Secure and Resilient Access Management for Distributed Intelligent Computing Systems

Sunyoung Kim, Computer Science
Mentor: Hokeun Kim, Assistant Professor
School of Computing and Augmented intelligence

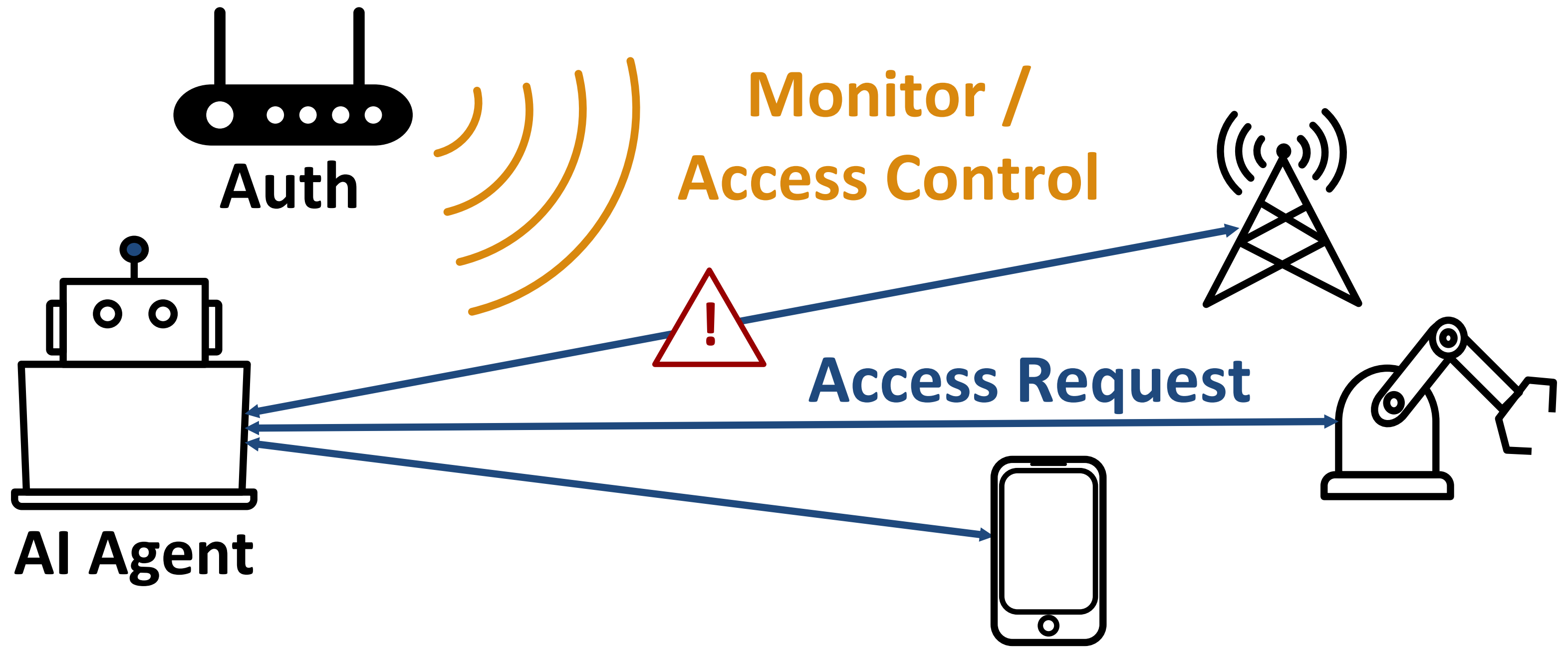
QR CODE

Motivation

- As distributed intelligent computing systems become more widely adopted, ensuring secure and reliable communication among devices has become a critical challenge.
- The growing deployment of AI agents, autonomous systems capable of perceiving, reasoning, and executing tasks, raises new security concerns [1]. Their ability to access and control external resources demands robust and real-time access management to prevent misuse or unintended behavior.

Background

Prior work proposed Secure Swarm Tool (SST) [2], an open-source decentralized security framework that uses local authorization entities (Auths) to manage trust and ensure secure communication among distributed devices.

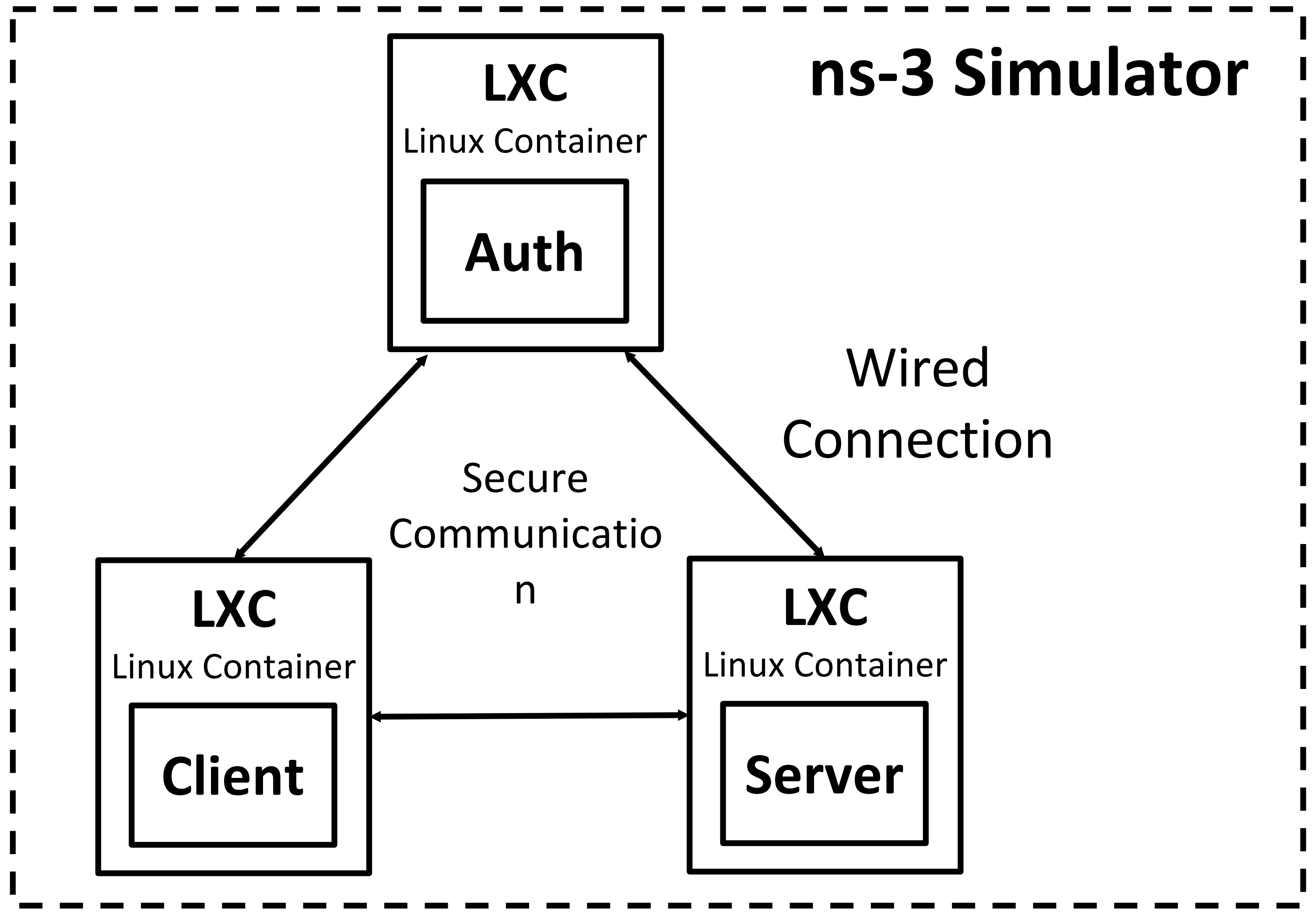


Proposed Research and Goals

- **Enhancing Robustness and Latency**: Building on our open-source project, SST (https://github.com/iotauth), we propose an enhancement in which the Auth entity continuously monitors traffic volume and notifies other entities when sudden spikes are detected. This method could reduce response latency and enhance the system's resilience.
- **Secure Access for AI Agents**: We plan to apply this experimental approach to scenarios where an AI agent has access to external resources, such as IoT devices, enabling it to work with the Auth entity to detect and respond to potential security threats through continuous traffic monitoring.
- **Simulating Real-World Scenarios**: To evaluate system robustness against practical threats, future work will incorporate the Iot-23 dataset to build a realistic test environment that includes distributed denial-of-service (DDos) attacks.

Work in Progress

- Each Auth and entity is placed in a separate Linux Container (LXC) with its own virtual network interface.
- We simulate the network environment using ns-3, a standard tool in network research and development.
- The interfaces are connected via Linux bridges to TAP devices linked to ns-3 nodes.
- We test scalability of our network simulation with 11 auths, 69 clients, and 54 servers.



References

[1] Zehang Deng, Yongjian Guo, Changzhou Han, Wanlun Ma, Junwu Xiong, Sheng Wen, and Yang Xiang. 2025. AI Agents Under Threat: A Survey of Key Security Challenges and Future Pathways. ACM Comput. Surv. 57, 7, Article 182 (July 2025), 36 pages. https://doi.org/10.1145/3716628

[2] Hokeun Kim, Eunsuk Kang, David Broman, and Edward A. Lee. 2020. Resilient Authentication and Authorization for the Internet of Things (IoT) Using Edge Computing. ACM Trans. Internet Things 1, 1, Article 4 (February 2020), 27 pages. https://doi.org/10.1145/3375837

FURI

ASU Ira A. Fulton Schools of Engineering
Arizona State University