Poster Abstract: Rethinking Collaboration Among Mobile Devices in IoT Environments

Hetvi Shastri[1], Walid A. Hanafy[1], Li Wu[1], David Irwin[1], Mani Srivastava[2], Prashant Shenoy[1]
[1]University of Massachusetts Amherst, USA
[2]University of California Los Angeles, USA

Abstract

Many emerging IoT devices are mobile, enabling them to visit new environments and networks beyond their home networks. Mobile devices often have to interact and collaborate with users and their devices, which belong to the different administrative environments they are temporarily visiting. In this paper, we envision a system for seamless collaboration among transient devices in IoT environments. The system is based on zero-conf collaboration and allows for fine-grained access control. Our proposed design supports hardware-independent interfaces and supports a large number of devices.

CCS Concepts

• **Security and privacy** → *Access control*; • **Human-centered computing** → **Ubiquitous and mobile computing systems and tools**.

Keywords

Internet of Things, Capability-based access control, Zero-configuration collaboration

ACM Reference Format:
Hetvi Shastri[1], Walid A. Hanafy[1], Li Wu[1], David Irwin[1], Mani Srivastava[2], Prashant Shenoy[1]. 2025. Poster Abstract: Rethinking Collaboration Among Mobile Devices in IoT Environments. In *The 23rd ACM Conference on Embedded Networked Sensor Systems (SenSys '25), May 6–9, 2025, Irvine, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3715014.3724065

1 Introduction

Recent technological advances have led to rapid growth in the Internet of Things in varied domains, such as smart homes, autonomous driving, mobile health, and entertainment. As a result, a broad range of static devices, such as smart appliances and mobile devices, such as robots, wearable AR/VR headsets, and fitness trackers, are becoming commonplace in the home and work environments. Advances in hardware have enabled IoT devices to evolve from *passive* sensing and actuating devices to *smart* collaborating devices that interact with one another. Prior research has largely focused on static environments, where the set of devices is largely static and devices belong to a single user or administrative domain, and have addressed topics such as performance, security, and privacy that arise in this settings [1, 3].

SenSys '25, May 6–9, 2025, Irvine, CA, USA

ACM ISBN 979-8-4007-1479-5/25/05
https://doi.org/10.1145/3715014.3724065

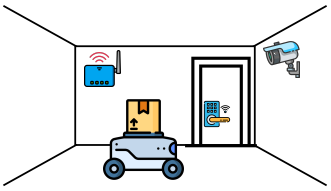

Figure 1: Collaborative Delivery Robot Scenario: Robot entering, gaining access to the lock and camera.

In contrast, in this work, we focus on transient environments, where users and their smart devices *roam* across IoT environments. In this case, the roaming devices must access and collaborate with heterogeneous devices owned by multiple administrative authorities, requiring seamless and fine-grained access.

Motivating Scenario: Consider the scenario in Figure 1, where online stores are using delivery robots or drones that can deliver packages (e.g., Domino's Pizza delivery robots and drones). While delivery robots or drones are currently designed to deliver items to a user's doorstep, in the future, such robots can collaborate with IoT devices in a home or building to securely unlock a door (e.g., garage door) to drop off a package inside the home or building. These scenarios include one or more guest devices that temporarily access devices in a different network. Importantly, access to such devices or services must be done securely, and in a fine-grain manner where guest devices only access subset of devices or services.

Motivated by the aforementioned scenario and user studies on the future of IoT-based collaboration [2, 4] that point to the need for fine-grained access in collaborative IoT environments, we envision a system that enables seamless cross-domain collaboration between guests and native devices and services (e.g., embedded intelligence) running in the host environment. The design of the system is based on four key principles.

- **P1 Zero-Conf Collaboration:** The system should allow guest devices to roam in different environments and temporarily interact with devices in that environment with no manual intervention or configuration.
- **P2 Granular Access:** The system should allow granular access control, restricting guest devices to accessing specific native devices, actions, services, and rates, while providing users an easy way to manage and configure such granular access.
- **P3 Hardware Independent Communication:** The system should support hardware-independent communication, enabling guest devices to interact with other devices without knowing vendor-specific interface details.
- **P4 Scalability:** The system should operate efficiently in crowded environments where the number of devices is large, and the set of guest devices changes frequently.

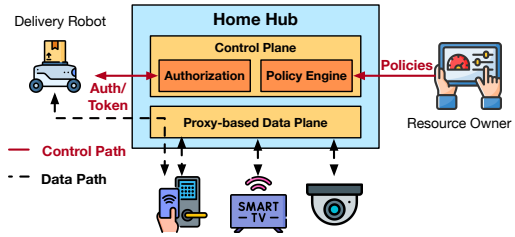

Figure 2: Design Overview.

2 System Design

Figure 2 depicts the architecture of our system that can be integrated into smart home hubs (e.g., Google Home and Alexa). Our system features a control plane that allows resource owners to figure out access control policies and a zero-conf authorization framework that automates granular access to guest devices. Additionally, our system comprises a data plane that enforces fine-grained runtime access controls, applies rate limits, and provides hardware-independent interfaces.

Policy Engine. The policy engine enables high-level access policy specification and translates them into fine-grained control rules. Once the policies are defined, no manual intervention is required upon arrival or departure of guest devices. The policy engine uses a fine-grained attribute-based access control model, allowing resource owners to define granular access and resource control over their devices. In addition, the policy engine integrates dynamic grouping, allowing high-level user-defined groups to abstract device enumeration and access details, which enhances scalability and usability.

Authorization. When a guest device arrives, the authorization subsystem uses the policy engine to find all access policies that match this device and generates a list of capabilities for each allowed device. The authorization subsystem then generates cryptographically signed capability-based tokens, which are distributed to the guest devices to facilitate secure and controlled access.

Proxy-based Data Plane. Our proxy-based data plane encapsulates all interactions with environment devices through a lightweight proxy responsible for enforcing access control policies, securing all communications, and providing hardware-agnostic interfaces. At runtime, requests are verified and forwarded to the device only if they comply with the assigned capabilities and remain within the specified rate limits. Our proxy-based data plane establishes hardware independence by implementing a virtual interface tailored to each device type. This abstraction allows guest devices to interact seamlessly with devices without having to know the device's specific API.

3 Preliminary Results

In this section, we demonstrate the effectiveness and performance of our system using a case study of the delivery robot. We implemented our prototype using the control and data planes using Python and GRPC. Figure 3 shows our experimental testbed. In this experiment, the delivery robot arrives at a house carrying a package for delivery to a designated corner. The robot then requests access to the garage door lock and camera, which aids it in making path-planning decisions. Table 1 shows the steps and the time

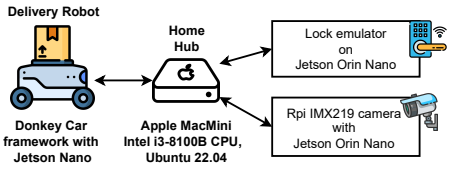

Figure 3: Experimental testbed

Table 1: Results of Delivery Robot Case Study.

Event	Time (ms)	Verification Time (ms)
Robot Entering	151.51	NA
Lock Access	43.22	1.07
Camera Access	85.36	1.13

taken by each step in this scenario, which does not require any human intervention — except for setting the high-level policies, which happens beforehand. The results highlight the efficacy of our system, where it takes only 151.51 ms to connect the guest device and allow it to access the lock and the camera (i.e., evaluate the access control policies, list the devices, generate capabilities, and generate the access control tokens). In addition, the results depict the end-to-end responsiveness of the proxy-based data plane, where it takes 43.22 ms to execute the unlock door command and 85.36 ms to access the camera stream, whereas in both cases, it takes ~1ms to verify the access token.

4 Conclusion and Challenges

The transient nature of many IoT devices requires rethinking their collaboration, where roaming devices must access and collaborate with heterogeneous devices owned by multiple administrative authorities. This paper envisioned a zero-conf collaboration system for transient devices in shared IoT environments. The system ensures secure communication through cryptographically signed capability-based tokens and allows granular access to devices and services. In addition, the system employs a vendor-agnostic approach, enabling easy device integration. In implementing our system, we highlight the following challenges. First, the current fine-grained access control specifications approaches are often based on complex syntaxes, which are not suitable for typical users. Second, our proxy-based data plane must support real-time tasks (e.g., video stream) and support concurrent connections. Third, the proxy interfaces must balance generality with effectiveness.

5 Acknowledgments

This research is supported by NSF grants 2211302, 2325956, 2213636 and US Army grant W911NF-17-2-0196.

References

[1] Vikas Hassija et al. 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* 7 (2019), 82721–82743.
[2] Weijia He et al. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *USENIX Security 18*. 255–272.
[3] Amit Kumar Sikder et al. 2021. A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications. *IEEE Communications Surveys & Tutorials* 23, 2 (2021), 1125–1159.
[4] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. 159–176.