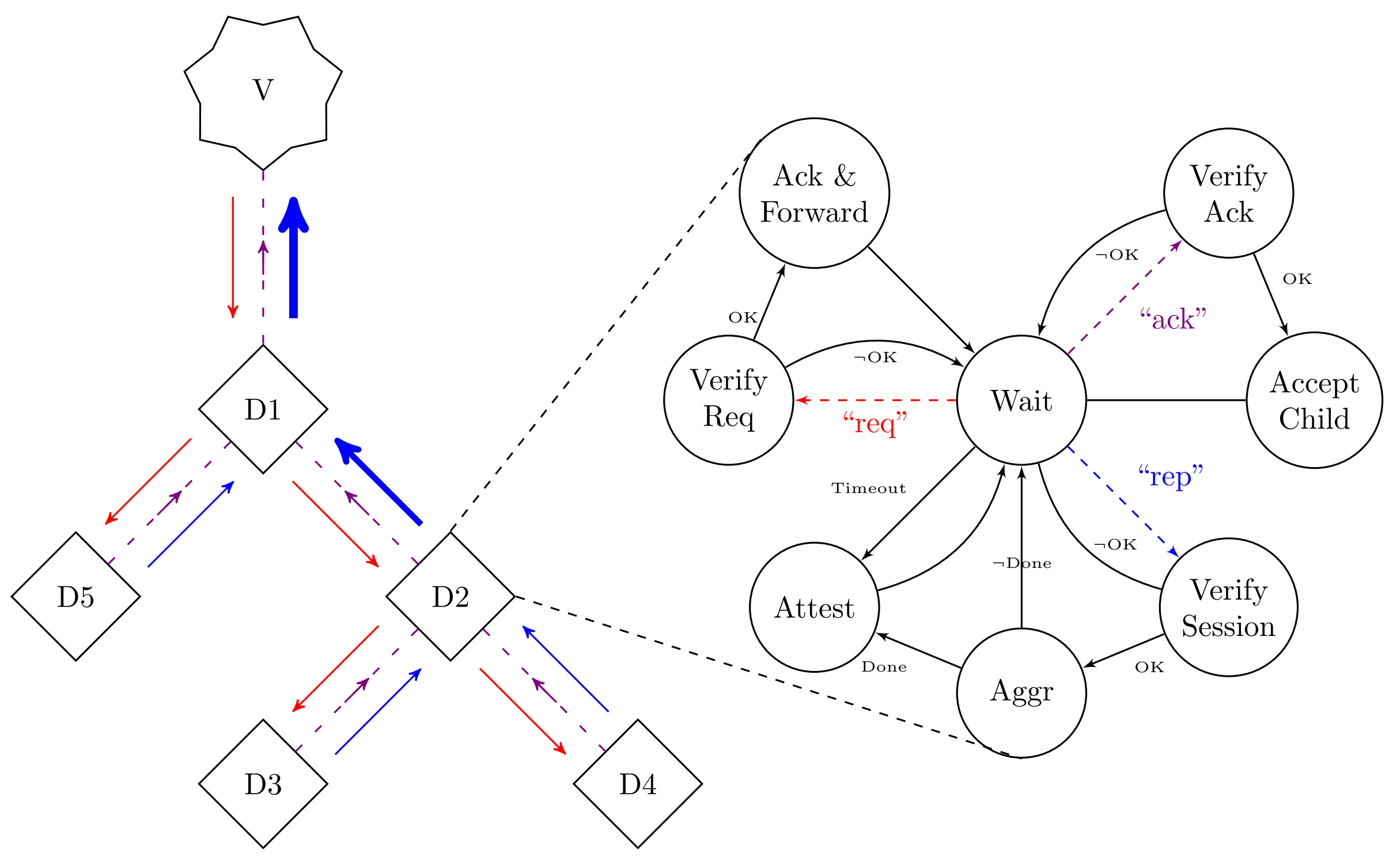
*LISA*α - Asynchronous

- Minimal change from single-prover RA
- Device collaboration only for propagating attestation requests and reports

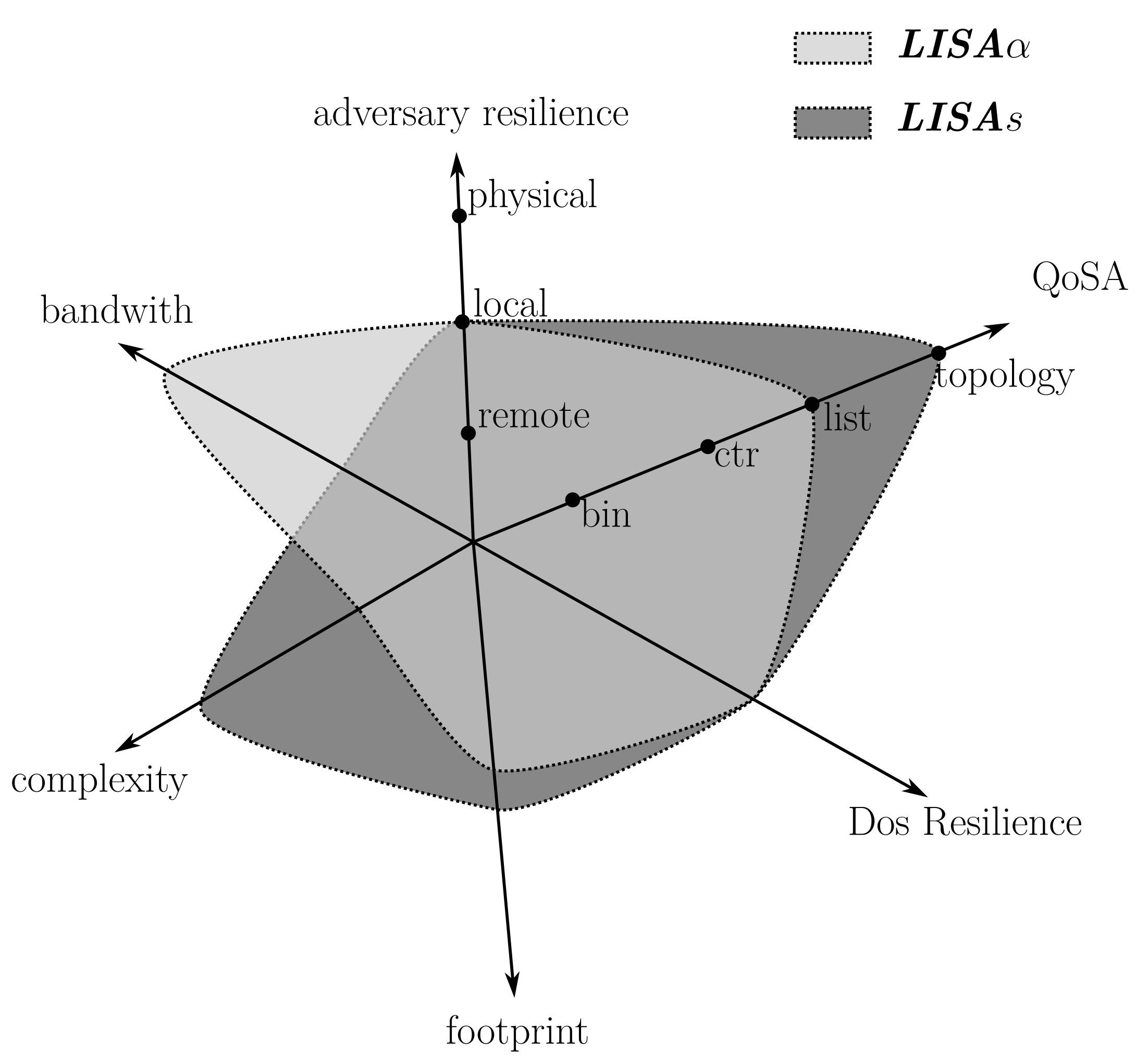


*LISA*s - Synchronous

- Aggregate many reports into a single report
- Wait for all children's reports before constructing own report

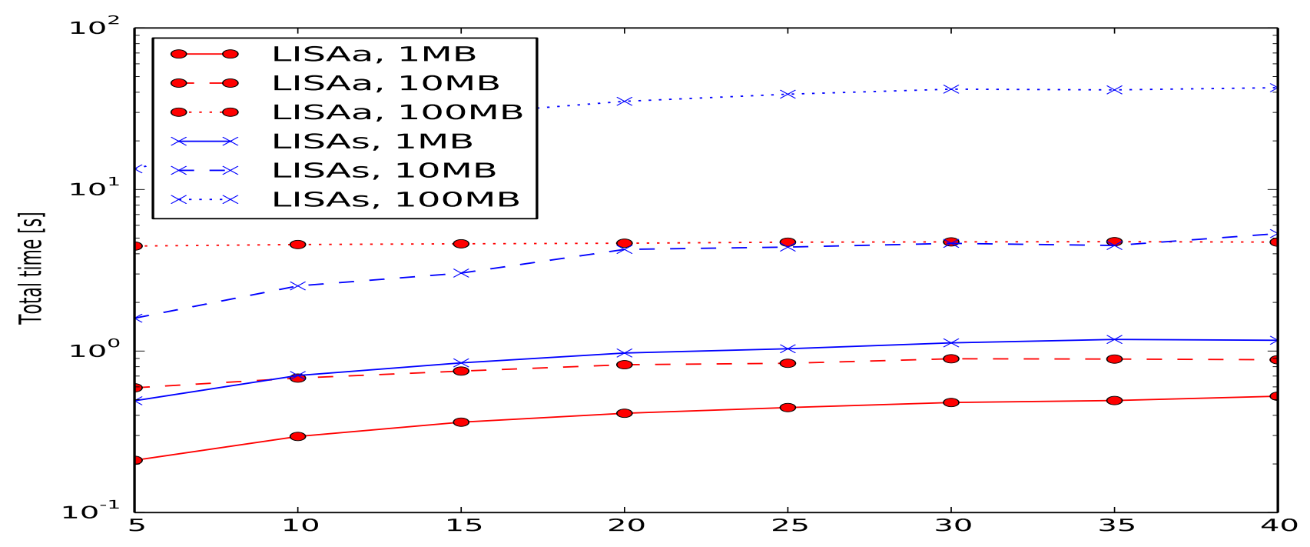


Comparison

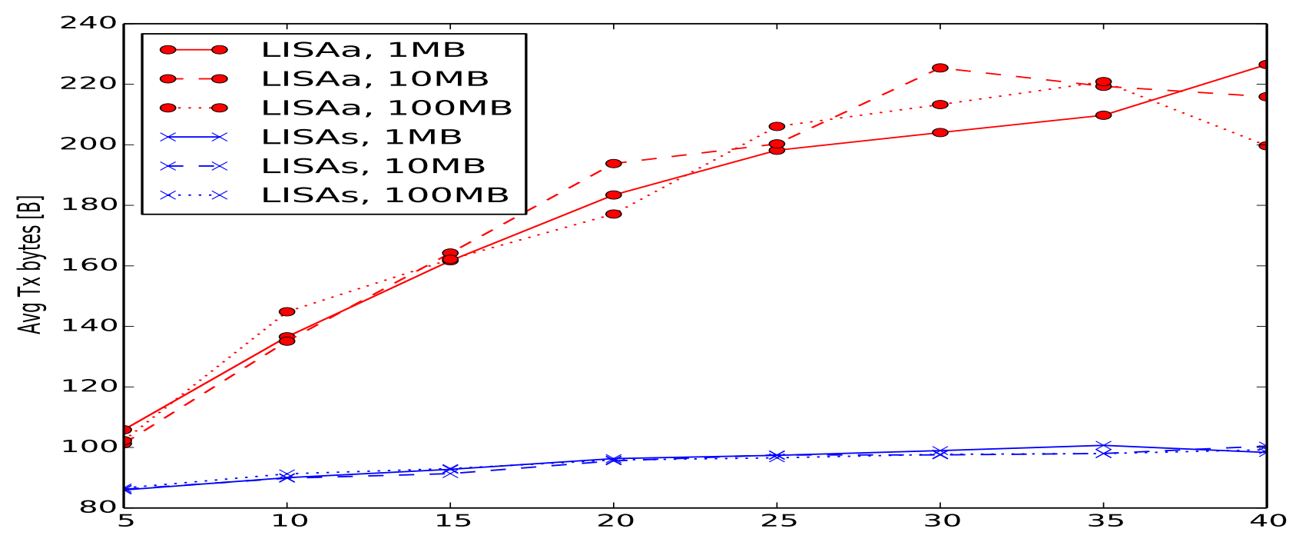


Experimental Results

Attestation Runtime: ***LISA***α is better.



Bandwidth Usage: ***LISA****s* is better.



Conclusion

This paper brings swarm RA closer to reality by designing two simple and practical protocols: ***LISA***α and ***LISA****s*. To analyze and compare multiple protocols, we introduced a new metric, called Quality of Swarm Attestation (QoSA) which captures the type of information offered by swarm RA.

References

[1] J. Ahrenholz, "Comparison of CORE network emulation platforms," in *IEEE Military Communications Conference (MILCOM)*, 2010.

[2] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, and C. Wachsmann, "SEDA: Scalable embedded device attestation," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2015.

[3] F. Brasser, A.-R. Sadeghi, and G. Tsudik, "Remote attestation for low-end embedded devices: the prover's perspective," in *ACM/IEEE Design Automation Conference (DAC)*, 2016.

[4] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito, "SMART: Secure and minimal architecture for (establishing dynamic) root of trust," in *Network and Distributed System Security Symposium (NDSS)*, 2012.