SST Testbed:

An Experimental Platform of Attacks and Defenses for Networked Embedded Systems

Carlos Beltran Quinonez, Dongha Kim, and Hokeun Kim

School of Computing and Augmented Intelligence

Arizona State University

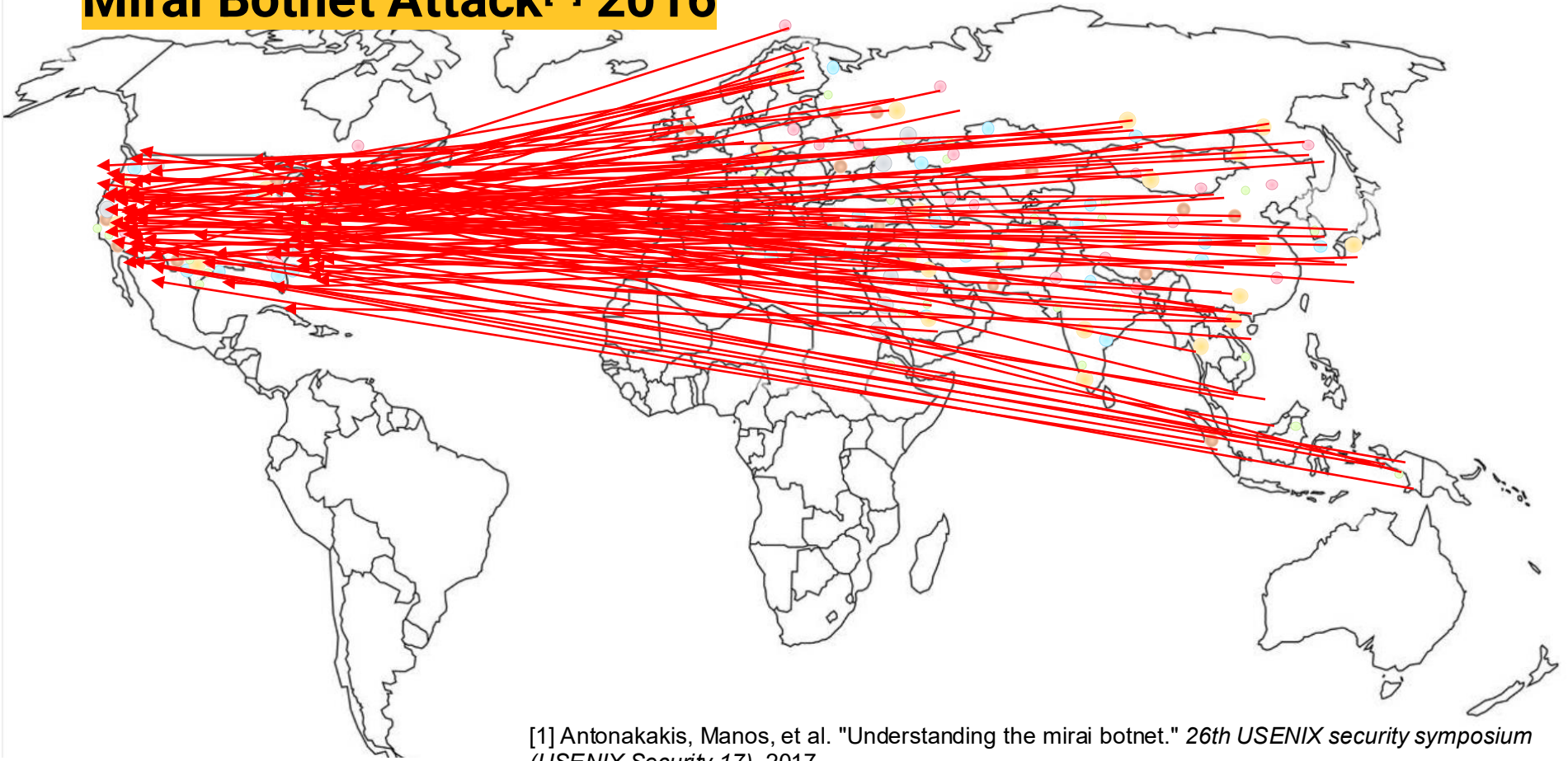
The 27th IEEE International Conference on Industrial Technology (ICIT), 4-6 March 2026, Monterrey, Mexico.

Contact: cjbeltr4@asu.edu, dongha@asu.edu, hokeun@asu.edu

Websites:

- https://labs.engineering.asu.edu/kim/
- https://jakio815.github.io/
- https://hokeun.github.io/

Mirai Botnet Attack[1] 2016



[1] Antonakakis, Manos, et al. "Understanding the mirai botnet." *26th USENIX security symposium (USENIX Security 17)*. 2017.

Motivation

- **Problem**
  - Rapid growth of IoT/embedded devices.
  - Widely integrated into daily life and infrastructure.
  - Limited resources + always connected to Internet→ **highly vulnerable.**
  - Large-scale IoT attacks (e.g. Mirai Botnet)[1] highlight serious risks.

- **Current limitations**
  - Traditional frameworks (e.g., Kerberos) not suitable for constrained devices.
  - Lack of lightweight testbeds for realistic attack/defense experiments.

-> SST Testbed for simulating network attacks on embedded/IoT systems.

[1] M. Antonakakis *et al*., 'Understanding the Mirai Botnet', in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

Contributions

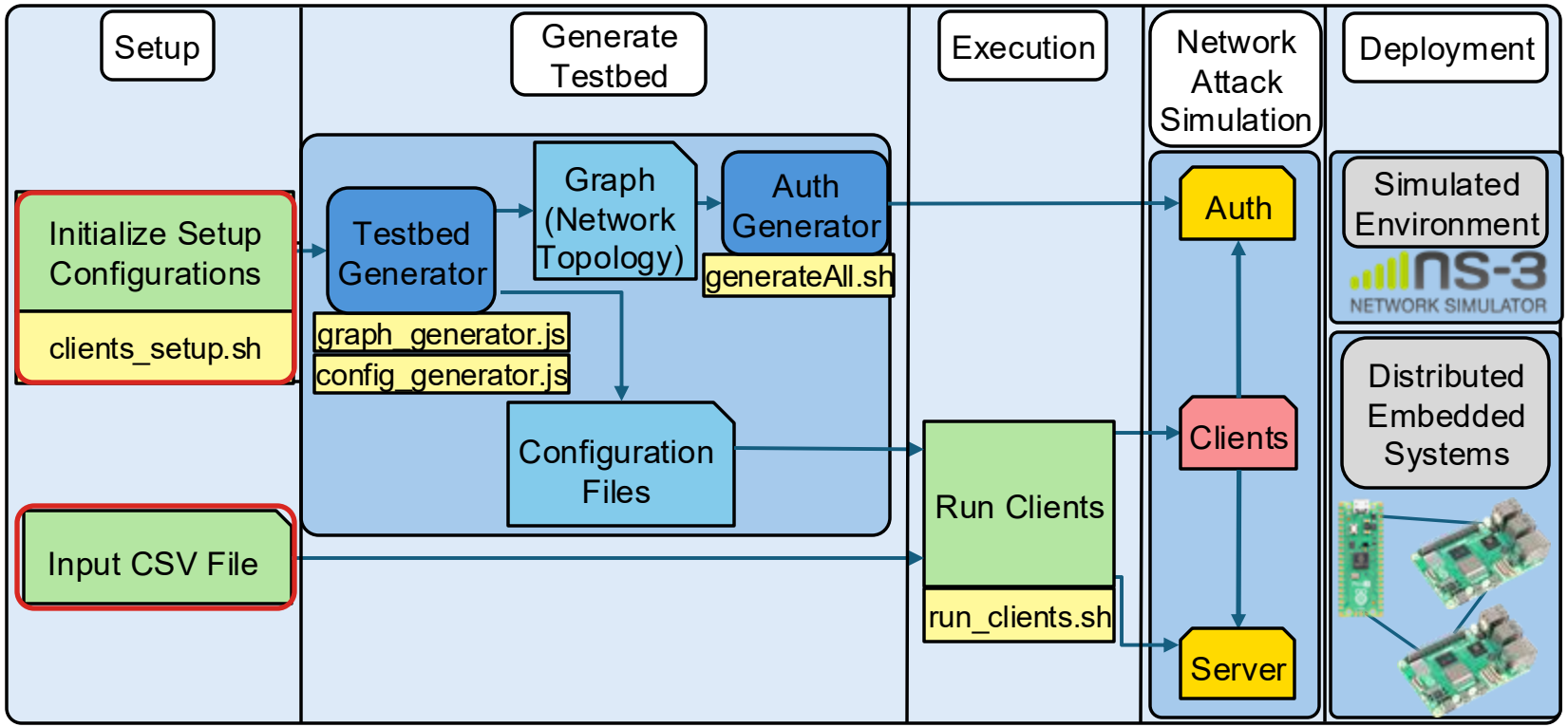
- Propose SST Testbed that **supports common network attacks**, including replay, SYN-flood, DoS & DDoS attacks.
- Support **parameterized inputs** to specify diverse attack scenarios.
- **Fully open-sourced** for researchers and developers.
- Can be used as an **educational tool for hands-on experience** of real world attack and defenses.

Background

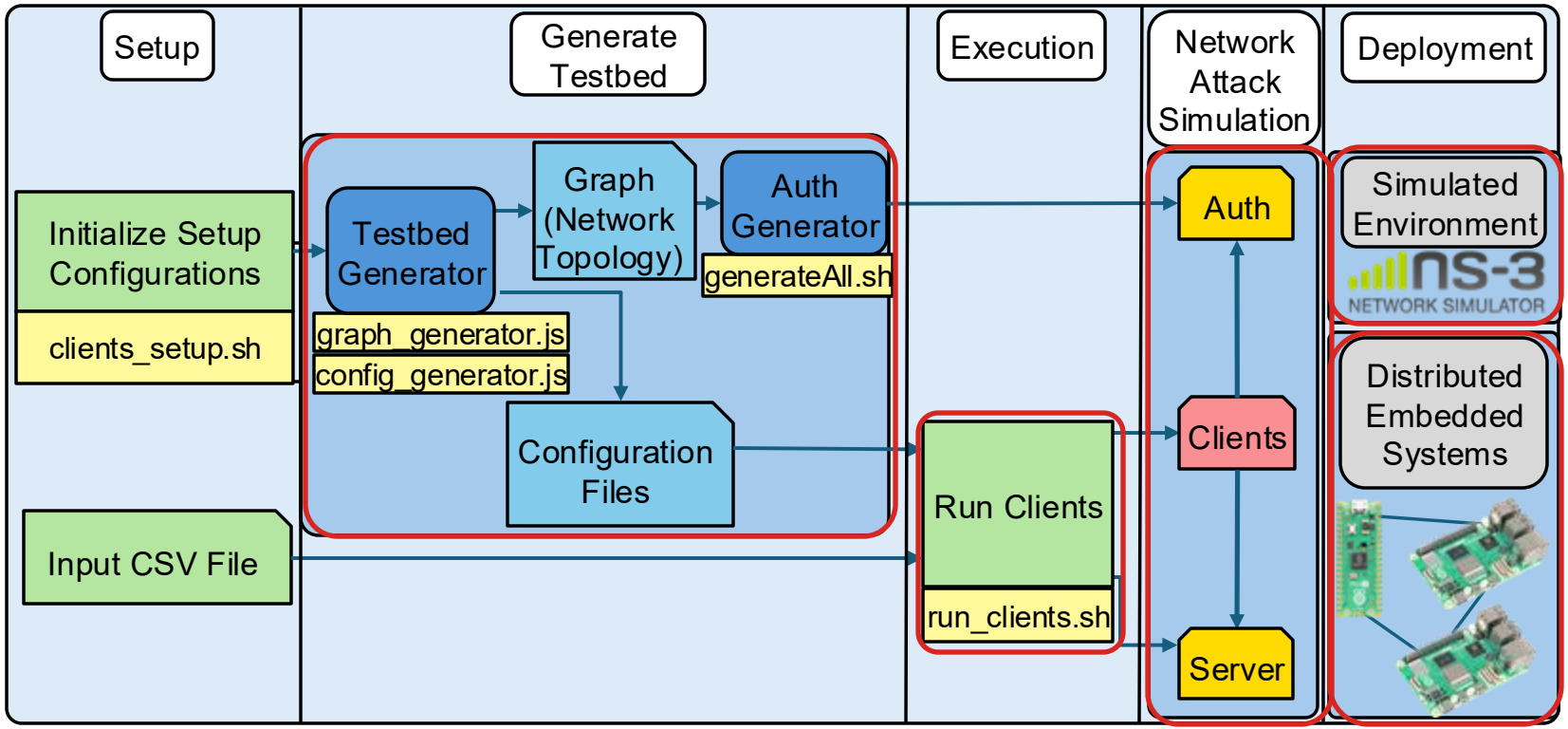
- **Network Attacks Supported**
  - **Replay Attacks:** Intercepted messages retransmitted to bypass authentication.
  - **Denial-of-Service (DoS) Attacks:** Overwhelming a service to make it unavailable.
- **Secure Swarm Toolkit (SST)[2]**
  - An open-source secure network tool with key distribution mechanisms for embedded devices.
  - ***Auth***, a local Key Distribution Center (KDC) for IoT sites. https://github.com/iotauth/
    - Provides **authentication and authorization** to local devices.
    - Locally centralized, but globally decentralized.
  - Provides a C API for embedded devices.

[2] Hokeun Kim, Eunsuk Kang, Edward A. Lee, and David Broman. 2017. A Toolkit for Construction of Authorization Service Infrastructure for the Internet of Things. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17). Association for Computing Machinery, New York, NY, USA, 147–158.

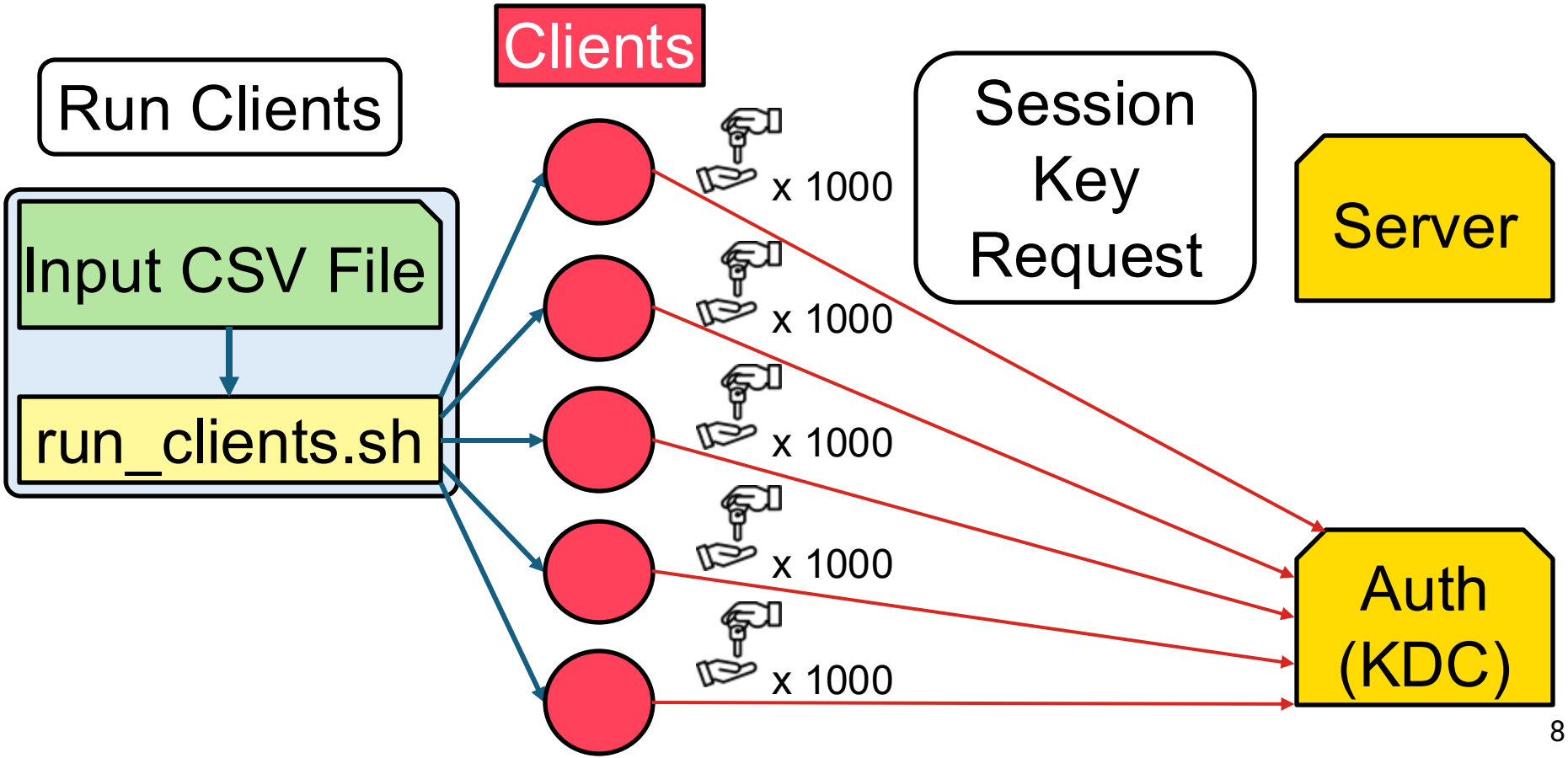
Design


Setup
Generate Testbed
Execution
Network Attack Simulation
Deployment
Initialize Setup Configurations
clients_setup.sh
Input CSV File
Testbed Generator
Graph (Network Topology)
Auth Generator
generateAll.sh
graph_generator.js
config_generator.js
Configuration Files
Run Clients
run_clients.sh
Auth
Clients
Server
Simulated Environment
ns-3
NETWORK SIMULATOR
Distributed Embedded Systems

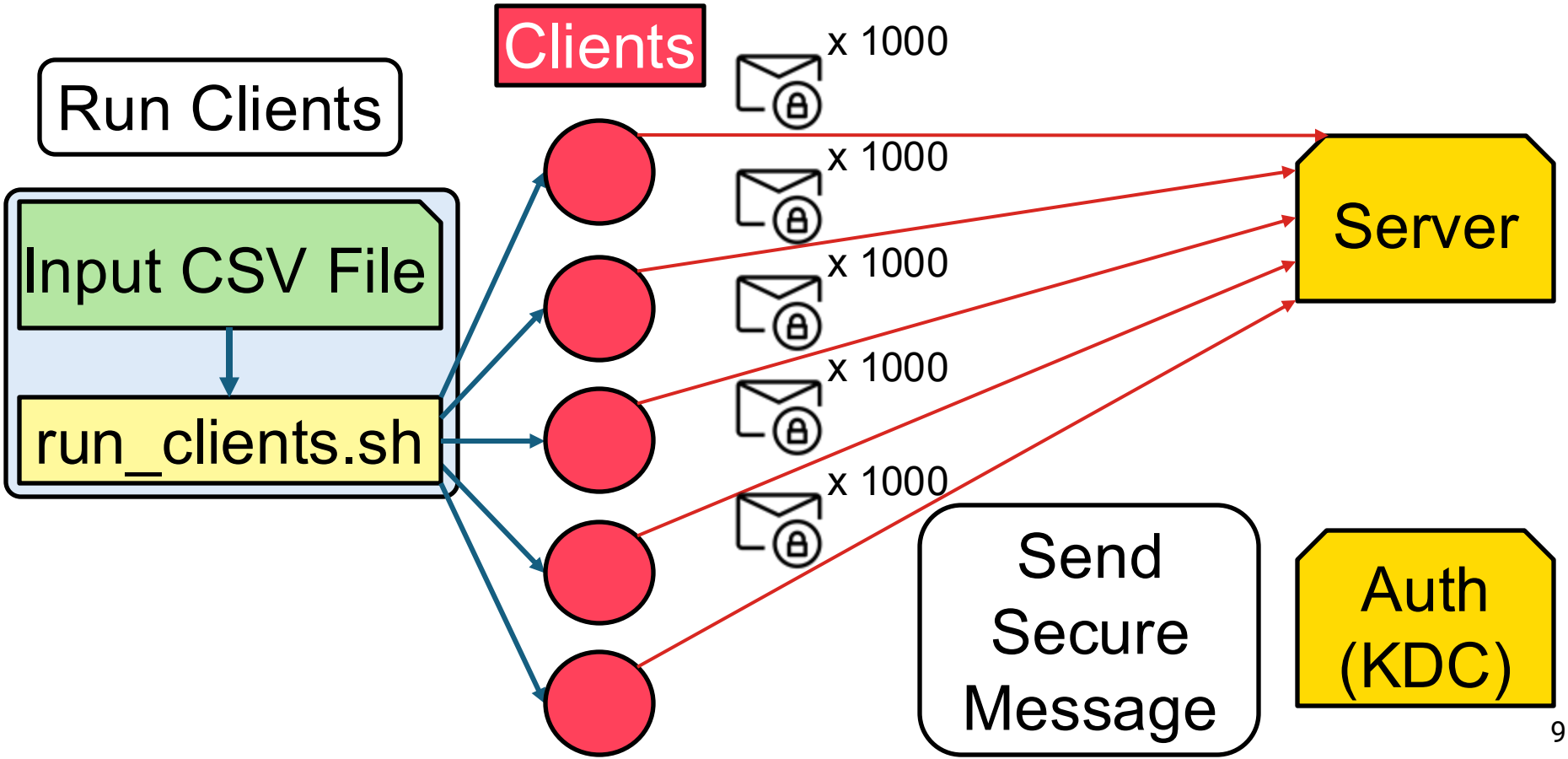
Design


Setup
Generate Testbed
Execution
Network Attack Simulation
Deployment
Initialize Setup Configurations
clients_setup.sh
Input CSV File
Testbed Generator
Graph (Network Topology)
Auth Generator
generateAll.sh
graph_generator.js
config_generator.js
Configuration Files
Run Clients
run_clients.sh
Auth
Clients
Server
Simulated Environment
ns-3
NETWORK SIMULATOR
Distributed Embedded Systems

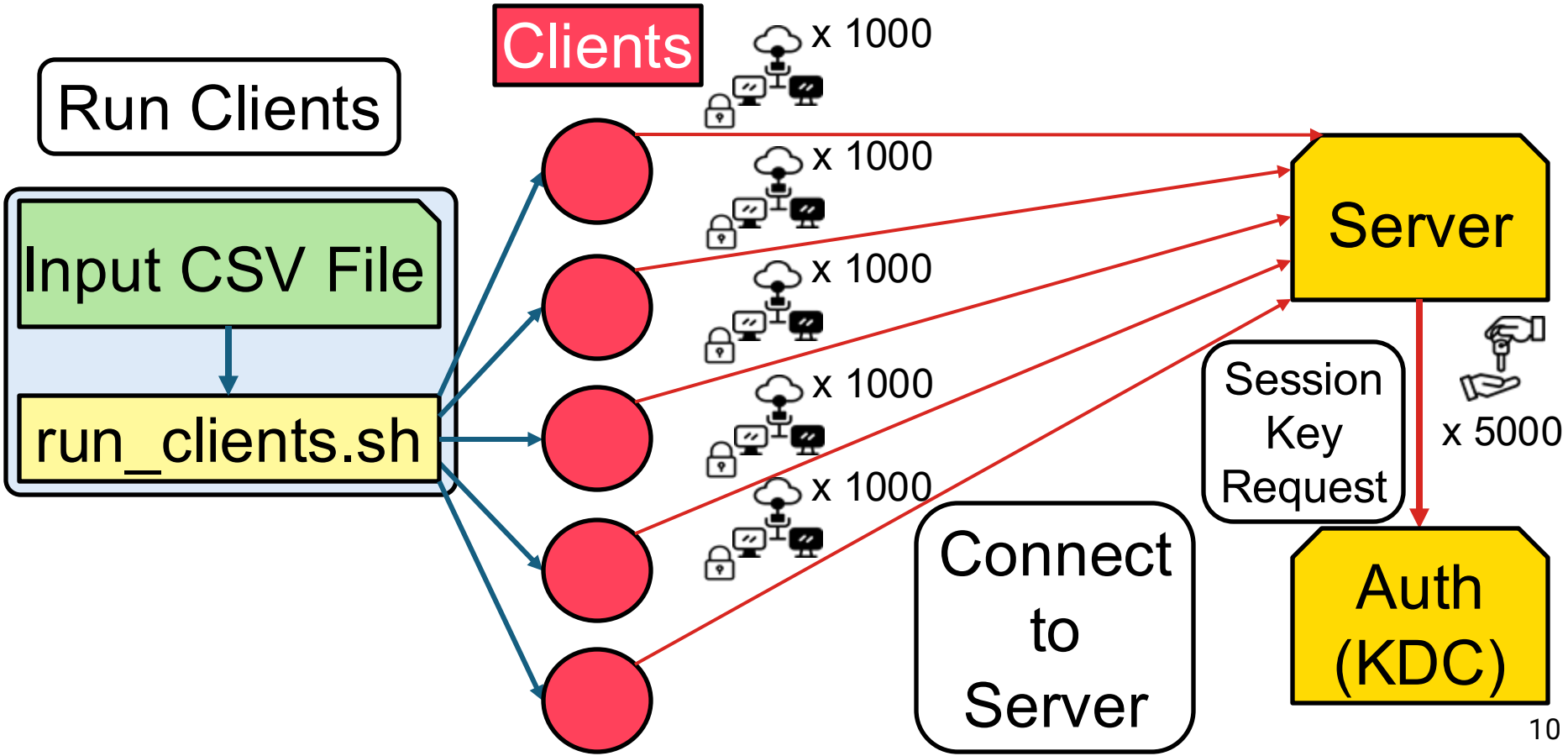
Attack on the Auth (Key Distribtuion Center)



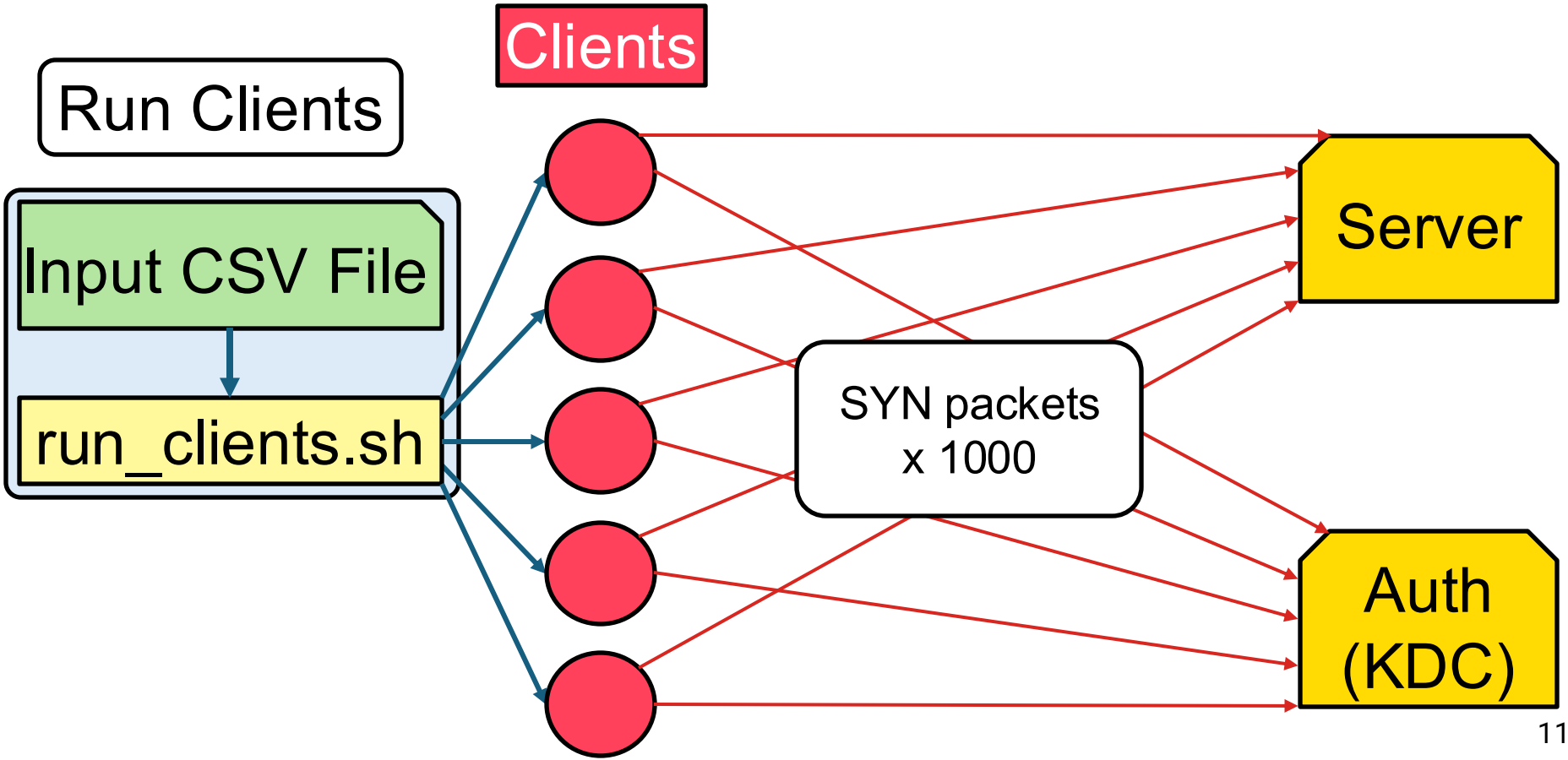
Attack on the Server



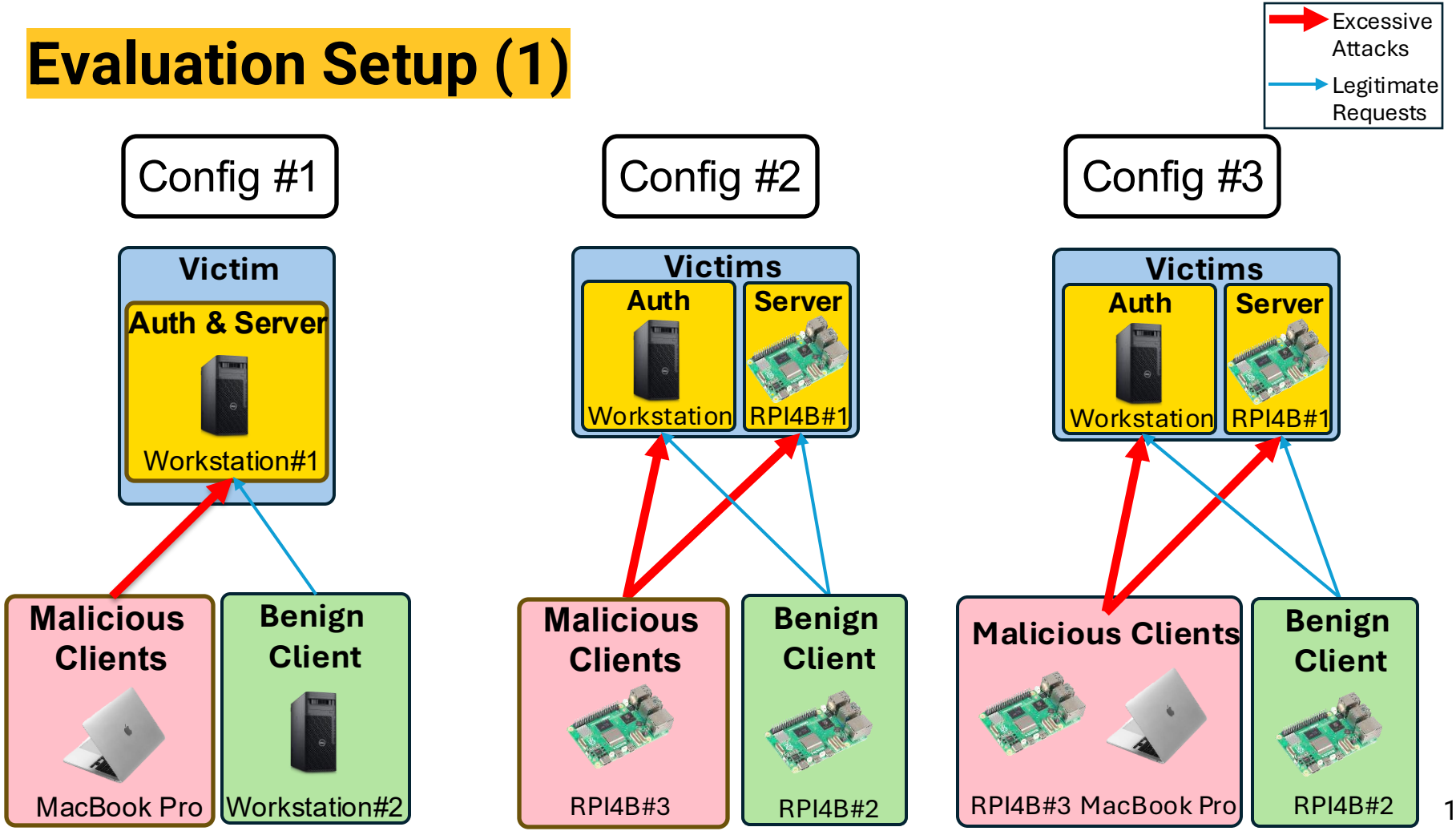
Attack on the Auth (KDC) via the Server



SYN flood attack



Evaluation Setup (1)

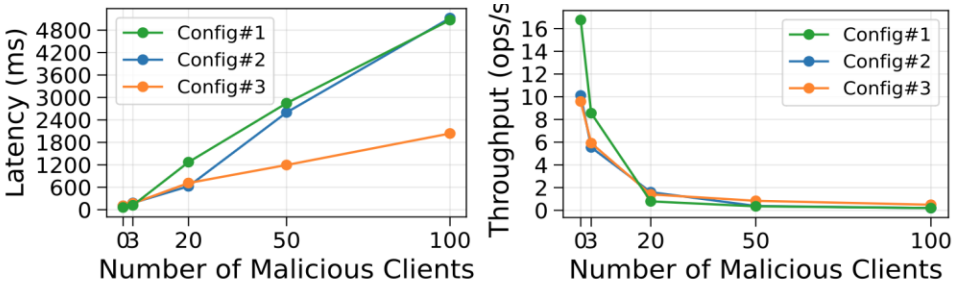


Evaluation Setup (2)

- **Setup**
  - Increase number of malicious clients from **0 to 100.**
  - All in same network.
  - **Latency**: Average response time.
  - **Throughput**: Completed operations per second.

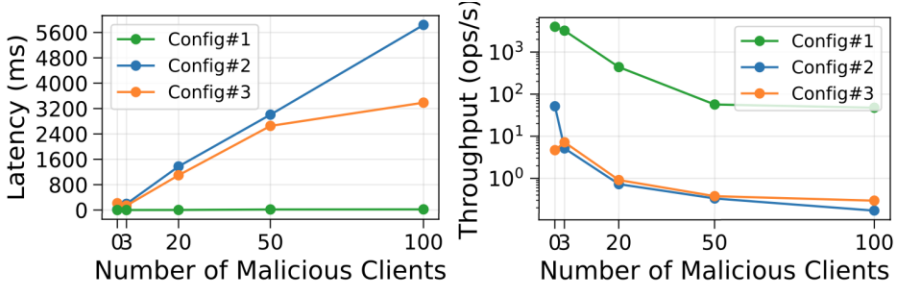
Evaluation Results (1)

- **Performance**
  - **Latency**: Increased up to 301 times.
  - **Throughput**: Decreased up to 99.99 percent.



(a) Latency degradation (b) Throughput degradation

Fig. 6: DDoS Key Attack Latency and Throughput

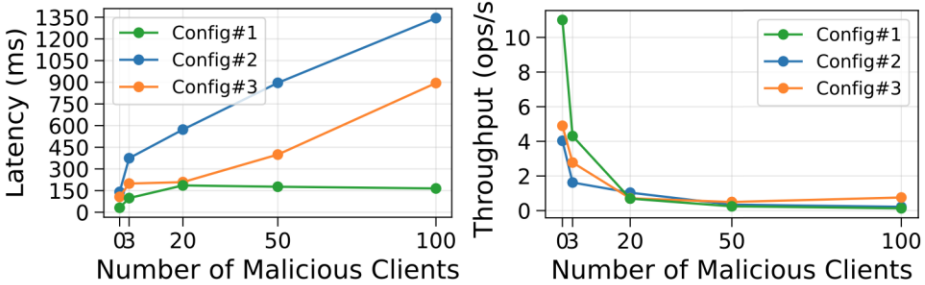


(a) Latency degradation (b) Throughput (log scale)

Fig. 7: DDoS Message Attack Latency and Throughput

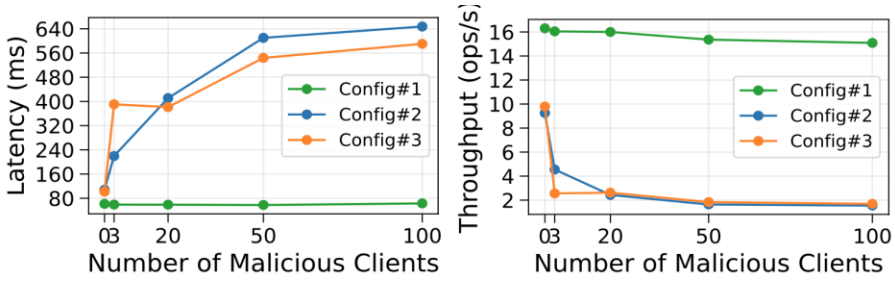
Evaluation Results (2)

- **Further results**
  - **Connect attack:** Legitimate clients fail connections.
  - Successful attacks only using resource –constraint device



(a) Latency degradation (b) Throughput degradation

Fig. 8: DDoS Connect Attack Latency and Throughput



(a) Latency degradation (b) Throughput degradation

Fig. 9: DDoS Syn Flood Latency and Throughput

Summary

ASU KIM
KNOWLEDGEABLE & INTERACTIVE MACHINES

- Propose **SST Testbed, an open-source platform** for simulating network attacks in IoT and embedded systems.
- Support **parameterized inputs** to specify diverse attack scenarios.
- **Evaluation** demonstrates that even a small number of malicious devices can cause severe performance degradation.
- For future work, we plan **to integrate defense mechanisms** into the testbed framework.

https://github.com/iotauth/sst-c-api

IEEE Industrial Electronics Society

Websites:
- https://labs.engineering.asu.edu/kim/
- https://jakio815.github.io/
- https://hokeun.github.io/

Authors:
Carlos Beltran Quinonez, **Dongha Kim**, and Hokeun Kim
Contact:
cjbeltr4@asu.edu, dongha@asu.edu, hokeun@asu.edu