Ira A. Fulton Schools of Engineering
Arizona State University

Securing Edge-Based Real-Time IoT Systems

Dongha Kim and Hokeun Kim (Arizona State University) ***SenSys23, Nov 15, 2023, Istanbul, Turkiye***

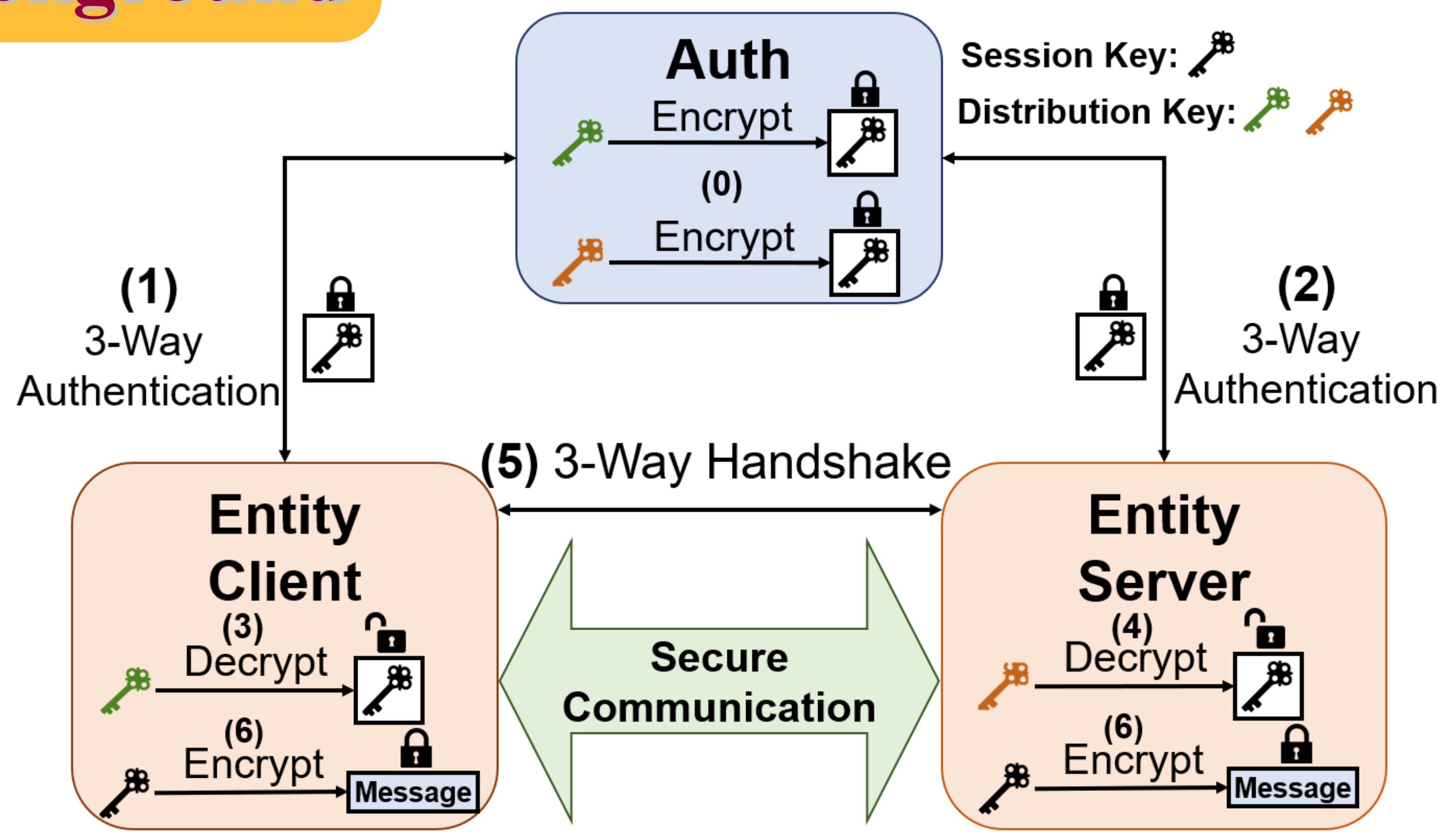
Motivation

- Many IoT frameworks do not provide enough support for securing resource-constrained devices.
- Security solutions for the general Internet (e.g., TLS) do not work well for critical parts of the IoT.
- Data Distribution Service (DDS), a widely used solution for distributed embedded systems, including ROS2 and AUTOSAR, suffers non-determinism in real-time embedded and time-sensitive IoT systems.

DDS FOUNDATION ROS 2 AUTOSAR

Background

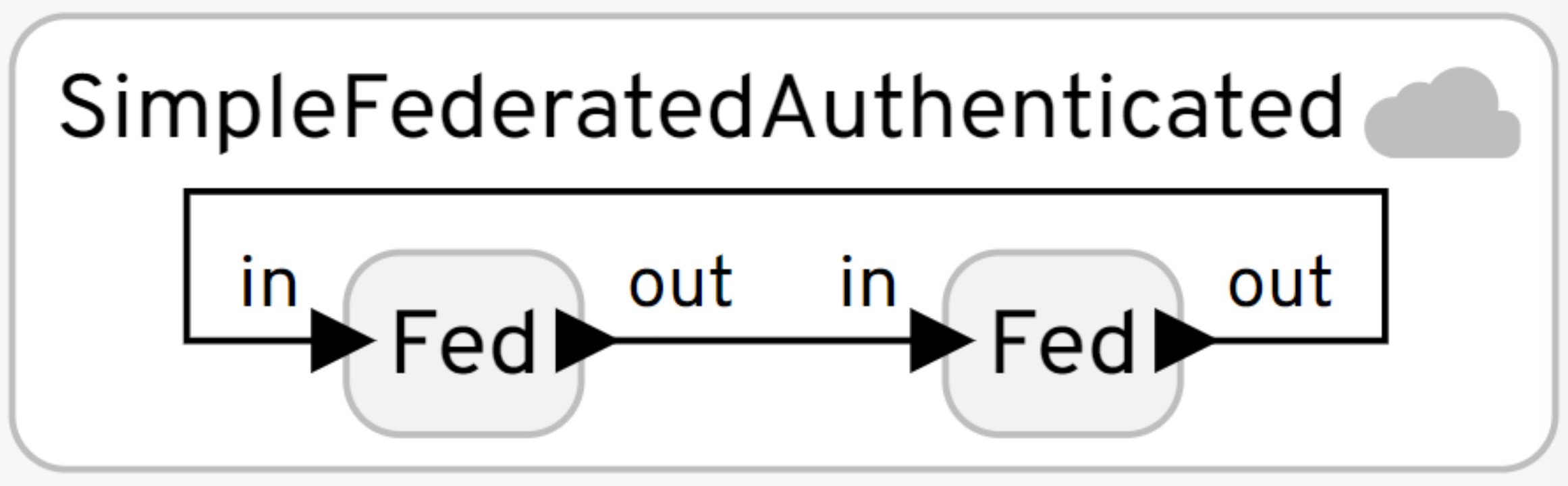
Secure Swarm Toolkit (SST)



- Edge computing-based open-source security solution for distributed IoT systems. https://github.com/iotauth/iotauth

Lingua Franca (LF)

LINGUA FRANCA

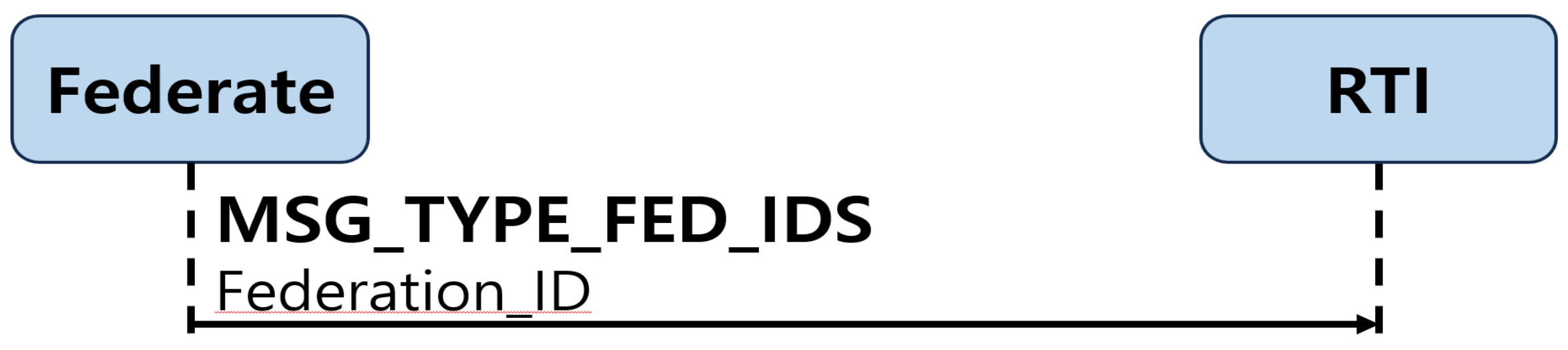


```
target C {
  timeout: 2 secs,
  auth: true
}

reactor Fed {
  input in: int
  output out: int
}

federated reactor {
  fed1 = new Fed()
  fed2 = new Fed()

  fed1.out -> fed2.in
  fed2.out -> fed1.in
}
```

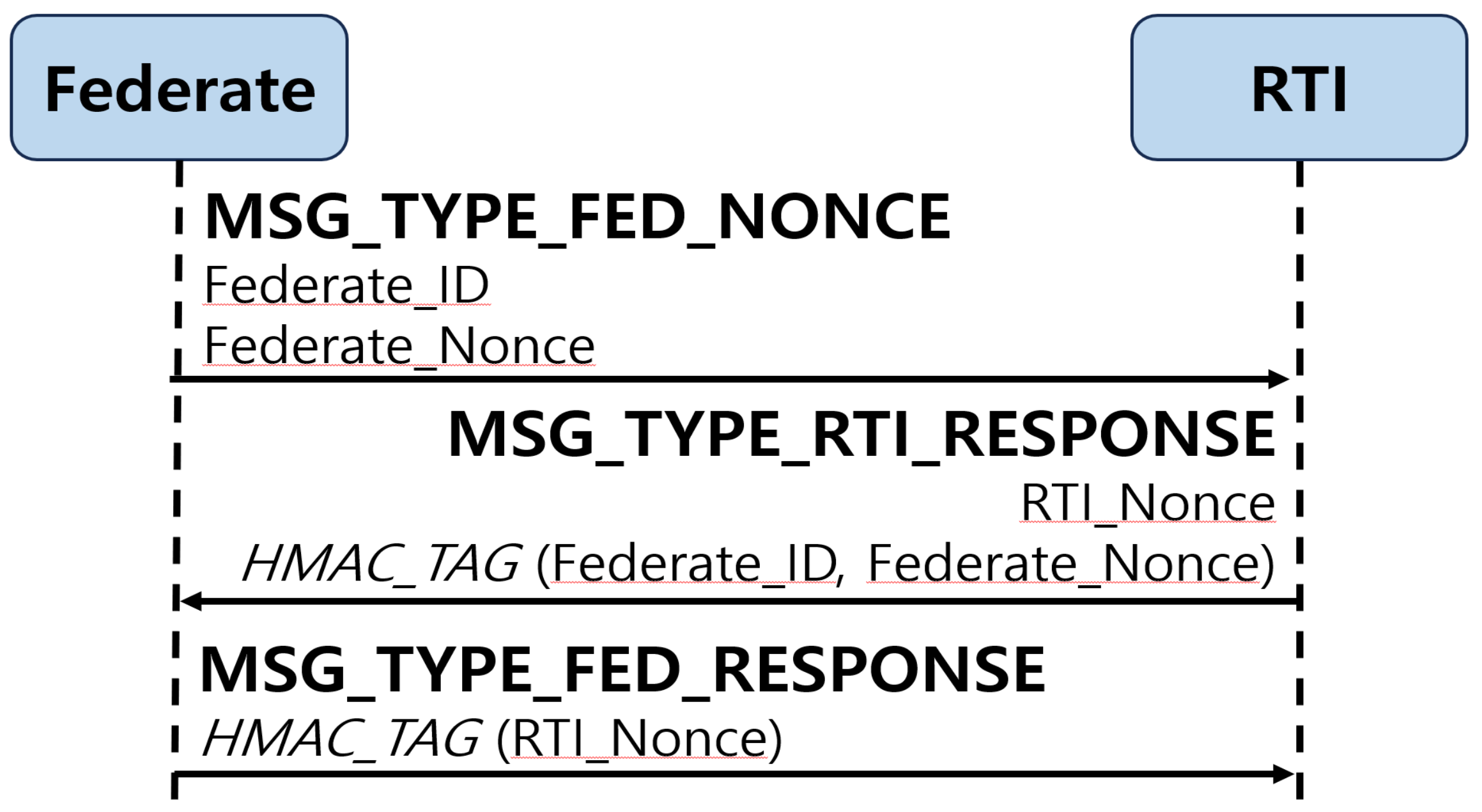
- Software platform for concurrent and time-sensitive applications.
- Supports distributed executions called ***federated execution***.
- Coordinated by runtime infrastructure (RTI) https://repo.lf-lang.org

Approach

Improved Authentication



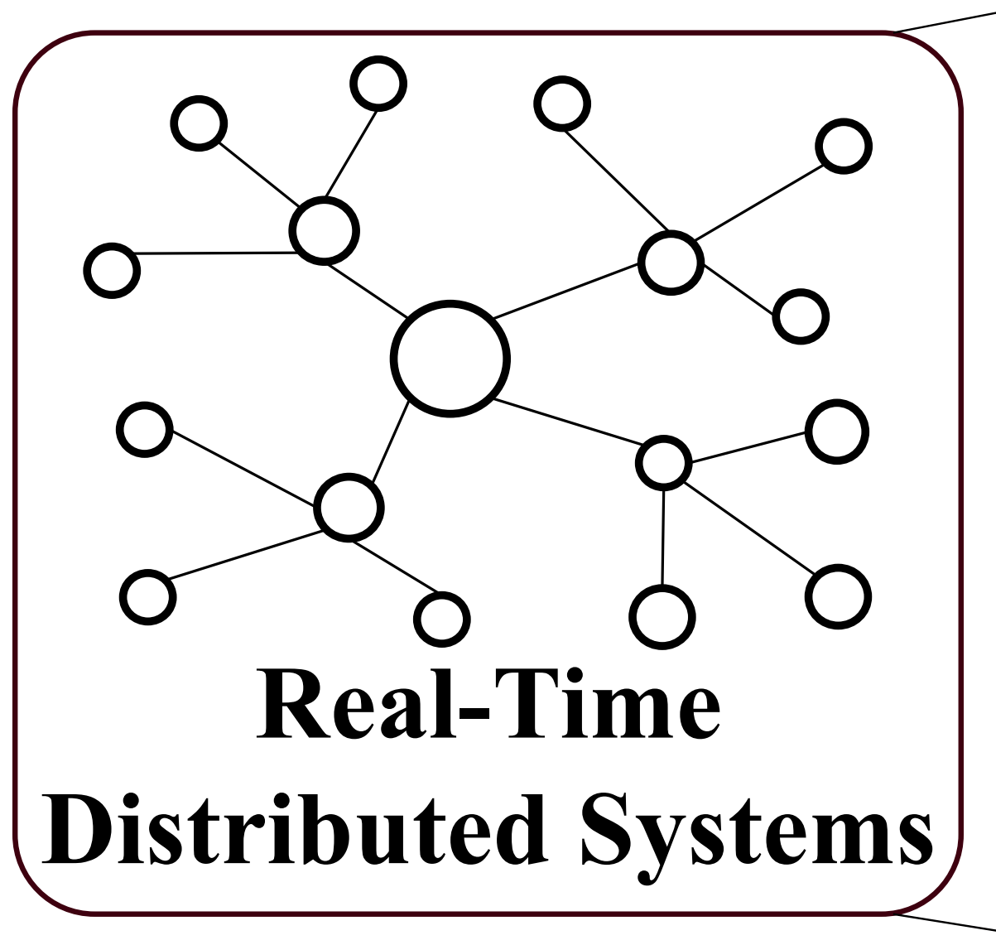
- LF, by default, performs authentication using *federation_id* sent in plaintext (not secure).



- We added HMAC-based authentication using *federation_id* as an HMAC key and a three-way handshake with *HMAC_TAG* based on random nonces (*federation_id* not sent in plaintext).

Securing Real-Time IoT Systems (Work-in-Progress)

- Support fundamental security guarantees (e.g., authentication, authorization, key distribution, secure deployment) for real-time IoT systems with resource constraints.



Timing Coordination

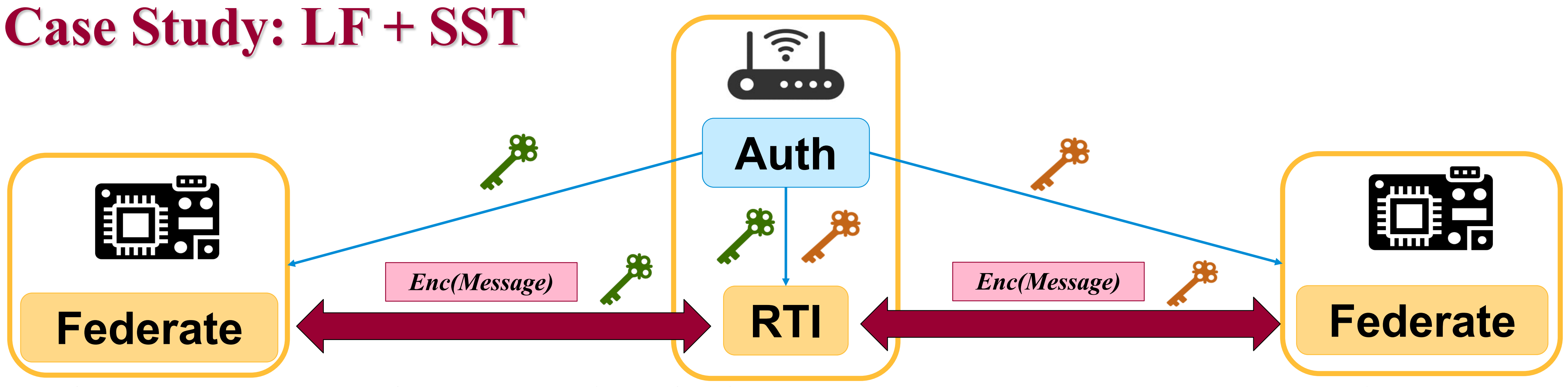
Data Protection

Network Communication

Embedded/IoT devices

Zephyr FreeRTOS SST TLS/CoAP OpenDDS MQTT ARDUINO NORDIC SEMICONDUCTOR

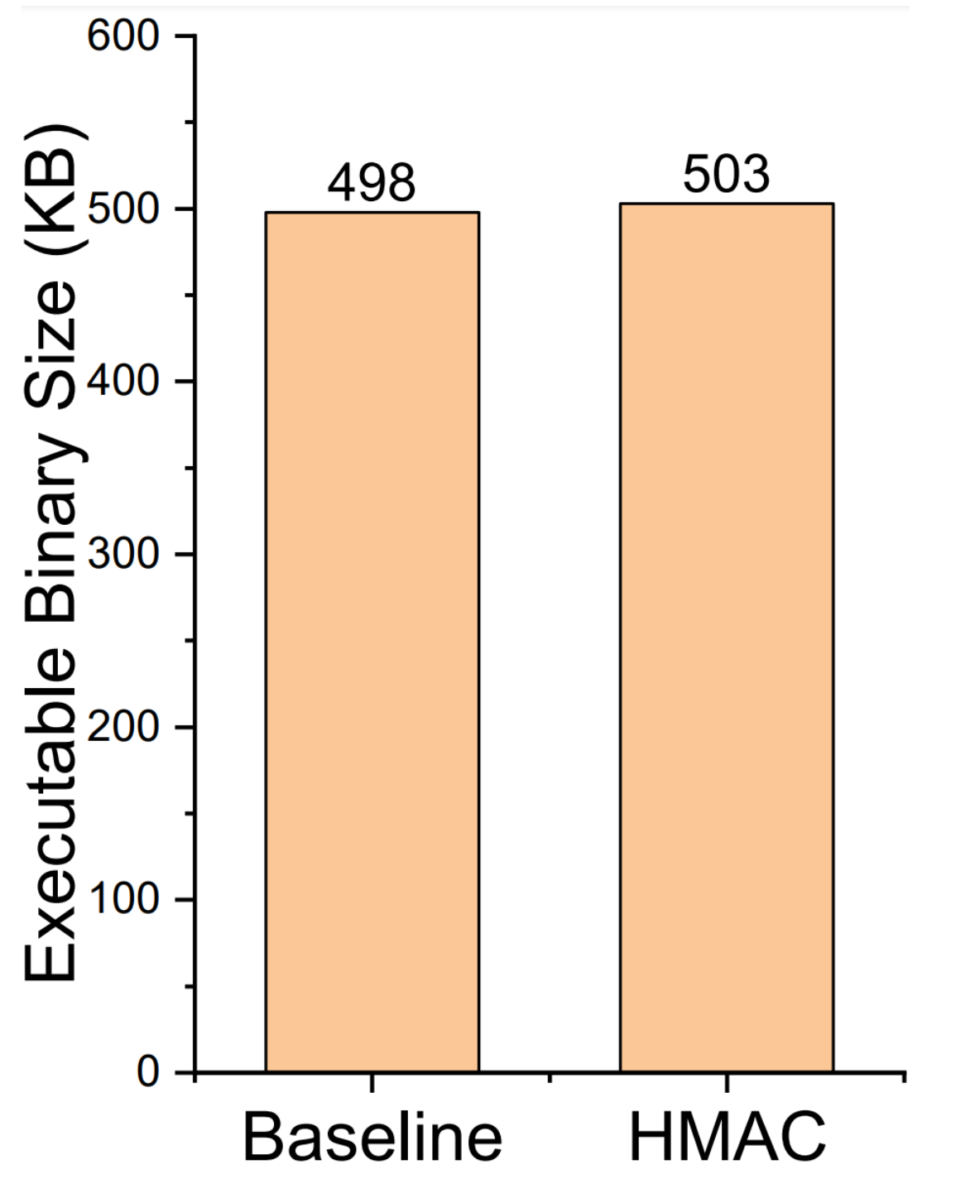
Case Study: LF + SST



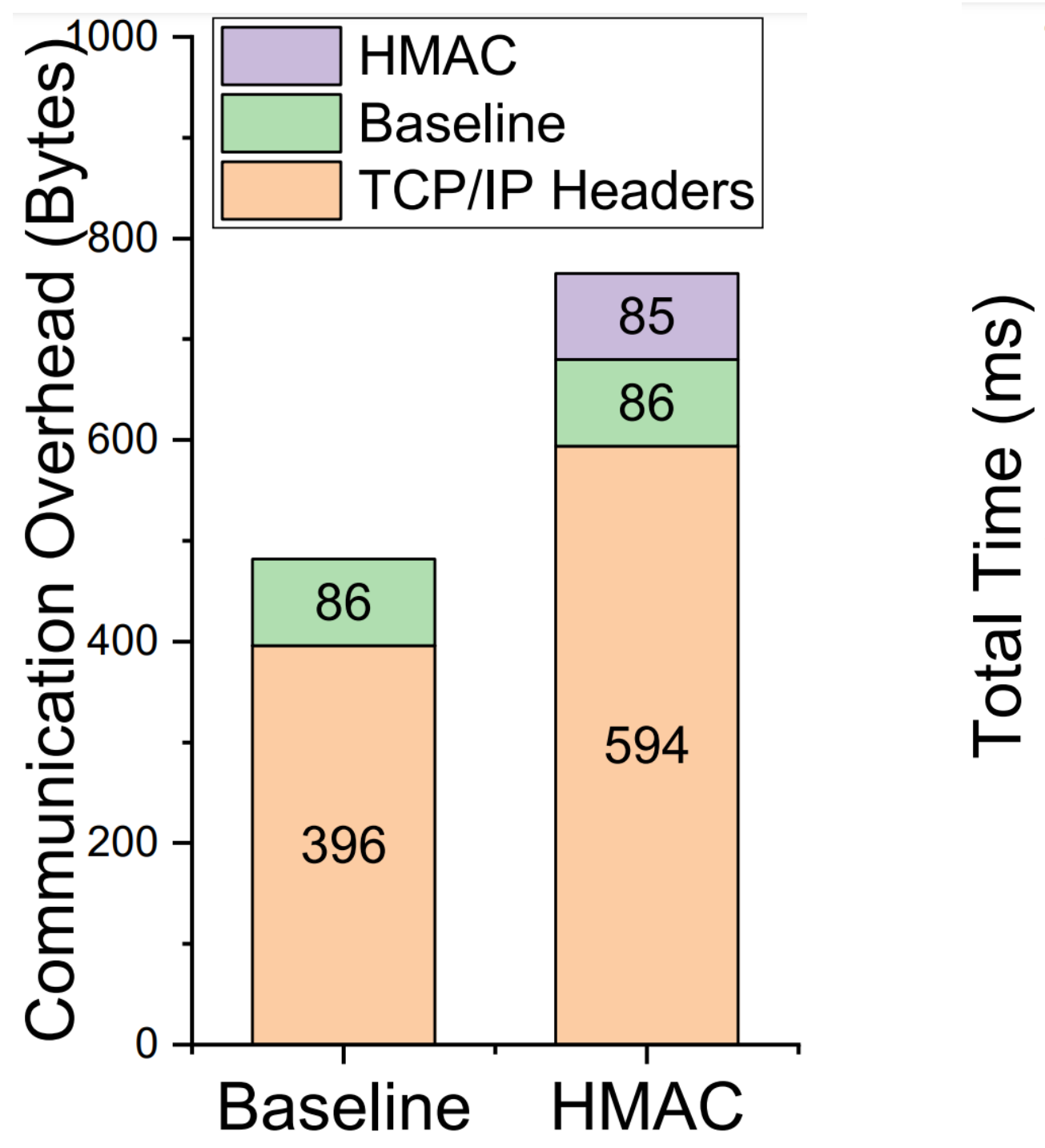
- Auth & RTI run on edge computing devices (e.g., smart gateways, on-premise servers).

Preliminary Evaluation

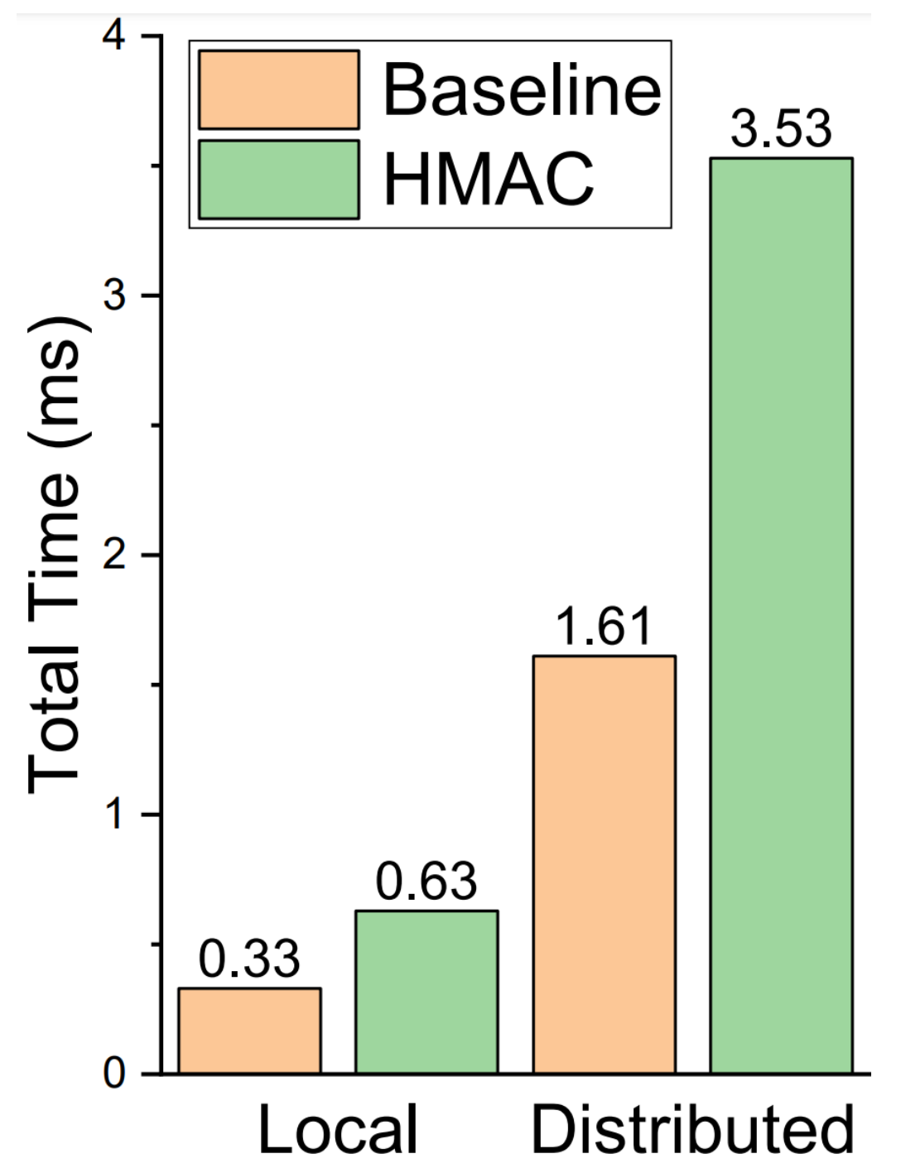
HMAC Authentication



- Only 5KB increases in binary size



- 85 bytes of additional communication overhead



- 1.92ms of additional execution time

Security Guarantees Using SST

LF Options Security Guarantees	Baseline	HMAC	TLS	DDS	SST
Secure Authentication	X	O	O	O	**O**
Access Control	X	X	X	O	**O**
Data Protection	X	X	O	O	**O**
Deployment Support	X	X	X	X	**O**
Support for Resource Constraints	X	X	X	X	**O**